A Network of One's Own

struggles to domesticate the Internet

David Chatting

Department of Design
Goldsmiths, University of London

Thesis submitted for the degree of Doctor of Philosophy (PhD)

Declaration

The work presented in this thesis is my own.

David Chatting

Acknowledgements

To those whose kindness and support, large and small, have enabled me to engage in this thesis work over the past five years. This has been a huge challenge for me intellectually and personally, with a good portion of it completed as we worked through the troubles of a global pandemic together. It is inconceivable that I could have completed this without your help, thank you.

First and foremost, I want to acknowledge my deep gratitude to my supervisors Bill Gaver and Andy Boucher, for in equal part their guidance, care, and good humour. It is their example that brought me here and the opportunity to pursue this thesis work with them has been the ultimate privilege. I am deeply grateful to my examiners, Phoebe Sengers and Alex Taylor who engaged with this thesis in such careful and constructively critical ways; together they made my viva day the most intellectually engaging experience of my career. My upgrade examiners Matthew Fuller and Rebecca Fiebrink also gave valuable early feedback and encouragement for which I am thankful.

The Interaction Research Studio has been the most stimulating environment and I am proud to count its talented members: Mike Vanis, Andy Sheen, Dean Brown, Naho Matsuda, Liliana Ovalle and Jen Molinera, as my colleagues and good friends. This thesis is the latest chapter of a professional journey that I started as an apprentice at BT Labs, through a scholarship to Birmingham University and then eventually to the Royal College of Art; I am profoundly grateful to my teachers along the way and especially to Tony Dunne and Fiona Raby who believed I could be a designer. John Bowers, you know you are deeply entangled in this story too – thank you.

Many thanks to Alex Wilkie for regularly making me think very hard, not least by convening the excellent Design Matters seminars. The Goldsmiths Design community has been a huge support to me intellectually and emotionally. Special thanks to Sarah Pennington who has been there at the end of a video call for many of the final hours of this writing and to Thomas Marriot who has been a good friend and excellent company along this journey. Sincere thanks also to Becca Rose Głowacki, Mike Thompson, Liam Healy, Tom Keane, Tim Miller and Tom Critchley. I am looking forward to comparing notes with Paulina Yurman on this next phase of the academic journey, thank you for your early encouragement.

Over the past nine years, I have made Newcastle my home and I am forever grateful to David Kirk and Abigail Durrant for showing me the academic path and this beautiful part of the world. I am indebted to the city's design research community at Newcastle and Northumbria Universities, and to colleagues new and old. In particular, I want to thank Nick Taylor and Jon Rogers for their kindness and support during the latter stages of this thesis. Rob Anderson, Clara Crivellaro, James Hodge, Dan Jackson, Kyle Montague, Tom Nappey, Tim Shaw, Vasilis Vlachokyriakos and Zander Wilson; thank you for the many ways in which you have individually helped me and made it fun – not least with the occasional pint. I am exceeding thankful for the wise counsel of Sarah Taylor. Andy and Amanda Gower, Tim Sergent and Scott Kirkman, your friendships defy my simple categories!

Cally Gatehouse, Chris Elsden, Ed Jenkins, Andy Garbett, Emma Allen, Siobhán Quinn, Dan Foster-Smith and Tom Schofield; for your excellent company and your numerous kindnesses, simply thank you. My dear transatlantic friends have been there virtually for me too: Mark McKeague, Naomi Elliott, Diego Trujillo Pisanty and Koby Barhad, I can't wait to see you in three dimensions! Josh Edwards thanks for getting me outdoors; it's been a huge joy to play football with you, Adam, Ben, Dom, Josh T, Josh D, Joel and Lewis on a Thursday evening – cheers lads!

Many thanks to all the participants in my studies, without your generosity there would be no thesis. This work has been made financially possible with the support of the AHRC Design Star, Centre for Doctoral Training, with the administrative support of Polly Harte at Reading University and Rosamond Eele at Goldsmiths.

Finally, to my family: Trevor and Eileen, Sarah and Steve, Daniel and Katie – thank you for your unwavering support – it's done!

In loving memory of my Grandma,

Susannah Simmonds (1903 – 1982)

Abstract

This thesis is a design research practice-led inquiry into the domesticated Internet. It first seeks to complicate simplistic corporate and academic visions of the home by naming some of the struggles it encounters – not least to assert a private home and network of one's own. It is argued that a century of domestic technologies has emphasised invisibility, ubiquity, and automation in ways that obscure a network of exploited people and finite resources. Furthermore, these technological ambitions are met through machine surveillance, in ways newly enabled by the domesticated Internet, that threaten the privacy of the home.

In response, this thesis seeks some practical ways to design alternatives that assert a network of one's own and makes the work it implicates visible. The methodological approach is broadly Research Through Design supplemented by a practice described as *designerly hacking* through which hidden technical potential is revealed and given meaning. Two empirical studies are described that together make an account of the technical possibility and social reality of the networked home: an autobiographical technical exploration of the author's home and network with the making of hacks and Research Products privately and in public; and a cultural probe engagement with six rented households surfacing contemporary accounts of the domesticated Internet and in particular the challenges and opportunities of wireless networking. Together this yields a series of technical and social insights for design and two forms are offered to communicate these: a framework for understanding change in the networked home (*The Stuff of Home*) and a set of 30 design patterns for a network of one's own; each invites different analyses. The conclusion then draws together the multiple threads developed through this thesis and offers some reflection on the complexity of doing contemporary technical design work.

Table of Content

List of Figures

Chapter One: Introduction

This thesis is about how we domesticate the Internet; at its heart, it questions what we mean by home and what we want it to mean. The subject of my concern is the domestic Internet of Things (IoT) as they exist and could shortly be – an ad hoc collection of computers, tablets, phones, televisions and games consoles, with an increasing number of lights, doorbells, security cameras and thermostats, that constitute the networked home, or perhaps even the so-called *smart home*.

This introductory chapter serves to lay out the context and questions of this thesis; it has four sections. Firstly, it introduces some divergent ways home is commonly talked about and idealised, to suggest that homes have some exceptional qualities and are often somewhat static. Secondly, it offers a broad account of the domestication of the Internet over the past twenty years; how British homes have been changed to accommodate the Internet and how our imagination of both has evolved. Thirdly, it seeks to demonstrate that domestication is but one struggle that is situated in the home, newly exacerbated by the network – the others being struggles of precarity, independence, living with others, productivity, the market and centrally of privacy. Finally, with deference to Virginia Woolf, it suggests ways to struggle for *a network of one's own*, a self-determining private home, as an alternative to the corporate privatising logic of Silicon Valley's Internet of Things. In doing so, this chapter sets the scene for the design research inquiry of the thesis, an exploration of how such alternatives might be practically designed and how one might negotiate the inherent complexities of the network.

Idealising Home

I live in a rented top-floor two-bedroom flat in Osborne Court, Jesmond – a prosperous area of Newcastle upon Tyne in the North East of England. Osborne Court is a 1930s Art Deco apartment building, built by a local Jewish businessman for European refugees fleeing from the rise of Hitler. I have lived there, on my own, since 2013 when I moved from London to take a position at Newcastle University. While my PhD studies are at Goldsmiths in London, I can afford a better quality of life in Newcastle. My home is prioritised by my sense of privacy, stability and comfort – a sanctuary.[1]

[1] At times this thesis will very deliberately adopt a biographical, indeed autobiographical, tone with respect to some of the characters it implicates to suggest a little of their motives and position, including often my own.

In this section, I explore some of the ways that home is talked about – as it is, as it was – because this shapes a collective imagination of how it could be. My ideas of *homely* are firmly rooted in a British experience, culturally entangled most strongly with Europe and Northern America. Nonetheless, these are not particularly consistent ways of talking about home; some are practical, some are romantic; each prioritises a different aspect of homelife from a different perspective. To offer a flavour of this, consider these popular idioms in use in the English language:

Home is Where the Heart is: generally attributed to the Roman naval commander, Pliny the Elder (CE 23-79). Clearly, this emphasises the positive emotion of being at home and implicitly the love of family that surrounds it. It does not suggest that home is necessarily historically or geographically rooted, just that emotionally this is where there are feelings of belonging.

Home, Sweet Home and *There's no Place like Home*: these are song lyrics by Henry Bishop in the opera Clari, first performed in London in 1823 – and re-popularised by The Wizard of Oz in 1939. They emphasise the exceptional positive qualities of home, distinct from everywhere else; they also have an implied sense of permanence and longevity.

An Englishman's Home is his castle: established as English common law by Sir Edward Coke in 1644. The original quote is: "*For a man's house is his castle, et domus sua cuique est tutissimum refugium [and each man's home is his safest refuge]*" (Coke, 1644, p. 161). This is a home set in opposition to a hostile world and a home in which the individual (man) has dominion over the goings-on within – *behind closed doors*. The symbolism of the castle is of permanence and feudal power; with the implication the man is the *king*. Yet this is more than an idiom, in 1999 the so-called *castle doctrine* was used to defend Norfolk farmer, Tony Martin, who shot a burglar dead in his home, and variants of this law can be recognised internationally.

The *wildness of domesticity* is G.K. Chesterton's (relatively unknown) conception of the home as a place of liberty; it shares some of the *castle doctrine's* intention, but perhaps with a gentler whimsy. "*The truth is, that to the moderately poor the home is the only place of liberty. Nay it is the only place of anarchy. It is the only spot on the earth where a man can alter arrangements suddenly, make an experiment, or indulge in a whim. […] For a plain hardworking man, the home is not the one tame place in a world of adventure. It is the one wild place in a world of rules and set tasks .*" (Chesterton, 1912).

A woman's place is in the home: attributed to the Greek playwright Aeschylus (BCE 467). The full translation is, "*Let the women stay at home and hold their peace.*" This is an explicitly sexist statement putting a *woman's work* in the home and placing them in obedient subservience to men. While these attitudes have been challenged by a century of feminism, sadly this idiom is not unfamiliar and gendered struggles continue in various guises. Gender is a theme to which I will return.

Have nothing in your house that you do not know to be useful, or believe to be beautiful: William Morris' mantra was first delivered in a lecture in 1880[2]. The use of *your house* (rather than home) speaks of ownership and implies an individual's will (rather than a collective endeavour). While it seeks to balance a desire for utilitarianism with aesthetic pleasure, there is also an apparent elitism that hints that the home (and by extension the individual) will be judged by the outside world.

A house is a machine for living in – Une maison est une machine-à-habiter: known more widely by those associated with architecture, Le Corbusier's influential principle was first published in 1923 (Jeanneret, 1923). Perhaps shockingly utilitarian, the home is disavowed of emotion and there is a sense of powerlessness, not of ownership and self-determination. Yet, as I shall later argue this is key to understanding the development of what I shall call the *automated home*.

The property ladder: has been in use since the 1940s (Joint Committee on Housing, 1948, p. 531) and was a matter of popular concern by the 1980s. It reflects the home as something to be owned; an appreciating asset that will shortly be exchanged for a larger more desirable property. There is no emotion here or even utility for being lived in, the home is an investment and nothing more. In Margret Thatcher's first speech as Conservative Party leader in 1975, she declared an agenda of creating a "*property-owning democracy*". When in government she notably enacted the Right to Buy, selling council homes to tenants at reduced rates and preventing councils from replenishing their stock. This fundamentally shifted British attitudes to the home, homeownership and personal debt; the divergence of wages and house prices contributes to our current housing crisis and as I shall later describe the identification of a growing number of people as the *precariat*.

These linguistic memes and others shape the ways in which we talk of home and slowly, in turn, their use reflects our shifting priorities. While they differ considerably, there is some agreement that home is, in one way or another, exceptional and often somewhat static. In the remaining sections of this chapter, I endeavour to show how these attitudes profoundly frame the process by which the new technologies of the Internet have become domesticated and the tensions or struggles that are then exposed in how we idealise home.

[2] To the Birmingham Society of Arts and School of Design, February 19, 1880.

The Domesticated Internet and the Networked Home

I use the term domestication deliberately, both in the domestic sense of belonging to the house and the process by which something wild is domesticated; in its own behaviour and the design and refinement of its descendants. There is a tension here with Chesterton's wildness of domesticity.

Since around the year 2000 we have witnessed enormous growth in the domestic use of the Internet and the home networking to support it. Around 2015 there was then an explosion in the number of devices from light bulbs to thermostats and security cameras that became attached to these networks. These are the so-called Internet of Things that we might hesitatingly suggest constitutes the modern smart home. Regardless, for many people the Internet and computation have become firmly embedded in the fabric of their homes; the Internet has been domesticated. How then has the modern British networked home developed? It starts with the telephone.

The Telephone Begat the Internet

To understand the modern domesticated British Internet, one should first consider the domestication of the telephone – shaped as it was by a series of incremental technical, social and political developments, marked by periods of government ownership and regulation of the telecoms industry – each scaffolding the next.

After almost a century of innovation by the end of the 1970s the telephone was reaching practical ubiquity in UK homes[3]. British Telecom, then the General Post Office (GPO), was a nationalised company and controlled and owned all aspects of the network including the home socket and the telephone itself – or in their terms Customer Premises Equipment (CPE). In readiness for the privatisation of BT in 1984, by 1981 the Thatcher government was moving to open up competition in the telecoms market. A critical part of this was to break BT's monopoly of CPE. A new wall connector (BS 6312) was standardised by the British Standards Institution with new equipment being approved by the independent British Approvals Board for Telecommunications (BABT) which opened a new market for home telephones.

In my childhood home change was relatively slow; our rotary phone and old socket remained on the wall in the draughty hall (as it typically did) until the late 1980s; here you stood uncomfortably to make calls, ever conscious of the time and

[3] https://www.statista.com/statistics/289158/telephone-presence-in-households-in-the-uk/

consequent cost. Over the next decade or so the telephone made its way by means of new extension cables from the periphery into the heart of the house, entering the living room and beyond – new wireless handsets giving the ultimate flexibility. British landlines were used almost exclusively for voice services. Meanwhile, as I discovered on my school exchange trip in 1991, Minitel terminals for domestic data services were already in widespread use in French homes.

By the time I became a teenaged apprentice at BT Labs in 1993, the standardisation of the socket was allowing a range of devices to be connected directly to the network, including fax machines, modems and, on occasions, videophones. While business customers had new digital lines installed at their premises, most households maintained the same wiring to the home as they had for the previous 30 years – designed exclusively for voice calls. By the mid-1990s the first Internet Service Providers (ISP) had appreciable numbers of home customers in the UK. Surfers of the World Wide Web were typically using a modem tethered to a single desktop computer via a short serial cable; the placement of the phone socket then dictated the placement of the PC. The modem co-opted the existing voice infrastructure, blocking the line for other callers and was charged by the minute. A fast modem in the late 1990s had a transfer speed of 56 kilobits per second.

In the earlier years of this century providers in the UK began to offer broadband services over ADSL (Asymmetric Digital Subscriber Line), a technology that again reused the existing copper wire phone network and the wall socket, but significantly allowed the telephone to be operated in parallel and a new subscription charging model to be introduced. BT Broadband was first available in 2002 and twenty years later, while fibre-optic connectivity directly into the home allows faster speeds, ADSL is still used by a significant number of people on decades-old copper networks. The first ADSL routers offered wired networking to multiple devices over Ethernet cabling, which enthusiasts wound around their homes. Adoption was fast and by the end of 2006 half of all adults in the UK lived in households with broadband, having an estimated average (download) speed of 3.8 megabits per second (Ofcom, 2007).

The asymmetry of transfer speeds in ADSL is worthy of note; the network is configured with the assumption that the home will consume more than it produces. This seems in direct contradiction to the egalitarian philosophy of the World Wide Web, whereby peers exchange and share information freely. The adoption of ADSL changed the logic of the Internet to support power structured around centralised capital.

The Networked Home

Arguably the most significant development of the present-day networked home was that of WiFi which was standardised for consumer use in 1997 (IEEE 802.11) and increasingly adopted from around 2003 (Anderson, 2003). Finally, the network could break away from the telephone wall socket into every room of the house and beyond, leaking into gardens, the street and neighbouring homes.

While at the turn of the century Internet access was predominantly via immobile desktop computers, with the adoption of wireless networking there was a growth of mobile devices: laptops, tablets and smartphones. The predominance of WiFi separated the provision of the service from the physical fabric of the home; cables no longer needed to be routed through walls and around skirting boards. The Internet could be brought into the home with a small (relatively inexpensive) router that made a single connection to the wall.

Today a typical home network might consists of a router connected to broadband services that creates a WiFi short-range hotspot and provides wired networking sockets. Each networked device in the home is connected through the router to request and receive data from the Internet. Individual devices may address each other across the local network by IP address (typically in the range 192.168.0.0 – 192.168.255.255, reserved for private networking), but from the outside everything on the inside is addressed through the router and mechanism called NAT (Network Address Translation). The NAT's task is to maintain a translation of local and global IP addresses and intermediate between the two. This affords some privacy and security, where firewalls can enforce access rules; partially hiding the home network from the outside world. Further, the short range of WiFi or the physical connection of a wired network confines the visibility of a home network geographically, but often somewhat beyond the walls of the home. This gives us reason to think of home networks as largely private spaces.

Alternative configurations are to be found for the home network and may in time gain popularity. In serviced apartments, including student halls, Internet access might be centrally managed and WiFi routers integrated into the fabric of the building (especially in new builds). This enables policies to be enforced at the point of the router, perhaps limiting access to some websites or some kinds of data traffic. It is also typical that these networks will not distinguish between apartments – there is no logical boundary between your connected electronic stuff and everyone else's. Similarly, with the growing use of metropolitan-scale data networks (such as LoRaWAN and 5G), there is no locally managed point of connect and all devices connect directly to the network. Before the widespread adoption of WiFi, manufacturers have before turned to mobile data networks to provide the wireless connectivity for their products. For instance, in 2002, the Ambient Orb by Ambient Devices (an MIT Media Lab spin-off) showed weather, stock market activity, sports scores and energy pricing by associating them with abstract colours, using the mobile pager network to deliver the data (Feder, 2003). If such metropolitan data networks continue to be adopted, without the intermediating home router, the home network as we have come to know it will cease to be.

Imaginations of the Domestic Internet

Having given an account of the physical accommodation of the domestic Internet, let us switch focus to our imagination of it, what desires we project on it and what demands it makes of us.

The priorities of the Internet have changed since the first identifiable connections of the ARPAnet in 1969. Then a US military project with a concern for resilient connectivity, its adoption spread through international academic collaboration, finally being adopted by business and finance. Since the early days there has been a liberal idealism – as the Whole Earth Catalogue publisher and The WELL co-founder Stewart Brand said in 1984, "*information wants to be free*" (Brand, 1985)[4], a priority that is also present in Tim Berners-Lee's proposal for the World Wide Web in 1989 (Berners-Lee, 1989). Similarly, countercultural groups like the Cyberpunks were influential in shaping a popular conception of the Internet as a parallel cyberspace unencumbered by law and populated by anonymous users. Yet the adoption of secure protocols (and their associated authentication) enabled monitory transactions, that were predicated on identity disclosure. This enabled companies to gradually turn their businesses to the Internet, first internally adopting email and then outwardly via the Web as a means of advertising and sales; witness the extraordinary growth of Amazon.com since 1995. In this process the Internet struggled to be both an idealistic liberal space and a complex marketplace.

By the start of the century, our rationale for being online was as workers and consumers, the days of the ludic Internet surfer were already in decline. This was the Internet that we brought into our homes. Yet its contradictions were not fully resolved, and 20 years of domestication have further complicated it. With emergence of the so-called Web 2.0 (O'Reilly, 2005) the Internet took a decisive social turn around 2005. A new generation of websites including Facebook (2004), Flickr (2004), YouTube (2005) and Twitter (2006), were socially oriented and multimedia-rich. As the capacity of broadband networks grew, services like Netflix could stream high-definition content and

[4] While these are Brand's words, they have lost some important context in this popular quote. Chapter Four will situate it properly.

launched in 2007 in the USA, then in 2012 across Europe. The BBC iPlayer started in 2008 and other streaming services followed. With high-quality video delivery, the intimate pleasures of (legal) pornographic content remain a contentious factor in narratives of the domestication of the Internet (Tim Harford, 2019). Less in doubt, during this period online gaming finally reached a level of mass adoption; the hugely popular Microsoft's Xbox 360 (2005), Sony's PlayStation 3 (2006) and Nintendo's Wii (2006) and all made considerable demands of the network. By perhaps 2008, the Internet had become (somewhat) domesticated.

In parallel with the Internet, as it is commonly understood, are the so-called *deep* and *dark webs*. The deep web refers to the parts of the World Wide Web that are not indexed and made searchable by search engines such as Google and as a result, are difficult to reach. Interestingly, IoT devices and apps will likely call on resources in such corners of the web that are otherwise inaccessible by obscurity. The dark web is a relatively small part of the deep web which is designed to resist the tracking and accountability of the public WWW, using protocols such as TOR (The Onion Router) to maintain anonymity. Access to TOR requires some specific software and know-how. It has a popular reputation for illegal and harmful content, such as the Silk Road site for drug dealing. Yet these technologies do retain some of the web's countercultural roots.

By 2015, there was a growing category of popular Internet connected products for the home, including Nest Labs' Nest Learning Thermostat (2011), Philips' Hue lights (2012) and Amazon's Echo voice assistant (2014) – as well as a new generation of Internet connected flat-screen televisions. What marks these connected products out is an ability to change their behaviour in response to resources drawn from across the Internet. Further, this behaviour, codified in the device's firmware, is also subject to change through over-the-air updates. Frequently these updates are automatic and mandated by the manufacturer; changing the product in potentially profound ways without the owner's say so.

The popular Twitter account internetofshit[5] has documented some of the category's more unlikely objects that have found themselves on the network – many doomed to financial failure; notably the long-predicted smart fridge. LG launched their Internet Digital DIOS model in 2000 to a muted reception, since then manufacturers such as Electrolux, Samsung and Whirlpool have tried, and so far, failed to find customers for this product. Many Internet connected products have failed to become domesticated. Tobias Revell's Former Internet of Things[6] documents a growing list of products

[5] https://twitter.com/internetofshit

[6] https://formerinternetofthings.tumblr.com

that while meeting some initial consumer success, failed to sustain the long-term revenues needed to maintain them; examples include Nabaztag (2006), Little Printer (2012) and Jibo (2017). Other older products have been rendered obsolete when their Internet services are withdrawn or software updates are no longer available.

Connected devices are then defined by a network of resources that necessarily shift and change with the world. To understand this precarious reality of domestic electronic stuff is then to imagine the so-called *Cloud* and describe its nature. As James Bridle suggests, "*Today the cloud is the central metaphor of the internet: a global system of great power and energy that nevertheless retains the aura of something numinous, almost impossible to grasp. We work in it; we store and retrieve stuff from it; it is something we experience all the time without really understanding what it is.*" (Bridle, 2018, p. 7). This network thinking fundamentally complicates our concept of ownership and pulls into question the politics and priorities of the domesticated Internet.

Regulating the Domestic Internet

In recent years the Internet and by extension the domestic Internet has been subject to regulation, let us briefly consider some of this key legislation. In UK law there is a distinction drawn between *cyber-dependent* and *cyber-enabled* crimes[7] and as the domesticated Internet has become commonplace, these now increasingly apply at home. Cyber-dependent crimes include illicit intrusions by hacking and the disruption of computer functionality (for instance through a denial-of-service attack); these are typically covered by the Computer Misuse Act (CMA) of 1990[8]. Interestingly this legislation allows the court to interpret a contemporary definition of computer, an ambiguity that has made it rather resilient and able to negotiate the expansive use of computers since. Cyber-enabled crimes are those not dependent on computing but transformed by it, such as fraud, intellectual property crime or sexual offences. These tend to be covered by more general legislation. Yet, the regulation of seemingly private behaviour on a public Internet highlights tension with ideals of the home as one's dominion – the castle doctrine.

The cyber-enabled intellectual property crime of copyright violation, by the free sharing of duplicated music and films files, certainly contributed to the early adoption of the domesticated Internet. Through the distribution of tools and data protocols, audio CDs and latterly DVDs could be easily ripped (Patrizio, 1999) and shared online. Services like Napster (1999) and The Pirate Bay (2003) facilitated this through peer-to-peer sharing

[7] https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

[8] The CMA was brought into law after there was unauthorised access to the Duke of Edinburgh's private Prestel electronic-mail account in 1984.

protocols, such as BitTorrent. Illegally copied music and video were in widespread circulation, but few successful prosecutions were brought. While the sharing of copyrighted material continues today (2022), the ease by which vast catalogues of music and films are accessed at a relatively low price through well-designed services, removes many of the incentives. Services such as Spotify (2006) and Netflix (since 2010) typically deliver real-time streamed content, that is hard to rip and share.

Since the early days of the Internet, there have been concerns about the criminal and harmful content that is distributed online and consumed increasingly from behind the locked doors of homes. The early Internet Service Providers successfully argued that they were not liable for the content they provided, regardless of its legality. Through legislation such as Section 230 of the Communications Decency Act (CDA) of 1996[9] in the USA, it became established that an ISP was not to be treated as publishers of content, but rather as intermediaries, with liability resting solely with the originating author.

While democratic nations have largely adopted these rather liberal controls of the Internet in the name of freedom of speech, groups have formed in response to curb the worst excesses. The Internet Watch Foundation (IWF) is a British charity that was founded in 1996 with a mission to, "*minimise the availability of online sexual abuse content*"[10]. The IWF maintain a daily updated URL list of over a million websites that it judges to distribute harmful content which it provides internationally to ISPs to block access at a network level and to search engines to filter these pages from their index and so results. Operating without oversight, the IWF is a controversial organisation, which has on occasion been accused of censorship (Davies, 2007).

However, as of April 2022, the UK government is seeking to regulate content publishers on the Internet. In response to the 2019 Online Harms White Paper[11] the government is consulting on plans to expand Ofcom's (The Office of Communications) remit to require publishers (including Facebook and Google) to protect their users from "*harmful and illegal content*", with the sanction of fines or prison sentences for executives of companies who do not (Hern and Waterson, 2020).

As the networked home continues to become every day, it can be expected that the laws regulating the domestic Internet increasingly apply to the Internet of Things and human behaviours mediated through them. This is likely to further highlight struggles as we negotiate how the state can reach into private homes.

[9] https://www.eff.org/issues/cda230

[10] https://www.iwf.org.uk/

[11] https://www.gov.uk/government/consultations/online-harms-white-paper

The Home as a Site of Struggle

While our ideal of home may be that of stability and harmony, in reality it can be the site of significant struggle and change. Struggle is meant here to reflect Mouffe's conception of agonism (Mouffe, 2000); that there is no resolved state, that "*no victory is final*", and that each liberty has to be constantly contested. Here I will briefly enumerate some of these apparent ongoing struggles in the home and suggest how they respond to or are exacerbated by the Internet. I suggest seven types of domestic struggle: domestication, precarity, independence, living with others, productivity, with the market and centrally for privacy. This section now briefly summarises these apparent struggles and Chapter Two will unpack each of these to demonstrate the complexities of the modern networked home. Struggle will be a recurring theme in this thesis, as will ways of struggling through design.

Domestication can be framed as a struggle to integrate the old and the new, how the home responds to changes from within and from external worldly influences. As the previous discussion of the adoption of the Internet shows, this can be a slow process that integrates multiple interests and influences. Whilst this thesis is concerned with the adoption of new technologies and specifically the Internet, domestication is clearly a broader concern.

Precarity (Standing, 2014) describes a range of concerns with the stability of homelife, following from precarious employment and income. With short-term tenancies in the private rental market, many ideals of home are challenged. As landlords turn to remote network surveillance and intervention, tenants increasingly struggle for their liberty.

Independence at home is highly valued, especially for those in older age or when living with a disability when it might become a struggle to stay in one's own homes, surrounded by what is comforting and familiar. Home automation has long promised the support to live independently and now with the networked home these assistive technologies make claims to deliver new kinds of remote telecare; yet with higher degrees of automation and at what price?

Living with others presents perhaps the most complex domestic struggles; be that in family groups or between housemates – as power dynamics are expressed and shared resources contested. Gender is the basis for long-standing struggles inside the home, especially for women asserting an alternative to housewifery. This extends to the gendered use of rooms and domestic technologies – including now those implicated by the networked home. These struggles also include the ways the household lives with the community, perhaps being bound together in practices and beliefs that differentiate them from the outside world, in ways that need to be negotiated.

Demands to be productive at home struggle with traditional conceptions of the home, defined by the absence of work and leisure time, especially in an era of remote working. Yet this has always been complicated in working-class homes and especially so for women, with traditional implications of childcare and housework. The progressive promise of automation, that we might all be released from toils and enjoy idleness and leisure at home, is still unmet by the networked home and the Internet has instead enabled new kinds of (often unseen) labour.

The market has long been a feature of homelife through advertisements in newspapers, magazines, radio, television and latterly online; the domesticated Internet, coupled with instantaneous electronic payments, brings participation in the market directly into the home. However, it is not always clear what fair exchange is being made, especially where the product appears to be free. Shoshana Zuboff's Surveillance Capitalism (Zuboff, 2019) offers a way of understanding the bewildering domestic activities of the largest Silicon Valley dot-com companies; concluding that they are attempting to predict and manipulate the (monetisable) needs of individuals through ever richer surveillance data. If Zuboff's analysis is correct, Surveillance Capitalism represents an urgent struggle for free will, liberty and the sanctity of the home.

This desire to live in a self-determining way in a private home is present in many of the popular idealisations of home and the preceding struggles that I have described – in many ways it is the overarching concern of this thesis. Most broadly, this is a struggle to live together in community groups, where an individual's liberty might be seen to be threatened by, or threaten, a wider society. In the networked home, this is played out through interactions with government, corporations, and the negotiated gaze of neighbours. This is the domain of the surveillance state, Surveillance Capitalism and hackers with criminal intentions.

This section has briefly enumerated some of the apparent ongoing ways the networked home is in struggle with some commonly held ideals of home. The purpose of this is twofold: to quickly establish the dynamic contested nature of homelife and to motivate alternative designs for the network home that participate in these struggles. These same struggles will be individually unpacked in some detail in Chapter Two and contextualised with a breadth of sources.

Ways of Struggle for a Network of One's Own

Virginia Woolf's seminal feminist text, *A Room of One's Own,* inspires a response to the struggle for a private homelife in the networked home, a network of one's own, that will frame my design research inquiry in this thesis (Woolf, 1929). For Woolf privacy is not an abstract notion, but one that suggests there are creative and fulfilling ways for homelife to unfold when one has these liberties – specifically for women's literature. "*Even allowing a generous margin for symbolism, that five hundred a year stands for the power to contemplate, that a lock on the door means the power to think for oneself*" (Woolf, 1929, p. 89)[12]. My design research inquiry is in part an exploration of the possibilities that are afforded when one has a private home network, it seeks to find practical ways to design alternatives that struggle with the corporate logics of Silicon Valley and with Surveillance Capitalism in particular. This demands some unusual methods and outcomes.

A condition of struggling with a system is to first reveal it – a point I shall make at length in reference to DiSalvo's Adversarial Design (DiSalvo, 2012) in Chapter Four. The Gizmodo article *The House That Spied on Me* (Hill and Mattu, 2018) offers a way to accomplish this for the networked home. Journalist Kashmir Hill describes how she had converted her one-bedroom apartment in San Francisco into a Smart Home – "*I connected as many of my appliances and belongings as I could to the internet: an Amazon Echo, my lights, my coffee maker, my baby monitor, my kid's toys, my vacuum, my TV, my toothbrush, a photo frame, a sex toy, and even my bed.*" Her colleague, Surya Mattu, then built a Raspberry Pi based router through which all these devices would connect to the Internet and which would log each and every connection. Through a careful journalistic analysis of this log, the (often puzzling) activity of the connected devices at all hours of the day begins to be legible. Such an intervention with the router is made possible (and widely applicable) because of this common home network configuration, which arises from its domestication via the telephone network previously described.

Once revealed there are technical ways one can respond to assert a network of one's own. Following a series of stories in which Airbnb guests had found themselves covertly filmed by their hosts, artist Julien Oliver distributed a script (*dropkick.sh*) which when run on the guest's laptop identifies and removes cameras on the local WiFi network using a well-known WiFi exploit (Oliver, 2015). Oliver's script embeds deep

[12] £500 in 1929, is equivalent to around £75,000 in 2020.

understandings of domestic WiFi networks, their operation and their vulnerabilities. Oliver describes his practice as Critical Engineering (Oliver, Savičić and Vasiliev, 2011) and his body of work frequently engages with networking technologies and produces open-sourced forms of knowledge – the work of the Critical Engineers represents an important model of potential struggle. These methods require close technical work and specifically an appropriation of techniques and tools from the security and hacking domains; but this is a world of command-line interfaces and super nerds with which most designers are unfamiliar.

Finally, to offer an overview of this thesis and to be explicit about its contributions:

- Chapter Two will next demonstrate that simple and static ideals of homelife overlook it inherent complexity. The chapter catalogues and elaborates the seven (predominantly social) struggles introduced here.
- Chapters Three and Four consider how one can respond methodologically to such techno-social complexity through design and in doing so create diverse alternative proposals for the networked home. Chapter Three is split into two parts, the first describes ways work is overlooked in the home, whether that be the work of people or machines. It applies the feminist conception of Invisible Work (Daniels, 1987) to argues that domestic technologies typically (and historically) emphasise invisibility, seeming ubiquity and automation; and in doing so the home can obscure its exploitation of people and resources. In response, the second part suggests ways to design alternatives that might reveal the struggles of the networked home, challenge its uncomplicated narratives, and make the work on which the home relies more apparent. This chapter draws together a breadth of scholarly and popular sources to give a rich account of the domestication of new technologies, their social implications, and ways to seek alternative paths. Chapter Four recognises the inherent technical complexity of the networked home and contributes a new method of *designerly hacking* as a means by which previously invisible technical possibility can be revealed and designed with, as part of Research Through Design practice-led inquiry. This is grounded in a description of the practices of hacking over the past fifty years and more.
- Chapters Five and Six then describe two design research practice-led complementary empirical studies, that apply these methods and that together make an account of the technical possibility and social reality of the networked home. Chapter Five is an autobiographical study of my own home and network, including a series of workshops in which participants were invited to *hack*

my house – this chapter documents some of the many designs that resulted. Chapter Six describes the Networked Home Study, an engagement with six rented households through cultural probe activities and three bespoke WiFi measurement instruments; it contributes a scholarly contemporary account of the domesticated Internet – specifically of home WiFi networks.

- Chapters Seven and Eight contribute two complementary ways to understand and design alternative networked homes that draw on the learnings from the studies and scholarship. Chapter Seven contributes *The Stuff of Home*, a new theory-led model through which to understand the domestication of the Internet and its relationship with infrastructure, and which responds to Stewart Brand's Shearing Layer model (Brand, 1995). Chapter Eight then articulates 30 design patterns for a *network of one's own* that contribute both a starting point for design that emphasises the visibility of work and a re-examination of Christopher Alexander's notion of a pattern language (Alexander *et al.*, 1977).
- Chapter Nine concludes with some reflection on these contributions and the journey by which they have been made.

Chapter Two: Home Struggles

This chapter catalogues and elaborates of the seven types of domestic struggle that I identified in Chapter One. Namely: the domestication of new, economic precarity, living in independence and with others, the demands of productivity, interactions with the market and living in private. Through these accounts, this chapter attempts to offer a broad contemporary picture of the ways in which home life is neither simple nor static. Many of these struggles suggest ways the networked home is incompatible with common ideals of home and how liberties are then perturbed. By framing these as struggles, using Mouffe's conception of agonism (Mouffe, 2000), I suggest that these can be challenged and that there are ways we might struggle with them through intervention and design. This thesis is intended to demonstrate ways to a struggle for a network of one's own; that the domestication of the Internet to come is neither inevitable, singular, nor permanent. There is a political motivation for this work and it is right that I acknowledge my own positionality and tell my own story as this proceeds. This chapter now considers each struggle in turn.

Struggles to Domesticate the New

In the previous chapter, I gave an account of the domestication of the Internet in Britain. In this section I will frame the domestication of new technologies more broadly as a struggle to integrate the old and the new, critically making the future contestable. To this, I shall bring some autobiography, a discussion of alternative futures and two theoretical accounts of the process of domestication. Through this, I will start to develop a vocabulary for talking about domestication and the pace of change in general that will later serve this inquiry.

At the time of my birth in 1977, we lived at 26 Clarkebourne Drive, Grays, Essex – a three-bedroom semi-detached house built in 1959. This was my parents' first home which they bought in 1970 for £4,900. The house had metered electricity and a gas supply, but no telephone line until perhaps 1974. Before 1976, only the living room was heated with a gas fire, after which gas central heating was installed. A television was purchased in 1979, a colour set with an aerial on the roof, able to receive the three terrestrial channels. Half a mile away my grandma lived at 40 Rosedale Road, a terraced house that she had rented since the early 1930s and where my father and his two brothers had been raised. The house had always had a gas supply and had been electrically lit since 1948. Grandma had a single electrical socket, into which was plugged the black and white television she had rented since the 1960s . From the late 1970s she also had a telephone, no doubt with the assistance of my uncle in the GPO. However, until her death in 1982 there was no bathroom or hot water and the only toilet was at the end of the garden. These were our realities of two contrasting homes in the late 1970s, scenes that would not be unfamiliar to many working people at the time. Yet our ad hoc modernity resisted the popular narrative of fast, relentless linear progress, towards an approaching definitive homogeneous future.

It is obvious that new domestic technologies at once make a promise of better times to come, but in doing so threaten ideals of domestic permanence and stability. Compelling narratives are needed to drive these futures and as I shall show in Chapter Three, these stories are sophisticated, using a variety of popular cultural forms from film to corporate promotion. However, it is evident that simplistic narrow futures can prevent us from facing present difficult realities; for instance, of energy use and related climate change. With this thesis' focus on struggle, the future (and present) can become contestable, open to possibility and perspective.

Alternative Futures

Through the work of Dunne and Raby (Dunne and Raby, 2013), Candy (Candy, 2010) and others, designers and design schools have begun to nuance the ways they approach futures – to acknowledge alternatives and to challenge the monopolies of linear thinking. Forms like Hancock and Bezold's possible and preferable futures cone diagram (Hancock and Bezold, 1994) have been widely and productively appropriated by this community (see Figure 1). The cone describes a diverging set of futures that become increasingly uncertain and contestable; creating a partitioned Venn space for possible, plausible, probable and preferable futures to be reconfigured and refined. The diagram makes the singularity of the present evident and so questionable[13].

[13] As Voros explains (Voros, 2017) Hancock and Bezold (Hancock and Bezold, 1994) were in turn following a tradition of such diagrams and taxonomies of the future, that include Taylor (Taylor, 1990) and Henchey (Henchey, 1978). These cones have an enduring form.

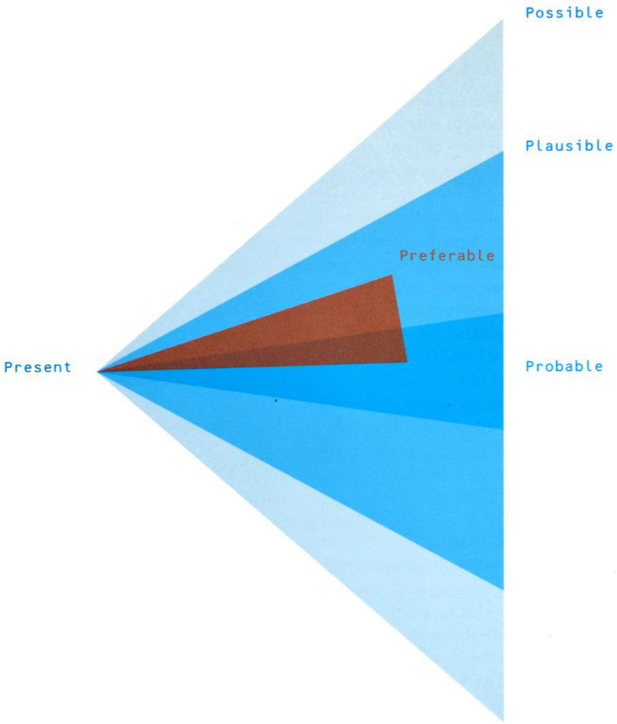


Figure 1. Futures Cone. © Dunne and Raby, 2013. Used with permission.

This acknowledgement of alternative futures then complicates present, future and past accounts of domesticated technologies – and frames domestication as a struggle of competing alternatives, not as the inevitable outcome of corporate visioning or scientific progress. Accounts of domestication should retain this breadth of wild possibilities.

Domestication Theory

Roger Silverstone's Domestication Theory of technology (Silverstone, 1992) has been influential in sociology. The Science and Technology Studies (STS) scholar offers a four-stage model which Haddon summarises as: *"'appropriation' captured the types of negotiations and considerations that led to the acquisition of technologies, 'incorporation' referred to how the ICTs were located spatially within the home, 'objectification' drew attention to how their use was scheduled in people's routines and hence time structures, while 'conversion' dealt with how we mobilize these ICTs as part of our identities and how we present ourselves to others, for example, in how we talk about and display these technologies."* (Haddon, 2011, pp. 312–313)

While Silverstone's model offers an account of the domestication of individual technologies, it does not draw particular attention to the home, its architecture and technologies, evolving slowly over time.

The Shearing Layers

Stewart Brand’s Shearing Layers model (Brand, 1995) offers another way to talk about domestication, that explicitly acknowledges that the whole home in is struggle – its layers shearing against each other, resisting fast infrastructural change. In this way, Brand describes how buildings change and learn from their use at different rates. Six layers are identified, six rates of change in a building (not specifically a home): Site, Structure, Skin, Services, Space plan and Stuff (see Figure 2). Each layer moves successively from the outside of the building in; from the site on which the building stands, down to the Stuff within it. Each layer gains pace of change, from tens or hundreds of years to months or days. With each layer change is increasingly mutable with less work. Each shapes the possibilities of the adjacent layers as they shear against each other, as they resist or demand change of each other; e.g. the bright window that restricts the placement of the television . Brand frames this adaptation, through maintenance, as the system learning. A building that fails to learn can become precarious and ultimately fall.

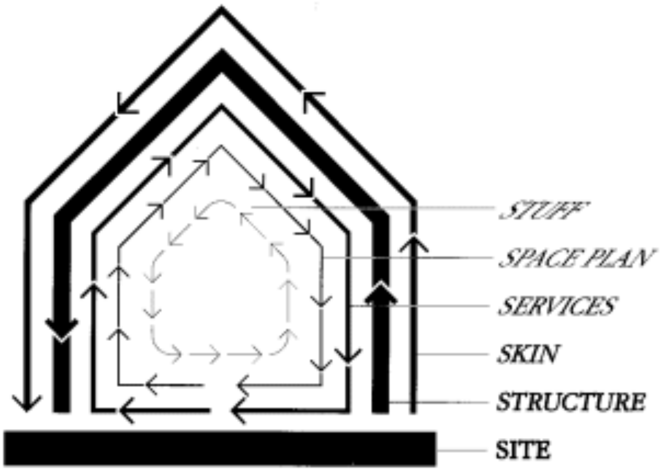


Figure 2. Shearing Layers Diagram. © Stewart Brand, 1995. Used with permission.

Brand’s six Shearing Layers are themselves unpacked from architect Frank Duffy’s (Duffy, 1990) proposal of four layers to account for the change in the interior of commercial buildings in the 1970s: Shell (Site, Structure, Skin), Services, Scenery (Space Plan), and Set (Stuff). Brand describes his layers as follows:

> ***Site*** *- This is the geographical setting, the urban location, and the legally defined lot, whose boundaries and context outlast generations of ephemeral buildings. “Site is eternal,” Duffy agrees.*
>
> ***Structure*** *- The foundation and load-bearing elements are perilous and expensive to change, so people don’t. These are the building. Structural life ranges from 30 to 300 years (but few buildings make it past 60, for other reasons).*
>
> ***Skin*** *- Exterior surfaces now change every 20 years or so, to keep up with fashion or technology, or for wholesale repair. Recent focus on energy costs has led to re-engineered Skins that are air-tight and better-insulated.*
>
> ***Services*** *- These are the working guts of a building: communications wiring, electrical wiring, plumbing, fire sprinkler systems, HVAC (heating, ventilating, and air conditioning), and moving parts like elevators and escalators. They wear out or obsolesce every 7 to 15 years. Many buildings are demolished early if their outdated systems are too deeply embedded to replace easily.*
>
> ***Space Plan*** *- The Interior layout—where walls, ceilings, floors, and doors go. Turbulent commercial space can change every 3 years or so; exceptionally quiet homes might wait 30 years.*
>
> ***Stuff*** *- Chairs, desks, phones, pictures; kitchen appliances, lamps, hairbrushes; all the things that twitch around daily to monthly. Furniture is called mobilia in Italian for good reason.*
>
> *(Brand, 1995, p. 13)*

As this thesis unfolds, I will suggest that the Shearing Layers offers an illuminating account of how new technologies have become domesticated over the past century and where they have failed or fallen short of their promise, often by making simplifications of the complexities of home life.

Importantly, the Shearing Layers also give a human perspective, allowing me to describe the liberties of individuals be they dwellers or other stakeholders (such as landlords or service providers) to make change to the home, with respect to their different kinds of ownership and responsibility. The Shearing Layers shall be an important analytic lens throughout this thesis and in Chapter Seven I shall revisit this critically when I develop the Stuff of Home framework to make accounts of the domesticated Internet. Brand has since proposed the Pace Layers model (Brand, 2018) to describe a durable social society with six layers (from fast to slow): Fashion/ Art, Commerce, Infrastructure, Governance, Culture and Nature (see Figure 3). Unlike the Shearing Layer model, the Pace Layer model does not imply a strong containment relationship between layers. His philosophy is that complex stable systems can often be decomposed into multiple coexisting layers, accommodating different rates of change.

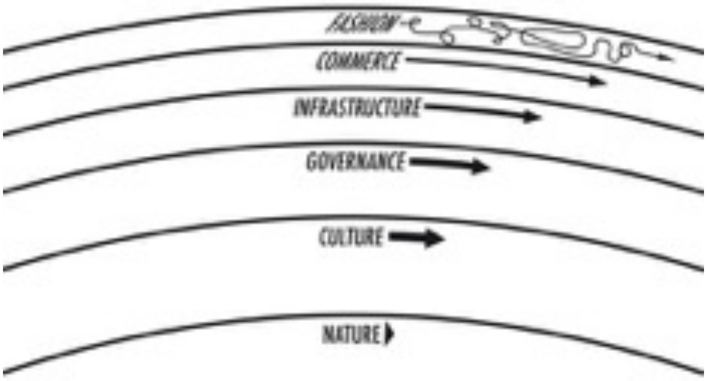


Figure 3. Pace Layers Diagram. © Stewart Brand, 2018. Used with permission.

In their application of Brand's Shearing Layers to Human Computer Interaction (HCI), Rodden and Benford helpfully make the corollary that the "*home is never static*" (Rodden and Benford, 2003). This simple observation runs counter to common intuitions and ideals of the home, but it need not represent an existential threat. With maintenance and with the regulation of change governed by the slower layers, a dynamic stability can be achieved that allows the system to persist over long periods of time.

This section has argued that the process of domestication is often gradual and can be seen in terms of struggle, suggesting Brand's Shearing Layers can be used descriptively for this purpose. In doing some vocabulary for talking about domestication and the pace of change in general has developed, which I shall use frequently as this thesis unfolds.

Struggles with Precarity

In a modern world of economic instability, zero-hour contracts, large-scale migrations, densely populated cities, housing bubbles and environmental crisis, the ideal of a private home in which to seek refuge is unknown or at least constrained; for many people homeownership seems unobtainable. Living with some form of precarity is an ongoing struggle for many in their homes today, including for myself. The Precariat, as described by Standing in his book of the same name (Standing, 2014), are those in short-term (but not necessarily low paid) employment and whose lives consequentially have little certainty or stability. In the context of housing, this is the domain of the private rental market with its short-term tenancies and rental agreements that restrict tenants from making even minor changes to their homes (at least in the UK). This struggle then expresses possible conflicts of interests between the tenant and the landlord, or the tenant and the housing association – newly expressed through the networked home.

Through its enablement of sensing and surveillance technologies, the networked home allows a much finer grain datafication of everyday life than has previously been possible and this has implications for those living in precarity. The Housing Technology's The Internet of Things in Housing report makes this potential clear, "*For housing providers, the main benefits of IoT are access to real-time data about the performance of their housing portfolios and (to a lesser extent) the behaviour of their tenants, reduced costs and better and easier maintenance, while for tenants, the benefits are mainly around better customer service, such as pre-emptive repairs and more accurate maintenance schedules, followed by lower costs, typically based on cheaper energy bills.*" (Tweedie, 2017, p.12). Reporting the words of James Brook, group marketing manager at Rix Petroleum (a large heating oil supplier), Felicity Hannah describes the benefits of smart thermostats, *"[They] give the landlord peace of mind during cold months such as the winter, if the tenant is working away or on holiday, the heating can be activated remotely via the app. This will certainly limit or reduce the chance of frozen or burst pipes caused by cold weather.*" (Hannah, 2017). This narrative is then of benevolent surveillance and remote intervention – allowing landlords to manage their properties (and by extension their tenants' behaviour) in real-time. Yet with this new availability of data and actuation, how might existing tenancy restrictions be enforced and what new demands might be made of the Precariat in their networked homes?

In Desiree Field's Red Pepper magazine article, *Beware the Automated Landlord*, she critiques automated rental payment systems and the surplus data they produce – the datafication of the process. "*Tenants of the automated landlord are effectively (and unwittingly) paying two rents: one consisting of money, the other of information, extracted as they do things like renew their lease or request a leaky tap be fixed.*" She argues that *data harvesting*, "*creates new opportunities for capital accumulation. For example, lists of tenants who occasionally pay rent just a few days late might be sold to a data broker, and ultimately used to target ads for credit cards, [and] payday loans[.]*' (Field, 2017). In this light, the infrastructural Internet of Things can become the focus of struggle between tenants and landlords, with entry systems currently being the most apparent example. Concerned that new smart locks and apps were tracking their activities, residents of a Manhattan apartment building legally challenged their landlord's attempts to replace their physical door keys (Ng, 2019). Residents of a rent-stabilised apartment building in Brooklyn resisted their landlord's attempts to replace a key fob entry system with facial recognition (Misra, 2019). That a tenant can freely come and go from their home, without being observed or harassed seems a fundamental liberty

– in the UK at least, the covenant of *quiet enjoyment*[14] makes this protection for renters.

While some landlords are solely motivated by the accumulation of private wealth, others have more societal objectives. In 2017, Sandjar Kozubaev and Carl DiSalvo worked with Atlanta Housing, the largest public housing agency in the southeast United States, to help them understand the opportunities and issues of smart technologies and services in a new facility (Kozubaev and DiSalvo, 2019). A large, multi-building site was planned with an agenda to address "*placemaking and community building through a focus on sustainability, life-long learning and economic development*". Through a series of participatory design workshops held with residents and building managers, themes of fear and mistrust of smart devices reoccurred; "*When the residents in our workshops were acting on those data, as in the discussions around monitoring family, the utility of these systems was embraced. However, when the data were being acted on by outsiders, even in the name of public safety, our participants had real concerns around the consequences those external judgments and actions would have*" (Kozubaev and DiSalvo, 2019, p. 11). External agendas and individual freedoms do not necessarily align, however seemingly well-intentioned.

The Sensorstation project by Teresa Denefleh and colleagues (Denefleh *et al.*, 2019). was a speculative design project concerned with tenant/landlord sensor data sharing. Working with the residents of a shared apartment they made a design intervention and speculated about proactively sharing humidity sensor readings from the bathroom with their landlord. One tenant argued that this accountability would then be indisputable and transform domestic contention. Other housemates had privacy concerns and they debated the landlord's right to know what was occurring in *his house*, and yet this seems to run counter to a tenant's right to *quiet enjoyment*. The authors speculate that, *"There is an opportunity to design 'Smart Home' systems that allow [one] to configure spaces within shared apartments that reflect personal spaces like physical places do.*" (Denefleh *et al.*, 2019, p. 691).

Beyond struggles with landlords or housing associations, many precarious workers must also work from home as they have no physical place of work – reliant on access to the Internet for their livelihoods. This is especially so for a growing number of freelancers and businesses that are entirely virtual without any shared office. This is later described more fully as a struggle to be productive.

[14] The covenant of quiet enjoyment is legalise commonly found in letting agreements (including my own) giving the tenant the right to live in the property in peace, without undue disturbance from the landlord or their agents.

Finally, fixed-term contracts for services can be difficult for those living precariously. Contracts for broadband in the UK might typically require a minimum period of 12 or 18 months, which if broken would result in considerable penalty charges. As a result, in low-income areas, the uptake of broadband contracts can be very low[15]. One strategy adopted is to create WiFi hotspots on smartphones to share connectivity with local devices.

A struggle with precarity includes people who might not be typically thought of as disadvantaged or poor. While living in private rented accommodation might be relatively stable it is often coupled with precarious employment. As I have argued in this section, precarity restricts one's liberty to control the interior space of the home and this can be further exacerbated by the network.

Struggles to be Independent

Many people struggle to live independently in their own homes, as their environments render them disabled through their physical and cognitive predicaments. For some these are lifelong conditions, perhaps blindness; but for many this will be straightforwardly older age when familiar surroundings may be both of greatest comfort and become challenging. Many people will feel pressure or acknowledge the necessity to move into some form of sheltered housing – where there can be some centralisation of care. Yet that provision can be scarce, labour intense and as a result expensive. It is widely acknowledged that there is an international social care funding crisis (Butler, 2019) with an ageing generation of post-war baby boomers making the situation urgent. In some significant ways the domesticated Internet and assistive technologies can facilitate independence, relieving some of the pressure on the social care sector and yet they also complicate the liberties of individuals. This section describes some of these networked technologies and the struggle to be independent in your own home.

Since the 1970s commercial emergency alert systems have been available for elders to request remote assistance. These are typically wireless body-worn emergency buttons, perhaps on a pendant or wristband, that have connectivity via a landline telephone or latterly a mobile cellular network to a call-centre agent, with whom the elder person can speak. Wilhelm Hormann's Hausnotruf (home alert) is acknowledged as the first of these Personal Emergency Response Systems (PERS) being developed in the 1970s (Greene, Thapliyal and Carpenter, 2016). By the late 1980s these systems, such as with LifeCall in the USA, had significant commercial success.

[15] This became apparent in conversations with Byker Community Trust, who manage the iconic Byker Wall social housing estate in Newcastle upon Tyne.

Over time PERS developed to incorporate features of what became known as telecare, incorporating a range of sensors to monitor the individual and the home. Common modern telecare sensors include: movement and fall detectors; door, bed and chair sensors; worn GPS tracking devices; epileptic seizure alarms; incontinence sensors; medication dispensers and reminders; heat and temperature sensors; and flood, smoke and gas detectors (Which, 2020). These sensors then rely on some interpretation by a remote observer to determine whether an incident has occurred, rather than the explicit call for help by a button press; that observer may be a person or maybe an algorithm. As I shall describe in Chapter Three, these contextual reasoning systems are examples of surveillant Ubiquitous Computing.

The earliest articulations of the *smart home* suggested ways in which technologies may be assistive to the blind and elderly, through sensing and voice interfaces to speak alerts and understand calls for help (Smith, 1988). Georgia Institute of Technology's Aware House (Kidd et al., 1999), aspired to: support social connections, support everyday cognition and identify potential crisis situations and in doing so broaden the scope of ways the home may be supportive, beyond the emergency. This subsequently became an active research area, with work that addressed issues of dementia (Orpwood et al., 2005) and loneliness (Austin et al., 2016), among others. With a smart home focus, these systems survey individuals through an ever-growing range of sensors and then invariably adopt rather simple normative models to automatically reason about behaviour; models that can become restrictive rather than enabling. This is beautifully explored in Superflux's speculative film Uninvited Guest where an elderly man struggles with an array of smart devices sent by his children to monitor his diet, health and sleep from a distance (Superflux, 2015). He perceives these devices as an attack on his liberty and reacts by finding ways to trick each of them into believing that he is compliant.

Some PERS have become mainstream, notably through the fitness industry and devices such as the step-counting Fitbit (2007); which was significantly acquired by Alphabet/Google in 2020. As this device category has developed a range of biometric sensors are now commonplace. The popular Apple Watch combines accelerometery, GPS and heart rate with data connectivity to offer fall detection. If an impact is detected followed by immobility, the watch can automatically contact the emergency services, stating the individual's location.

The struggle to be independent in one's own home is then a tension between being enabled by the systems and technologies of the home, and being subjected to excessive surveillance and normative standards of behaviour.

Struggles to Live with Others

It is tempting to see the home as a whole and cohesive unit, and while single occupancy is increasing and isolation brings its own challenges, most people live in one way or another together with others and this invariably brings its complications. As an illustration, this section considers this struggle from the perspectives of parental authority, keeping house, community living, religious households, domestic abuse and gender dynamics. As homelife is increasingly enacted on the home network, this struggle will also be played out there too.

Parental Authority

As the Internet has become domesticated, the established power dynamics of the home, such as those between the parent and child, have become mirrored on the home network. Consider a mother limiting her daughter's screen time on a tablet computer. These parental controls[16] are now a common feature of networked devices, in which access to particular services, websites and apps are limited, within prescribed hours of the day. This content filter may be situated on the device or on the network. Most Internet Service Providers (ISPs) offer this through a so-called proxy-server sited at their premises, through which all the home's Internet traffic flows and where specific websites can be white or blacklisted, or keywords filtered. Browsing can then be categorised as pornographic, gambling, shopping, social media and so forth. However, many parental controls are weakly secured with a short password or passcode and more elaborate controls can become circumvented. In a networked home traditional structures of parental authority can become destabilised – especially where technical expertise does not rest with the nominal head of the household.

Keeping House

Several studies have examined family life as expressed through the home network and these tend to focus on the tasks of digital housekeeping. Peter Tolmie and colleagues (Tolmie et al., 2007), and Marshini Chetty and colleagues (Chetty, Sung and Grinter, 2007) describe the maintenance and management of the home network, as undertaken by individuals with technical skills, framing these as everyday household chores or as ongoing DIY projects. Those individuals in Chetty's study were dominantly male (Chetty, Sung and Grinter, 2007) and interestingly the gender was deliberately unreported by Tolmie (Tolmie et al., 2007). Struggles of gender are described later.

[16] https://www.nspcc.org.uk/keeping-children-safe/online-safety/parental-controls/

Beyond digital housekeeping, there can be contention with the shared finite resource of network bandwidth. The Home Watcher display (Chetty et al., 2010) lets a household ask, who's hogging the bandwidth? Six households were recruited: three families with teenage children, one married couple and two homes with adult roommates. As well as publicly graphing the data consumption devices, it also allowed anyone with access to the device to limit the bandwidth of others. They concluded that, "*revealing resource usage in the home affects different types of households, by surfacing household politics and enabling new forms of contention.*" (Chetty *et al.*, 2010, p. 668).

As previously described, the Sensorstation project by Teresa Denefleh and colleagues (Denefleh *et al.*, 2019). was a speculative design project concerned with tenant/landlord sensor data sharing, in the context of a shared student apartment. A set of smart sensors (SensorTags) allowed individuals to exercise, "*self-monitoring, control over others, and […] reward systems and penalties*". A tablet computer in the kitchen then allowed them to develop combinations of rules for these sensors, creating some self-defined application, which would typically result in a notification being sent to a smartphone. The sensors were then placed around to home to capture the desired phenomena. Some applications were playful (a SensorTag on the refrigerator door that exalted them to "*enjoy their meal*"), some attempted to nudge the household towards good behaviours (for correct waste separation); all had an unacknowledged absurdity. The authors concluded that, "*Sensorstation severely redrew the boundaries between private and shared rooms*", that data generated in private rooms was broadcast "*to the base station in the kitchen and to personal devices simultaneously*" (Denefleh *et al.*, 2019, p. 690). Further, "*previously acknowledged physical boundaries in the home, such as closed doors that would demarcate private rooms, have been compromised by smart home applications.*" (Denefleh *et al.*, 2019, p. 692). In this sense, the networked home, and especially wireless technology, disrupts the social order that walls nominally construct within the home – the router seeing everything equally without distinction.

Community Living

Beyond an individual residence, small community living enables and presents different struggles. These communities may have been established to promote a particular set of values, perhaps an environmental outlook or a particular religious perspective. The groups provide the supportive structures needed to maintain these practices in face of the external pressures and expectations of the wider society. An example of such a community is the *cohousing* movement, studied by Tom Jenkins in the context of the Internet of Things, (Jenkins, 2017, 2018). Cohousing is a Danish concept of communal living (*bofælesskaber* – living communities), founded in the 1960s that establish living patterns that promote a village-like community.

“*Cohousing is a type of intentional community that is designed to operate like a village. Residents are active in the community as neighbors, live independently in their own homes, and share ownership of a larger “common house” as well as the community’s land.*” (Jenkins, 2018, p. 667)

Jenkins’ work with cohousing communities in the USA describes some of the ways in which the households coordinate their common activities, such as meals or yard work. Three IoT prototypes are presented that were designed in response to the ethnographic study: Cohousing Radio, Physical RSVP and Participation Scales. Each home has a Cohousing Radio allowing members of the community to send audio between devices. Located in the common house, the Physical RSVP device is a bowl into which place electronically readable physical tokens (NFC[17] tagged marbles) publicly demonstrate their intended attendance at an event. Finally, the Participation Scales physically represent an individual household’s level of participation in the community. Each can be seen to perform across particular boundaries of the home, more or less in public – as the individual struggles with and for the community, as the community struggles for its continuing relevance and so survival.

Religious Households

For those of religious faith, the Internet can be a place where blasphemy and prohibited behaviours are seen to be normalised. Like books, films, television and radio have before; the Internet brings the outside world across the domestic threshold and struggles ensue. Over the past twenty years, some small ISPs have offered content filtered Internet access tailored to specific religious groups. *MSTAR.net* was an ISP that spun off from the Church of Jesus Christ of Latter-day Saints in 1998; it advertised with the slogan, “*Your home. Your values. Your Internet. Help maintain LDS values when you use the Internet.*” (Willard, 2002, p. 1). While few such specialised ISPs have survived commercially today, these struggles are no longer limited to religiously conservative homes; the Internet, and especially social media, is increasingly seen as an illiberal space of Twitter trolls and YouTube alt-right influencers (Lewis, 2018).

Some religious communities have rather more direct teachings relating to technology. The Amish reject utility services, such as electricity from the grid, as it brings *worldly influences* (Ems, 2014). Yet this is not necessarily a Luddism; batteries are widely

[17] NFC (Near-Field Communication) is a technology for proximate wireless data exchange, it enables mobile payments for smartphones.

used as they can be resourced locally, especially for lighting, but also for calculators, clocks, cash registers, drills and electric fences. Lindsay Ems describes a series of workarounds that complicates the common account of the Amish and technology, including the use of an *internet-disabled* computer.

A weekly day of rest, or a Sabbath day, is to be found across many major world religions and can also shape the use of technology at home. Orthodox Jewish households might typically observe halacha law on their Sabbath or Shabbat or Shabbos from sundown on Friday, until the appearance of three stars in the sky on Saturday night, prohibiting 39 acts of work or creation. These laws include the writing of words and the extinguishing or lighting of a flame. Orthodox scholars consider electricity and specifically the filament bulb to have the qualities of a flame and so many strictly observant Jews refrain from using electrical devices on Shabbat; use by this interpretation means to directly manipulate. Like the Amish, observant Jews have found workarounds and manufacturers have developed ways of using their devices whilst being compliant.

So-called Shabbat Modes can be found on a range of domestic appliances, from refrigerators that can disable the door light, to light switches that operate by an optical, rather than mechanical, switch. Allison Woodruff, Sally Augustin and Brooke Foucault (Woodruff, Augustin and Foucault, 2007) studied 20 Jewish families who used home automation technologies to enable their Shabbat observance. Some homes used simple timer switches to schedule lights, others were more sophisticated using X10 (a wired automated home networking technology) and others a commercial system[18] developed for Shabbat that enables a sequence of sensor-based rules to play out over the day. This work predated the domestic Internet of Things, but subsequent articles suggest the networked home is being used in similar ways (Rohwedder, 2019). Voice interfaces such as Amazon's Alexa have been generally interpreted favourably, "*It has an LED and not an incandescent bulb. It is voice operated and always on.*" (Eisenberg, 2015).

[18] The paper curiously anonymises the name of the system.

The Shabbat example shows how networked technologies can then orchestrate a household's religious practice or ritual; the Interaction Research Studio's Prayer Companion is another (Gaver et al., 2010). The Prayer Companion is a device designed specifically for an order of Roman Catholic nuns to find international and personal news stories as a resource for their prayers. These Poor Clare nuns take vows of poverty, chastity and obedience, and significantly also of enclosure – like the Amish the threshold of their community with the world is carefully managed. With sensitive design both in terms of appearance and behaviour, the Prayer Companion successfully negotiated this divide and remained part of the nuns' daily rituals for five years.

While rituals can be formalised by religious practice, they can also emerge within households and have rather more secular and quotidian functions. These rituals may do "*the work of being a family*" (Kirk *et al.*, 2016) and through practice demonstrate an in-group membership of the household. The Family Rituals project (to which I contributed) took a ritualistic perspective on the separation from the home when family members work away (ibid.). Through engagements with five such families, the project explored both how rituals might be established remotely around the Internet of Things devices and how these rituals can become a point of reflection and ethnographic inquiry, as a home struggles with separation. Five bespoke machines were designed for each family, sensitised by a cultural probe study. One was a wine dispensing machine connected to an electronic beer bottle opener, allowing a separated couple to share a drink at the end of the day. Another allowed a young boy to find his father, as he travelled around the UK for work, through an illustrated telescope. While these machines did create regular reflective moments, none became truly ritualised in the short study period. Family rituals are evidently difficult to manufacture or commodify.

To live with others in a religious household can then be a complex negotiation of private conviction and world influences, managed at the threshold of the home. With the domesticated Internet, this struggle is ongoing and with the Internet of Things actively asserting itself on the behalf of others, it will likely become more intense.

Domestic Abuse

While many homes are places of nurture and mutual support, others do become dysfunctional or worse abusive and dangerous environments; places where often gendered crimes are perpetrated behind closed doors. With the domestication of the Internet come concerns about the growing prevalence of new forms of network-based abuse; using the domestic Internet of Things to surveil, exercise control over or gaslight victims (Bowles, 2018; Lopez-Neira et al., 2019).

Gaslighting refers to Hamilton's play of the same name from 1938 in which a young woman is driven to disbelieve her own sanity by the deceitful actions of her husband in their Edwardian townhouse. This centres around his construction of her moments of incongruence, when stuff is inexplicably moved or missing. The crimes he attempting to disguise are finally revealed by the dimming of the gaslights – a network effect as the utility service responds to increased demand – he is using a lamp in the house when he is ostensibly absent.

Writing in the New York Times, Nellie Bowles reports a series of abusive incidents enabled by the Internet of Things, "*One woman had turned on her air-conditioner, but said it then switched off without her touching it. Another said the code numbers of the digital lock at her front door changed every day and she could not figure out why. Still another told an abuse help line that she kept hearing the doorbell ring, but no one was there.*" (Bowles, 2018).

The ongoing Gender and Internet of Things project at University College London is seeking to investigate these new forms of networked domestic abuse, in which often technology-savvy males abuse their often-female victims (Lopez-Neira et al., 2019).

Gendered Dynamics

Throughout the 20th Century and now into the 21st, the home has been the site of gender struggles. As I described in the previous section this includes often gendered domestic abuse, here I shall focus on the struggles of women asserting an alternative to housewifery and the gendered home. Over time attitudes to and practices of gendered housework have shifted – at least in most of Europe and Northern America. According to the 2017 British Social Attitudes Survey, 8% of British people agreed with the statement, "*a man's job is to earn money, a woman's job is to look after the home and family.*" – whereas in 1984 that stood at 43%. Yet there is still gendering of the home and housework, even today.

As prosperity grew in the 1950s and 60s, explicit gendered expectations of homemaking and homemakers motivated many labour-saving domestic technologies – from electric irons to vacuum cleaners. This is clear from the advertisements of this period, as I shall discuss in Chapter Three. However, Ruth Schwartz Cowan's critique of 20th Century domestic technologies, More Work for Mother (Schwartz Cowan, 1983), concluded that instead of reducing housework, these innovations instead made it more solitary and time-consuming, as ever-higher standards of outcome were expected. In the case of the vacuum cleaner, it had even regendered floor cleaning from a male to a female task.

As the conception of the *smart home* developed through the 1980s (Smith, 1988) there was arguably a shift away from labour-saving technologies, towards domestic control systems and services – heating, lighting and alarms – a priority still present in today's domestic IoT products. Writing in 1995, Anne-Jorunn Berg examines the gendered socio-technical construction of the smart home, as it was emerging in early scenarios and prototypes. Berg states that, "*It is a widely held popular belief that new technologies in the home have rationalized housework so that it is no longer an important source of inequality between the sexes.*" (Berg, 1995, p. 74). She argues that this is an ignorance of housework, perpetrated by male designers and producers. "*They have ignored the fact that the home is a place of work (women's housework) and overlook women, whose domain they are in effect transforming, as a target consumer group.*" (Berg, 1995, p. 85). It is argued then that the smart home is itself a gendered construction.

Beyond the activity of housework, the landscape of the home is also gendered, with perhaps the kitchen being the most apparent site of gendered work. However, as Cynthia Wall points out, rooms are not simply gendered by use or work, but by the power to command the interior space and to bring order to them – predominantly male (Wall, 1993). Wall's argument is constructed from 18th Century literature of high society homes, referencing Daniel Defoe's Roxana (1724), Samuel Richardson's Clarissa (1748) and Jane Austen's Pride and Prejudice (1813). However, this distinction between gendered use and gendered command is still relevant today. As previously described in Chapter One, Virginia Woolf's essay A Room of One's Own directly addresses the control of space and the activities this facilitates – here that the dearth of women's literature was significantly explained by women not having rooms of their own (Woolf, 1929).

With an eye to the future smart home, Bell and Dourish discuss the modern masculinised (and implicitly working class) space of the garden shed, as a "*counter-point to the perceived feminization of the home, and the staging point or proving ground for technologies*" (Bell and Dourish, 2007, p. 4). "*In addition to thinking about how technologies move into and out of the home, then, one must also ask who brings them in, how they arrive, by what mechanisms they are domesticated, and what kinds of power displacements they achieve.*" (ibid, p. 10). In their analysis, the shed exists on the edge of the home and acts as an important gateway through which technologies first become domesticated and then may exit as their usefulness becomes questioned – a gateway controlled by men. The technologies of the home, including the home network, are a predominately male domain.

It is instructive to re-examine Brand's Shearing Layers (Brand, 1995) in light of this analysis of the technologies that constitute the smart home and the gendered command of the interior space. If domestic IoT largely ignores labour-saving technologies, in favour of the infrastructural including the network, then this represents a priority of Services over Stuff. If the work in a room is female through the manipulation of everyday things, but the control of the space is male, then this is a division of male Space Plan and Services, with female Stuff. That being the case the Shearing Layers themselves represent a gendered struggle – where the slower layers of the home are predominantly male, and the faster layers (perhaps only Stuff) are typically female. Brand makes a similar (but ungendered) observation regarding property ownership.

There are further ways in which networked homes are troubled by gender. In a report UNESCO (The United Nations Educational, Scientific and Cultural Organization) identified the rise of gendered AI and its troubling repercussions, citing the default female voices and subservient characters used by Amazon's Alexa, Microsoft's Cortana, Google Assistant and Apple's Siri. (UNESCO, 2019). These themes of gendering machine work and of subservience will be returned to in Chapter Three .

This section has then exposed some of the complexities of living with others, specifically: parental authority, keeping house*,* community living, religious households, domestic abuse and gender dynamics. While this is clearly not an exhaustive treatment, its intention is to demonstrate some of the complexities of the social lives within the home, to act as a counterpoint to the idealised households inhabiting the fantastical smart homes of Chapter Three.

Struggles to be Productive

The prevalence of remote working has created an additional struggle at home to delimit work life – be that the precarious freelancer or salaried corporate worker. For those in small, rented homes, these workplaces are often makeshift and socially isolating. This has been exacerbated by the COVID-19 pandemic lockdown restrictions of 2020 and 2021. Nonetheless, there is a popular discourse on so-called work/life balance – in which we are encouraged to "*Leave work at work*", (Jeffries, 2014). Yet this is only a partial picture and for many, the home and the home network remain necessary sites of labour; domestic productivity is then a necessary concern.

Many traditional conceptions of home define it by the absence of work, yet this has always been complicated in working-class homes and especially so for women, where the work of housework is ignored. Since the time of Bertrand Russell's In Praise of Idleness (Russell, 1935) and later in Hanna-Barbera's The Jetsons (1963), there has been the progressive promise of the automation of housework; that people might be released from their toils and enjoy idleness and leisure time at home, away from their paid (or unpaid) work.

Woodruff, Hooker and Aipperspach's heterogeneous home is a useful design exploration of paid work boundaries that emphasises the home as a restorative environment (Aipperspach, Hooker and Woodruff, 2008). They present a series of design sketches that explores boundary making between home and networked work at different scales and layers that, "*provides choice about boundaries, connection, stimulation, and variation in the home*" (ibid. p. 222; see Figure 4, in which they make the distinction between *house* and *home).* There are parallel concerns here with the Amish's concerns of delimiting worldly influences. Both create a sanctuary from the outside world, but the heterogeneous home acknowledges this as a gradient and transition, rather than as an absolute threshold.

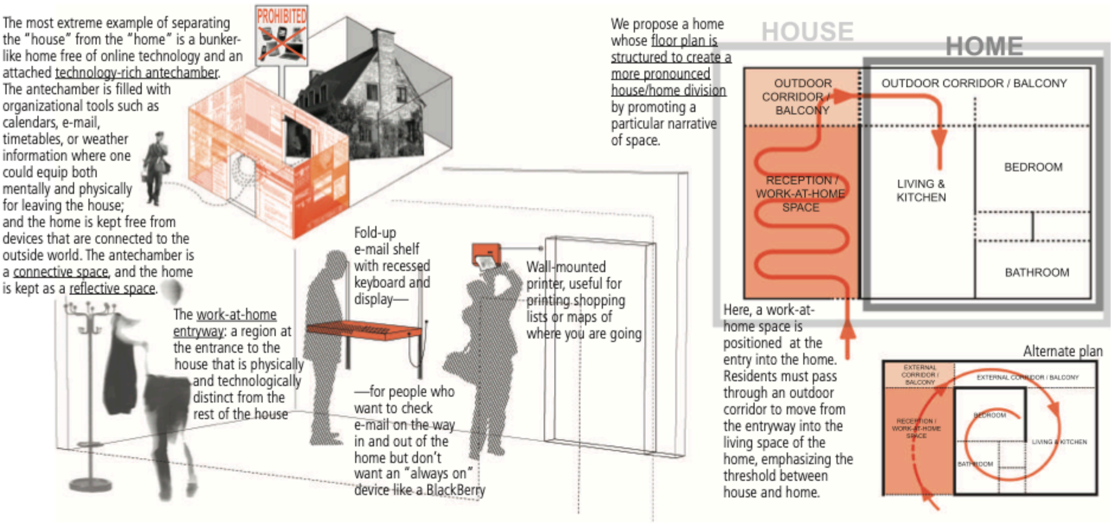

The most extreme example of separating the "house" from the "home" is a bunker-like home free of online technology and an attached technology-rich antechamber. The antechamber is filled with organizational tools such as calendars, e-mail, timetables, or weather information where one could equip both mentally and physically for leaving the house; and the home is kept free from devices that are connected to the outside world. The antechamber is a connective space, and the home is kept as a reflective space.
PROHIBITED
The work-at-home entryway: a region at the entrance to the house that is physically and technologically distinct from the rest of the house
Fold-up e-mail shelf with recessed keyboard and display—
—for people who want to check e-mail on the way in and out of the home but don't want an "always on" device like a BlackBerry
Wall-mounted printer, useful for printing shopping lists or maps of where you are going
We propose a home whose floor plan is structured to create a more pronounced house/home division by promoting a particular narrative of space.
HOUSE
HOME
OUTDOOR CORRIDOR / BALCONY
OUTDOOR CORRIDOR / BALCONY
RECEPTION / WORK-AT-HOME SPACE
LIVING & KITCHEN
BEDROOM
BATHROOM
Here, a work-at-home space is positioned at the entry into the home. Residents must pass through an outdoor corridor to move from the entryway into the living space of the home, emphasizing the threshold between house and home.
Alternate plan
EXTERNAL CORRIDOR / BALCONY
EXTERNAL CORRIDOR / BALCONY
RECEPTION / WORK-AT-HOME SPACE
BEDROOM
LIVING & KITCHEN
BATHROOM

Figure 4. The Heterogeneous Home. © Ben Hooker, 2008. Used with permission.

Set in opposition to the heterogeneous home is naturally the homogeneous home, in which life is defined by the consumption of undifferentiated services. In this light, today's networked homes do start to look a little bland and productivity-focused.

Gaver's ludic design asks us to consider the home as a place of playfulness rather than production. "*As computing has emerged from the office and laboratory, it seems to have brought along values of the workplace: concerns for clarity, efficiency and productivity; a preoccupation with finding solutions to problems."* (Gaver, 2002, p. 2). Ludic design then emphasises curiosity, love of diversion, exploration, invention and wonder.

Alex Taylor and Laurel Swan argue for domestic design that affords artful configurations of work, "*Most importantly, we suggest that technologies must be designed to accommodate the rich and diverse ways in which people organize their homes, providing them with the resources to artfully construct their own systems* *rather than enforcing ones that are removed from their own experiences.*" (Taylor and Swan, 2005). This work is returned to in Chapter Three.

It might be argued that the domesticated Internet has indeed enabled new kinds of leisure. The binge-watched streamed series on auto-play, the all-absorbing online game the infinite scroll of antagonising social media occupy hours of the day. It is distracting by design, tuned to hold attention for as long as possible, as often as possible. Where the boundary between work and leisure is ill-defined this wasted time can cause anxiety. For the precariat, as Standing observes, "*leisure is not the same as time not participating in paid labour.*" (Standing, 2014, p. 219). According to this logic, free time should be spent productively upgrading one's human capital through a range of unpaid work and training; improving the Curriculum Vitae in readiness for the next paying gig. For many, leisure time is then often neither particularly ludic, artful nor restorative.

Finally, for those who have the opportunity to sublet, there is additional pressure to make the home productive – to realise the value of their asset in the *Sharing Economy*. Here home has to perform both as a sanctuary and an Airbnb showhouse, judged in a marketplace of Instagram compositions .

There is then a struggle to create the time and space in the networked home for both productive time and restorative leisure. Like the religious households previously discussed, the management of understood boundaries is one response and a wirelessly networked home suggests ways of managing disconnection. Yet it seems there are ludic, artful or even wild ways to reconfigure these technologies, beyond simply turning them off.

Struggles in the Market

That we might seek a fair price for our labour and in turn be able to make a fair exchange for goods within a market that gives us a wide consumer choice; is a tenet of modern Capitalism. This relies on the operation of the free market to find that fair price and for individual consumers to operate in that market with sufficient (but imperfect) knowledge of it. This is broadly the philosophy of the economist Friedrich von Hayek (1899 – 1992), whose ideas were enthusiastically adopted by the Thatcher government (1979 – 1990) and shaped the British experience of Capitalism over the subsequent decades.

According to Hayek, understanding the distribution of knowledge in a market is critical to understanding how they operate to find an equilibrium of supply and demand, to settle on a stable price for something (von Hayek, 1937). Hayek's contribution was to show that free markets necessarily operate with individuals having imperfect knowledge of others and enacting their independent aims and desires. He argued that individuals can operate selfishly and yet there will be spontaneous order without the requirement for some centralising control, in sharp contrast to the alternative communist model. The economist Adam Smith's (1723 – 1790) Invisible Hand (Smith, 1759), is a related idea in which the operation of the free market implicitly ensures a social good.

This section considers the ways in which the market struggles to enter the home; first by the means of advertising and home shopping, then in an attempt to predict and manipulate the market, through the surveillance of the domestic Internet. In so doing this challenges ideals of the home as a sanctuary from the outside world.

Advertising: you are the product

For over 100 years the commercial world has struggled to gain access to the home, be that through newspapers and magazines, over the airwaves on radio and television, and now via the networked home. Advertisers seek to occupy both time and space in homes – to draw attention and persuade.

Some see adverts as an intrusion, some as an irritation, some as entertainment; or perhaps as a necessary way by which consumers become knowledgeable about the market and the choices open to them. Ad-blockers are widely used for browsing the web, either installed as a browser extension such as Adblock (Sorensen, 2002) or access to known advertising sites are blocked by the router for all machines on the network, e.g. Pi-hole (Salmela, 2014). We have developed ways to struggle with these unwanted advertisers; my father simply mutes adverts on commercial television.

Over the past twenty years, the Internet has grown to support a variety of business models. At first, speculative web services were free and idealistic, then pioneering advertisers attempted to reach new audiences with nascent multimedia experiments, but once electronic transactions could be routinely made, advertising could be integrated fully with purchasing and money started to flow. The new commerce was instantaneous and situated inside the home; the era of Amazon's 1-Click shopping had arrived (Brandt, 2011). Such electronic payment enables numerous purchasing decisions to be taken, be that online shopping or for the consumption of digital services such as films, gambling and gaming – all from within the home.

Today, free services tend to be supported by advertising targeted to the audience and coupled directly to sales – with advertisers seeking this *click-through*. In the networked home adverts have already escaped the web browser and now have begun to inhabit connected electronic Stuff. As I will discuss in Chapter Five, Amazon's Kindle book reader displays an advertisement on its surface even when it is turned off.

There is a common, but vague, understanding expressed of how attention and data are of commercial value, to be fairly traded for services – yet most struggle to articulate this precisely. It seems a mystery how Google can be so profitable when it has so many free services and diverse activities, from search to doorbells to DNS[19] and is almost advert free.

In the UK there has been a familiarity with commercial television and radio, supported by adverts, since the 1950s and 1970s, respectively. This trade between what is apparently free and our attention has long been understood – in 1973 Richard Serra and Carlota Fay Schoolman's short video work *Television Delivers People* was publicly broadcast in the US (Serra and Schoolman, 1973). "*You are the product of T.V.*", it declares, "*You are delivered to the advertiser who is the customer. He consumes you*". Today this is regularly reiterated for services we consume freely on the Internet, "*If you're not paying for it, you're not the customer; you're the product being sold*". This is a powerful counternarrative to that of adverts informing consumer choice.

It is clear that the market now operates from inside the home, with advertising that seeks to persuade and drive instantaneous purchases – a model understood from the days of commercial television and radio. What is less clear is the business model used by some of the largest Internet companies to profit from their numerous free services; and how we might, should we wish, struggle with them. Zuboff's analysis of Surveillance Capitalism offers an explanation.

Surveillance Capitalism: you are the abandoned carcass

Shoshana Zuboff, the author of *The Age of Surveillance Capitalism*, tells us to, "*Forget the cliché that if it's free, 'You are the product.' You are not the product; you are the abandoned carcass. The 'product' derives from the surplus that is ripped from your life.*" (Zuboff, 2019, p. 377).

Zuboff's analysis of Surveillance Capitalism offers a way of understanding the bewildering activities of the largest dot-com companies – namely: Facebook, Amazon, Netflix and Google (Zuboff, 2019). Zuboff's explanation is that they are engaged in nothing less than a restructuring of Capitalism, where instead of the free market operating to set a price by the complex unknown forces of supply and demand, they can instead know, predict and manipulate the motivations of each individual actor in the market. They strive to know and control the market completely. This is accomplished by

[19] The DNS (Domain Name System) is an esoteric infrastructural element of the Internet – to which I will return in Chapter Four.

multifactored real-time surveillance of large populations, producing big data and driving machine learning algorithms, through which individuals are laid bare. This seems an extraordinary claim, but Zuboff is persuasive. Her analysis reframes these companies' bewildering product ranges as their extended efforts to entangle themselves in every aspect of private lives, inside and outside of the home. Figure 5 shows a portfolio of Google's activities in 2019; more accurately of Alphabet Inc., Google's supersidiary since 2015. It is easy to read Surveillance Capitalism with a focus on surveillance and the consequential issues of privacy, but Zuboff emphasises this is, "*an assault on human autonomy*". If she is right, this represents an urgent struggle for our everyday liberty and the sanctity of the home. Rather than operating with free will in the market, we become trapped in normative algorithmic *filter bubbles* (Parramore, 2010).

*AdMob, AdWords Editor, american fuzzy lop, **Android**, Android Auto, Android One smartphones, Android Studio, Android TV, Backup and Sync, ATAP, Bazel, Blogger, Blogger Mobile, Boutiques.com, Build with Chrome, Calico, CapitalG, Catalogs, **Chrome OS**, Chromebook Pixel, Chromebox, **Chromecast**, **Chromecast Audio**, Chromecast Ultra, Chronicle, Dart, **DeepMind**, Drive, FeedBurner, Files by Google, Firebase, **Fitbit**, FlatBuffers, Flutter, Freebase API, G Suite, Galaxy Nexus, Gboard, Gerrit, Glass OS, **Gmail**, GN, Go (programming language), Google 3D Warehouse, Google Accelerated Mobile Pages (AMP), Google Account, Google Activity Report, Google Ad Grants, Google Ad Manager, **Google Ads**, Google AdSense, Google Alerts, **Google Analytics**, Google App Engine, **Google Assistant**, Google Authenticator, Google Bookmarks, Google Books, Google Business Solutions, **Google Calendar**, Google Cast, Google Charts, **Google Chrome**, Google Classroom, Google Closure Tools, Google Cloud Platform, Google Cloud Search, Google Crisis Response, Google Cultural Institute (also known as Google Art Project), Google Custom Search, Google Dataset Search, Google Daydream View, Google Developers (was Google Code), **Google Docs**, Google Domains, Google Drive, Google driverless car, Google Earth, Google Fi, Google Fiber, Google Finance, Google Firebase, Google Flights, Google Fonts, Google Fuchsia (unreleased), Google Fusion Tables, Google Get Your Business Online, Google Glass, Google Goggles, Google Groups, Google Guava, **Google Hangouts**, Google Hire, **Google Home**, Google Hotel Finder, Google Ideas, Google Images, Google Input Tools, Google Japanese Input, Google Keep, **Google Maps**, Google Maps Gallery, Google Marketing Platform, Google Mars, Google Moon, Google My Maps, Google News, Google Ngram Viewer, Google Now, Google OnHub, Google PageSpeed Tools, Google Patents, **Google Pay**, Google Pay Send, Google Person Finder, **Google Photos**, Google Photos Backup, Google Pinyin, **Google Play Store**, Google Podcasts, Google Primer, Google Product Search, Google Public Data Explorer, **Google Public DNS**, Google Safe Browsing, Google Santa Tracker, Google Scholar, **Google Search**, Google Search Appliance, Google Search Console Sitemap, Google Shoelace, **Google Shopping**, Google Sites, Google Sky, Google Station, **Google Street View**, Google Street View Inside Trusted, Google Surveys, Google Sync, Google Tag Manager, Google Tez, Google Toolbar, Google Transit, Google Translate, Google Trends, Google Trends Screensaver, Google Voice, Google Web Designer, Google Web History, Google Web Toolkit, **Google Wifi**, Google X, Google+, Googletest, GV, Jamboard, Jigsaw, Live Transcribe, Maps Navigation, Mobilizer, **Nest Labs devices**, Nexus One, Nexus 4, Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, Nexus 7 (2012), Nexus 7 (2013), Nexus 9, Nexus 10, Nexus Player, Nexus Q, Nexus S, Nik Collection, One Today, OpenSocial, Password Checkup Chrome Extension, Pixel, Pixel 2, Pixel 2 XL, Pixel 3, Pixel 3 XL, Pixel 3a, Pixel 3a XL, Pixel 4, Pixel 4 XL, Pixel C, Pixel Slate, Pixel XL, Pixelbook, Poly, Project Titan, Project Wing, Quick, Draw!, **reCAPTCHA**, Shopper, Sidewalk Labs, Sky Map, Smarty Pins, SMS Channels, Speak To Tweet, **Stadia**, Tango, **TensorFlow**, Tilt Brush, Titan Security Key, Translator Toolkit, **Waze**, Wear OS, Who's Down, Yinyue (music), **YouTube**, YouTube Remote and Zygote Body.*

Figure 5. Alphabet's portfolio. (Hartmans, 2018; Wikipedia contributors, 2019)

From Data Exhaust to Behavioural Surplus

Zuboff's Surveillance Capitalism story begins in the dot-com bubble and the subsequent crash of 2000 when it became clear that the exuberance of venture capital-funded Silicon Valley was unsustainable and without a path to long-term profitability. Google survived the crash and in around 2001 hit on a way to turn what had been considered the company's data exhaust, the logs of search activity, into an important asset. Using an individual's search history, for any given advert they could make a prediction of the likelihood that this user would click-through based on their inferred profile and interests. Google could now target adverts for their customers – it seemed like a win-win, where searchers weren't inundated with irrelevant ads and advertisers didn't have to pay to reach people who weren't interested – and search could stay free. This was an extremely successful and profitable strategy for Google. Zuboff terms this exhaust data behavioural surplus; that which is generated by the use of the system and can be used to infer an individual's current or future behaviour – the *prediction product*. Soon, Zuboff argues, Google was designing new services specifically to create this behavioural surplus at scale for large populations with services that observed lives in ever more detail.

Bruce Sterling offers a similar (earlier) account in *The Epic Struggle of the Internet of Things*, "*Google and Facebook don't have 'users' or 'customers'. Instead, they have participants under machine surveillance, whose activities are algorithmically combined within Big Data silos.*" And, "*Google sells network surveillance and collective intelligence. This is Google's actual, profitable, monetisable product. 'Search' is merely Google's front end, a brilliant facade to encourage free interaction by the public. People are not Google's 'customers' or even Google's 'users', but its feudal livestock.*" (Sterling, 2013)

Zuboff argues that a Surveillance Capitalist's primary objective is to create behavioural surplus and that their product's ostensive function need not bear much relationship to the data it creates. For example, when Google Maps is used to generate a driving direction, the convenience of having the map locate one's current position (via GPS) and having a bookmarked home location, then discloses where the user is now, where they are likely to be (and when) and a prediction of their socioeconomic situation from their home address. Given what is also known about this person from their use of other Google services and what similar people did previously in this situation a prediction product can be produced – perhaps a takeaway meal after a long drive far from home. Alphabet then has a product that they can auction at a price they determine – in this case, to a local restaurant making a timely advertisement. To extract the maximum amount of behavioural surplus these services then crave attention and are designed to hold it for as long as possible.

This goes some way to explain the explosion of Alphabet's diverse products and services. Operating at scale this behavioural surplus data can be mined by statistical methods and machine learning to extend Alphabet's oversight of an individual's real-time interests, relationships, wealth, location, physiology and anxieties etc – ways to know and predict the state of the market. Zuboff argues that this marks a fundamental shift in the operation of the market, that there is the construction of a new age of Capitalism, where only a few Surveillance Capitalists know and can manipulate the perfect market; something Hayek would see as an absurdity.

Manipulating the Market

A Surveillance Capitalist's ambition is not simply to know the market, says Zuboff, but also to manipulate it through the application of the psychology of behaviourism. In an interview with the Harvard Gazette she said, *"[Surveillance Capitalists] learn to tune, herd, and condition our behavior with subtle and subliminal cues, rewards, and punishments that shunt us toward their most profitable outcomes.*", (Laidler, 2019). This is the application of what Zuboff calls actuation or the *nudge* (Thaler and Sunstein, 2008).

The Pokémon GO craze of 2016 is perhaps the clearest current example of Alphabet's *actuation* of the market; launched in July by December it had almost 21 million daily active users in the United States alone. Pokémon GO is a location-based multiplayer game running on smartphones, where the objective is to collect the popular Pokémon characters by exploring the world. It was compelling and I played it for a few weeks myself.

"*While its initial players lauded the game for its incitement to head outside into the "real world", they in fact stumbled straight into an entirely fabricated reality, one based on years of conditioning human motivation through reward systems, and designed to herd its users towards commercial opportunities. Within days of the game's launch in 2016, its creators revealed that attractive virtual locations were for sale to the highest bidder, inking profitable deals with McDonald's, Starbucks and others to direct Pokémon hunters to their front doors. The players think they are playing one game – collecting Pokémon – while they are in fact playing an entirely different one, in which the board is invisible but they are the pawns.*", (Bridle, 2019).

Pokémon GO was developed by Niantic Labs, which was formed in 2010 as an internal Google start-up. It was spun out of the newly formed Alphabet in 2015, but Google maintained an investment and crucially provided the mapping infrastructure on which the app relied (Meyer, 2016). Pokémon GO then also demonstrates how through the supply of cloud-based APIs (Application Program Interfaces), Google can lure developers with well-designed reusable modules that ensure hundreds of thousands of apps also pump their digital exhaust back to Google. Curiously, Zuboff's account of Pokémon GO misses the contribution of these APIs.

Home as a Data Factory

So far, I have described Zuboff's Surveillance Capitalism feeding predominately off desktop search and smartphone apps. However, there are some very specific ways in which it can be seen as this is a struggle in the home, with Google and Amazon, in particular, having growing portfolios of domestic Internet of Things devices. As the design writer Justin McGuirk puts it, "…*the proliferation of smart, connected products will turn the home into a prime data collection node. It is estimated that there will be fifty billion wi-fi-connected devices by 2020, and all of them will collect data that is transmitted to and stored by their manufacturers. In short, the home is becoming a data factory.*" (McGuirk, 2015).

While the private accumulation of vast long-term repositories of highly personal data is a considerable privacy concern in itself, Zuboff's interest is less in the home as a data factory and more in it as an exceptional sanctuary for individual expression. A concern perhaps closer to Chesterton's desire for the wildness of domesticity. Of homes Zuboff' says, "*Now they are simply the coordinates for 'smart' thermostats, security cameras, speakers and light switches that extract and render our experience in order to actuate our behavior*" (Zuboff, 2019, pp. 477–478).

Critiques of Surveillance Capitalism

Since its publication in 2019 Zuboff's book on Surveillance Capitalism (Zuboff, 2019) the thesis has been widely discussed in the popular press (Bridle, 2019; Kavenna, 2019; Laidler, 2019) and increasingly by HCI scholars (Borning et al., 2020). Its reception has been largely uncritical, with the exception perhaps of the protracted review by the writer Evgeny Morozov (Morozov, 2019). Morozov makes two arguments relevant to my thesis: that claims for a new age of Capitalism, are melodramatically overstated, Surveillance Capitalism being simply capitalism; and that alternative explanations for data collection, beyond behaviour modification, are not entertained.

"*Amazon might indeed be harvesting our conversations from Alexa-enabled devices to eventually modify our behavior; moreover, it might even be modifying our behavior to extract more data. But it's also possible that Amazon simply wants to improve its voice recognition capacity, which it then monetizes through Amazon Web Services, the main source of its profits. Amazon, like most large tech concerns, does conceal its data extraction. But the invisibility of its operations proves, at most, that they are rogue. Zuboff's definition of surveillance capitalism hinges upon whether behavioral surplus is used to modify behavior, not whether data extraction is visible.*" (Morozov, 2019).

Morozov claims the ride-hailing company platform Uber is a counter-example of a company that gathers large amounts of data but isn't engaged in Surveillance Capitalism. However, he entirely fails to mention the dynamic pricing model of the platform, a price that is uniquely determined for the individual customer given what is known about their journey and their willingness to pay – a precise manipulation of the market (Mahdawi, 2018). In these details Morozov seems to be less than competent.

While I find that there is a hyperbolic tone to some of Zuboff's claims, at times there are technical ways in which Google's data gathering potential is actually underplayed. Google's insidious use of tracking cookies embedded through Google Analytics, its provision of Internet infrastructure through Domain Name Servers (DNS) and cloud-based APIs (Application Program Interfaces), all escape her attention. Similarly, Amazon's AWS (Amazon Web Services) cloud computing platform is unmentioned, despite providing the cloud services for many major Internet services (see Figure 6), contributing significantly to Amazon's profitability (Goode and Simonite, 2021) and presumably behavioural surplus.

*Aon, Adobe, **Airbnb**, Alcatel-Lucent, AOL, Acquia, AdRoll, AEG, Alert Logic, Autodesk, Bitdefender, BMW, **British Gas**, Baidu, Bristol-Myers Squibb, Canon, Capital One, **Channel 4**, Chef, Citrix, Coinbase, Comcast, Coursera, Disney, Docker, **Dow Jones**, European Space Agency, **ESPN**, Expedia, **Financial Times**, FINRA, General Electric, GoSquared, **Guardian News & Media**, Harvard Medical School, Hearst Corporation, Hitachi, HTC, IMDb, International Centre for Radio Astronomy Research, International Civil Aviation Organization, ITV, iZettle, Johnson & Johnson, JustGiving, JWT, Kaplan, Kellogg's, Lamborghini, Lonely Planet, Lyft, Made.com, McDonalds, NASA, **NASDAQ OMX**, **National Rail Enquiries**, National Trust, **Netflix**, News International, News UK, Nokia, Nordstrom, Novartis, Pfizer, Philips, **Pinterest**, Quantas, **Reddit**, Sage, Samsung, SAP, Schneider Electric, Scribd, Securitas Direct, Siemens, **Slack**, Sony, SoundCloud, **Spotify**, Square Enix, Tata Motors, The Weather Company, **Twitch**, Turner Broadcasting,Ticketmaster, Time Inc., Trainline, **Ubisoft**, UCAS, Unilever, US Department of State, USDA Food and Nutrition Service, **UK Ministry of Justice**, Vodafone Italy, WeTransfer, WIX, Xiaomi, Yelp, Zynga and Zillow.*

Figure 6. Amazon's AWS customers. (Gillard, 2020)

While Zuboff may not demonstrate a strong technical understanding of the mechanisms of surveillance; I am persuaded that Surveillance Capitalism is a useful working hypothesis and a genuine attempt to reveal the hegemony of the Internet and by extension the networked home. That being true, existing legislation is too narrowly focused on privacy to offer sufficient consumer protection. Indeed, Zuboff asks us to find new forms of collective action and to be the friction, to struggle in the market.

Struggles to be Private

The struggle to live privately is in many ways it is the overarching concern of this thesis and is reflected in its concern for a network of one's own. Most broadly, private life is a struggle to live together in community groups, where an individual's liberty might be seen to be threatened by, or threaten, a wider society. Freedom of expression has been a long-cherished value in Europe and Northern America, although not always equally enjoyed by all citizens. The *Declaration of the Rights of Man and of the Citizen* (1789) is a key text of the French Revolution and shortly afterwards the *First Amendment* to the United States Constitution is that of freedom of speech (1791). Coupled with ideals of the sanctity of and dominion over one's home, society and the state are kept at bay and private life can continue behind closed doors. In this section I am going to illustrate this struggle through the networked home's interactions with government, corporations, and hackers with criminal intentions.

From Governments

In recent years, governments and law enforcement agencies have sort to extend the legal ways in which the data produced by the networked home can assist in their investigations, a clear struggle with the castle doctrine of the home. Courts can now regularly use mobile phone cell tower location data in evidence and increasing timestamped data from devices like Fitbit trackers and Playstation games consoles (Burgess, 2018); there is seemingly a trend toward gathering digital evidence from the Internet of Things. In 2016, for instance, the police in Bentonville, Arkansas issued a warrant for Amazon to make available any possible recordings from an Echo assistant, suspected of witnessing a murder (Steele 2016).

Totalitarian regimes have employed increasingly sophisticated technologies to covertly observe the private lives of their populations, such that George Orwell's *Nineteen Eighty-Four* (Orwell, 1949) resonates in the public consciousness and is the basis for much popular critique – *Big Brother is Watching You!* A 20th Century history of the surveillance of individuals in their private homes is principally that of listening devices, a range of ingenious bugs and wiretaps of telephone lines, used notably by organisations such as the Communist East German Stasi (1950 – 1990). The film *The Lives of Others - Das Leben der Anderen* (von Donnersmarck, 2006) tells the story of a Stasi operator who develops an almost paternalistic (and yet unseen) relationship with the suspected dissident writer on whom he spies. This kind of surveillance is extremely labour intensive and consequentially it is necessary to be highly selective of targets. 21st Century state surveillance has taken quite a different turn, where now surveillance can be machine-driven, indiscriminate and with storage, retrospective. This is an age of bulk collection and mass surveillance.

The authoritarian Chinese government's so-called *Great Firewall of China* became operational in 2006 and blocks access to the majority of foreign websites, social media and messaging – in addition, content is regularly manipulated and removed by government agents. The Firewall seeks to control a whole nation. Individuals are accountable for their actions and can have their access revoked for a range of transgressions (Dreyfuss, 2018). These measures require the direct intervention of the Internet Service Providers and the oversight of an Internet police force said in 2013 to number two million people (Le, 2013). Some Chinese citizens are in struggle with this regime and employ a range of countermeasures to access the Internet beyond the firewall. These include the use of proxy servers and VPNs (Virtual Private Network) to bypass the firewall, but these paths often become known and then blocked by the authorities.

In 2013, Edward Snowden leaked classified detailed technical documents from the USA's National Security Agency (NSA) revealing the extent of the surveillance programmes run by the Americans and by association with the British (Greenwald, 2013). What became shockingly apparent was the degree of mass peacetime surveillance by democratic nations, accomplished through the monitoring, storing and manipulation of Internet traffic – a dragnet where everyone could be a target. Central to this was the PRISM programme, where major Internet companies, including Microsoft, Skype, Apple, Google, Facebook and Yahoo collaborated with the NSA to give direct access to their customer's data – providing access to massive amounts of information about their personal and professional lives.

In 2017, further publications of confidential CIA documents, via the WikiLeaks website, made it clear that the surveillance agencies had moved beyond the passive accumulation of communications data and they were actively hacking into phones, apps and the Internet of Things – exploiting security flaws in commercial software (MacAskill, Thielman and Oltermann, 2017). It was disclosed that a joint workshop between the CIA and MI5 in 2014 had led to the development of the so-called *Weeping Angel* exploit[20], which allowed the Internet connected Samsung televisions to be used as a remote listening device while appearing to be turned off. The documents also revealed that smartphones had also been targeted; detailing ways to exploit both Apple's iPhone and Android devices. Security agencies were, in theory at least, using the practices of hackers to target individuals by manipulating their networked homes.

The purpose of surveillance is not only to gather data about a state's potential adversaries but also as a means of exacting some control over its general population. As Snowden says, "*Under observation, we act less free, which means we effectively are less free*" (Snowden, 2014). In essence, this is a restatement of Jeremy Bentham's conception of the Panopticon prison (Bentham, 1791) and Michel Foucault's analysis of the *panoptical power* of self-surveillance (Foucault, 1977); that an individual's behaviour can be controlled through their knowledge of, or their suspicion of, their observation, making restrictions that go beyond what is directly codified in law.

Nudge describes another way in which an individual citizen's behaviour can be regulated without resorting to the law; typically, it is a relatively subtle intervention, sometimes with a surveillance component. The behaviourist concept of Nudge has gained (perhaps misplaced) academic and political respectability in recent years, being popularised by the book of the same name (Thaler and Sunstein, 2008).
In 2010, the UK government launched the Behavioural Insights Team which was

[20] https://wikileaks.org/ciav7p1/cms/page_12353643.html

unofficially known as the Nudge Unit. The Nudge Unit's successes included enrolling an additional 100,000 organ donors a year and persuading 20% more people to switch energy providers – typically with a simple change of language in a well-timed text message or email, often relating an individual's current behaviour to what is said to be normal (Rutter, 2015). The Nudge Unit was privatised in 2014.

The Chinese government's appropriation of network technologies for state control goes beyond its Great Firewall. Currently under development, the nationwide Social Credit System (SCS) is a reputation system that computes a single numerical score for each citizen, "*judging citizens' behaviour and trustworthiness*" (Kobie, 2019), as observed by the activity of an individual's smartphone. "*For the Chinese Communist Party, social credit is an attempt at a softer, more invisible authoritarianism. The goal is to nudge people toward behaviors ranging from energy conservation to obedience to the Party.*" (Hvistendahl, 2017).

The scope and operation of the *Social Credit System* are currently unclear – at least from my point of view in writing this section – with different observers drawing quite different conclusions. Its purpose within China is to nudge citizens into compliance, and this by design weaponises an ambiguity of surveilled behaviour and score outcomes. Outside China it is used to demonstrate the Communist country's disturbing authoritarianism; where (at least in the UK and US) it is frequently framed by reference to the popular Black Mirror episode, *Nosedive* (Wright, 2016) – a dystopian drama in which the protagonist is driven to increasingly desperate behaviours as her social score becomes reduced. In either case, the truth of the system is politically malleable – the system is never entirely revealed.

Seemingly, at the time of writing (April 2020), China's one Social Credit System is still in development, with reports suggesting a target deployment sometime in 2020 (Hvistendahl, 2017). However, a collection of similar regionally based and privately developed systems are already operational across China – notably the Sesame (or Zhima) Credit system owned by Ant Financial an affiliate of the Alibaba conglomerate. "*Sesame determines a credit-score ranking—from 350 to a theoretical 950—dependent on 'a thousand variables across five data sets,' according to the firm.*" (Campbell, 2019). Some of this data is drawn from Alibaba's multiplicity of services, which significantly includes Alipay. Alipay is now the default way to make payments in China, regardless of the outlet, in person or online. As the Chinese economy becomes practically cashless, all transactions leave a data exhaust and significantly payments can be centrally blocked if scoring criteria are not met for that type of purchase. Accountability is ensured by a user's Alipay ID, verified both to their smartphone and national identity card. In addition to ubiquitous electronic payments, the Alipay apps enable: food delivery, car insurance (linked to driving documents and endorsements), medical appointments (and health records), utility bill payment and a social network – scores are depend not only an individual's behaviour but also those of their family and friends (Hvistendahl, 2017).

High Sesame scorers enjoy a variety of perks, they "*can rent cars without a deposit, get better rates of foreign exchange and even skip hospital waiting lines.*" (Campbell, 2019). However, those with low scores (or associating with those with low scores) find themselves excluded, prevented from booking a range of services from travel tickets to hotel rooms. Reports of more punitive measures are confused but suggest that among other things university places are being denied to those with low scores (Chan, 2018). It is unclear whether any of the Chinese Social Credit Systems derive data from the usage of the domestic Internet.

One can only meaningfully struggle to be private from the activities of the government that are known or suspected, those which are covert are impossible to grasp. This is the motivation of whistle-blowers like Snowden and the journalists unpicking the Chinese Social Credit System. Their work has begun to reveal how private online lives and networked homes are now implicated in systems of surveillance; further that these systems now give governments the capacity to influence or modify the behaviour of their citizens in subtle (unseen) ways.

From Corporations

Since the earliest days of the Internet, many websites have attempted to provide some degree of personalisation, often through a notion of a user's account – granting specific views of content and maintaining preferences. With an authenticated account, a user's every seemingly private interaction with the service, over an indefinite period of time, can be obtained from an analysis of the server logs.

Server logs can give a corporation a detailed picture of an individual's use of a service, but for a broader picture another mechanism is used. A persistent cookie is a small piece of data, stored on the user's local machine which the website can interrogate. Modern browsers by default accept these cookies from visited websites without the user's explicit say so. Where multiple webpages include content from the same third-party, perhaps an embedded advertisement, this third-party can set a tracking cookie that will track a single user's interactions with all these websites. Almost every large modern website will embed tracking cookies, whether the advertising is evident or not. The largest players include Doubleclick (Google), Quantserve (Quantcast), Scorecard Research (ComScore), Facebook, Twitter, Google, AddThis (Clearspring), Adnxs (AppNexus) and Yieldmanager (Yahoo) – (Geary, 2012). Their use creates a rich profile of this user's private interests and behaviour, built up over time. Typically, this is an audience segmentation profile that categorises users by their inferred demographic, product usage, psychographic, behavioural and media-use profiles. These profiles can then be brokered, for a price, to third parties such as marketers and local authorities – as well as informing internal business decisions. Beyond a simple invasion of privacy, these profiles may be mistaken and may subject the individual to unfair treatment (Kaltheuner, 2018).

The Cambridge Analytica scandal of 2018 brought the issue of privacy and online manipulation into sharp focus for many (Graham-Harrison and Cadwalladr, 2018). Cambridge Analytica did not have to assemble partial pictures of users by tracking them across the Internet, instead they exploited the massive reserve of a decade of private data that had been entrusted to Facebook. In 2014, Cambridge Analytica designed a Facebook personality test that not only collected an individual's answers but also harvested personal details from their accounts and the accounts of their friends and family. In this way, Facebook later admitted that Cambridge Analytica collected psychometric profiles of 87 million users (Kozlowska, 2018). The purpose of this collection was political manipulation; to craft specific, often dishonest, political messages to resonant with an individual's fears and influence their voting. In this way it is claimed that the electoral process was manipulated for the benefit of Cambridge Analytica's clients; notably the UK EU referendum and US presidential election, both in 2016. These tactics have clear parallels with Surveillance Capitalism.

With increased public literacy of the threats posed by corporate private-data harvesting, demand has grown for regulation and control. One of the most significant recent legal events is the European Union's GDPR (General Data Protection Regulation) introduced in 2016 to govern data protection and privacy, within and transferred out of the European Union (EU) and the European Economic Area (EEA)[21]. The regulation entered into UK law through the Data Protection Act of 2018. Most apparently this law has changed our expectations for privacy when web browsing, with notices to accept the tracking cookies used, but its implications extend to all elements of the networked home. The law requires that consumers the have right to manage how data is collected about them, that they knowingly opt-in and can subsequently opt-out. Further that

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

there is a right of access to the data that an organisation holds on an individual through a subject access request. For domestic Internet products such as the video streaming service Netflix, successful subject access requests have returned detailed audience segmentation profiles and the minutiae of interaction events (Porter, 2019). Significantly GDPR makes these requirements for any product operating in the EU and EEA, regardless of its origin. As the enforcement of GDPR struggles to become established and its implications widely understood, it is hoped that these legal tools then enable individuals to struggle for their privacy (Naughton, 2020).

While data privacy has been the subject of academic study for many years, only a few works respond directly to private data and the domestic Internet. Databox is one such project and calls for a radical infrastructural redesign of data storage, such that personal account data is stored within the home and the algorithms of external agents are granted specific permissions to operate on it in situ, with only the data representing the result leaving the home (Crabtree *et al.*, 2018). This represents a significant shift of power from data centres to the edge of the network, back behind the home's closed doors.

From Hackers

Through the domestication of the Internet, more that is valued has been moved onto the network and with it the potential for serious digital crime has grown. Previously in this chapter I discussed networked-based domestic abuse from within the home, but with the global span of the Internet, aggressors might be located anywhere. Scammers, blackmailers, hackers and viruses are increasingly remotely targeting private home networks.

That the Internet of Things creates the conditions for hackers to terrorise us in our own homes, is an often-rehearsed theme by journalists; be that by exposing the intimate details of our lives or by driving our homes against us. Burke's report is typically chilling, *Man hacks Ring camera in 8-year-old girl's bedroom, taunts her: "I'm Santa Claus"*, (Burke, 2019). It is then rhetorically argued that IoT security is lacking, with insecure protocols used and default passwords left unchanged. While, some attacks are perpetrated by individuals, many others are armies of semi-autonomous scripts, or bots, acting for some puppet master. As these stories multiple, a parallel security industry grows, and the law plays catch-up.

Such acts of hacking are criminalised and the private citizen is offered the protection of the law; at least in the UK. Under the Investigatory Powers Act (IPA) of 2016[22] it is an offence to, “*intentionally intercept a communication […] in the course of its transmission by means of a public or private telecommunication system*” (3.1). However, significantly for my later discussion of designerly ways of hacking in Chapter Five, it is not an offence under 3.1 to “*intercept a communication in the course of its transmission by means of a private telecommunication system if the person, is a person with a right to control the operation or use of the system, or has the express or implied consent of such a person to carry out the interception.*” (3.2). That is to say, that hacking one’s own network is a legal pursuit in the UK. However, this may necessarily not always be the case and ways of struggling through hacking might imply some degree of law-breaking.

Conclusion

In this chapter I have described some of the struggles of contemporary home life that can be overlooked when home is idealised as simple, static and uncontested. These seven types of domestic struggle should not be considered to be exhaustive or necessarily universal, but simply representative of some of this complexity. However, many of these will reoccur as this thesis unfolds, not least Zuboff’s analysis of Surveillance Capitalism, which seems to offer an immediate challenge to a private network of one’s own. This chapter has necessarily been wide-ranging, drawing from a diversity of sources and covering many important issues, often at speed. Chapter Three will slow down and look closely at the work in and implicated by the home, that is also frequently overlooked or made invisible.

[22] http://www.legislation.gov.uk/ukpga/2016/25/contents

Chapter Three: Seeing Work in the Home

This chapter describes ways work is overlooked in the home, whether that be the work of people or machines. By applying the feminist conception of Invisible Work (Daniels, 1987) it argues that domestic technologies typically (and historically) emphasise invisibility, seeming ubiquity and automation; and in doing so the home can obscure its exploitation of people and resources. The dominant Silicon Valley and HCI research visions have expectations of invisible work that ultimately shape the contemporary possibilities of the networked home, and a critique of this is offered here. The invisibility of work parallels the overlooked struggles seen in the previous chapter as a means by which the home is rendered simple, static and uncontested.

This chapter is divided into two parts. The first part explores invisibility in the context of the Victorian country house and modern Ghost Work (Gray and Suri, 2019), then through the mass electrification of the suburban home in the 20th Century and a post-war push button culture, then in 1980s dreams of Smart Homes and finally in the Ubiquitous Computing agenda of the 1990s. The second part suggests some ways to design alternatives that struggle to make the networked home visible, starting with the whimsical machines of Rube Goldberg, then focusing on three influential speculative HCI and design research discourses (making by making strange, artful systems and making the invisible visible) that seek to challenge an uncomplicated narrative, reveal the hegemony and make the labour on which the home relies apparent. Broadly these suggest ecological, ethnographic and material ways to understand the home and lays a foundation for this thesis' methodological approach, which is developed in the next chapter.

Part One: The Invisibility of Work

When work is invisible it has the outward appearance of being automatic – hiding the necessary human labour and human decision making required for machines to operate. The automated home might then describe any home where its operation is simply experienced as automatic. This definition allows one to take a more inclusive historic perspective on the automated home (or home automation, or even domotics) over the past century and more, which includes both the operation of the Victorian country house and modern Internet-enabled domestic Ghost Work (Gray and Suri, 2019).

At the heart of this analysis of visibility is the feminist sociologist Arlene Kaplan Daniels' conception of Invisible Work (Daniels, 1987) used as means to reveal the private work of the home and the ways in which historically women's domestic labour was considered unremarkable and so devalued. Daniels argues that housework inside a private home is invisible to the outside world, but also invisible to the men within, who dismiss it as simply the moral order of things – perhaps even automatic. Daniels' analysis is contemporary with Cowan's critique of 20th Century domestic technologies (Schwartz Cowan, 1983) which also serves to make the reality of housework apparent. Lucy Suchman's related analysis of invisible work is concerned with the automation of professional workplace tasks, she argues that some professional identities promote a degree of secrecy and "*Making work explicit, visible increases workers' vulnerability to rationalizing agendas.*" (Suchman, 1995, p. 60). However, this invisibility can also lead others to devalue and disregard the skills and resources that work requires; for service work, "*the better the work is done, the less visible it is to those who benefit from it*" (Suchman, 1995, p. 58). The visibility of women remains a strong theme in feminist writing today, for instance Caroline Criado Perez's *Invisible Women: Exposing Data Bias in a World Designed for Men* (Criado-Perez, 2019) a widely lauded book from 2019.

This part of the chapter explores invisibility and invisible work in four interrelated sections: in the context of the Victorian country house and modern Ghost Work, then through the mass suburban electrification of homes in the 20th Century and a post-war push button culture, then in the 1980s dreams of Smart Homes and finally in the Ubiquitous Computing agenda of the 1990s. In all these periods the automated home has been an enduring and influential fantasy.

Out of Sight: Below Stairs and Below the API

Using my inclusive definition of the automated home, this section attempts to make a productive historic comparison between the domestic organisation of the Victorian Country House and the invisible labour of those below stairs, with modern Internet Ghost Workers, who are below the API – doing unseen work from within the machine. Each is taken in turn and together they paint an unsettling picture of exploitation and limited human expression.

Below Stairs in the Victorian Country House

The country houses of Victorian England were curious places. Often situated in large country estates, away from the industrialising towns and cities – homes to both the aristocracy and palaces for the nouveau riche. They were complex organisations, employing large numbers of people in the management of the land and the home. As Palmer and West describe, it was in these homes that many of the domestic technologies that became commonplace in the 20th Century were first gradually introduced – specifically: plumbing, central heating, the electric light and telecommunications (Palmer and West, 2016). Over time the functioning of these estates became reliant on these technologies, but in their early experimental forms they served to publicly signal the wealth, influence and learning of the owner – they were showcases of these new technologies for the wonderment of guests. Lord Armstrong's Cragside in Northumberland was the first home lit by Joseph Swan's electric incandescent lamp in 1880 (Palmer and West, 2016, p. 86) and is an excellent example of such a destination.[23]

A large Victorian house's demands for heating and lighting, and its occupants' needs for sanitation and food preparation required large numbers of servants working around the clock, with varying specialisms. Yet that labour and complexity were to all intents and purposes rendered invisible to the family. As Palmer and West comment, "*planners devised ways of keeping the servants out of sight in the course of their duties as far as possible, burying them in basement walkways or service tunnels*" (Palmer and West, 2016, p. 131). Indeed, the architectural segregation of staff is coded into the language – *Below Stairs* being a term used widely throughout the 19th and early 20th centuries, referring to the basement being occupied by servants. Similarly, the tradesman's entrance further divided the family from the external

[23] In February 1879 Joseph Swan publicly demonstrated a working electric incandescent lamp to an audience at the Literary and Philosophical Society, Newcastle upon Tyne, in which large portions of this thesis have been written.

tradespeople on whom their lifestyles relied, through a separate doorway. Some high-status servants had personal and trusted relationships with their masters and mistresses, but most operated largely out of sight. [24]

The new technologies of the 19th Century served not only the immediate comfort and entertainment of the family but also to manage the organisation of the home – whilst holding it at a distance. Palmer and West describe an evolution of domestic communications systems: pull cords mechanically coupled to a system of sprung bells, buttons wired to electric bells and powered by batteries, speaking tubes and finally household telephone exchanges (Palmer and West, 2016). Bells became a ubiquitous way for masters to summon attention and for instructions to be issued to be disseminated below stairs – "*You Rang?*". The bell then was a means to manage the visibility of labour.

High-status servants were then the interface between above and below stairs, obscuring the operation of the home beneath. The conspicuous presence, particularly of the male butler figure, signaled wealth and command to visitors – a living demonstration of mastery and subservience. Yet, these could also be relationships of mutual trust and discretion – where the butler was valued for his wisdom; consider P. G. Wodehouse's popular character Jeeves. The butler's persona is often one of intimidating formality; and this can have an emotional personal cost, consider Ishiguro's Stevens in the *Remains of the Day* (1989). The figure of the butler recurs frequently in popular framings of domestic technologies and automation, but their status also relies on the invisibility of the labour of those subordinate to them, who were typically less well treated.

Through its architecture, technologies and social structures, the Victorian country house might almost seem to work by itself – functioning to screen the family from the complex reality of its operation. Such homes might then be seen as the first automated (and inherently smart) homes.

Over time the original Victorian mechanical pulls were updated with new electrical pushes and these technologies were moved into affluent homes (and hotels) in the electrifying cities. Push buttons and networks of wire were more easily installed and maintained than their predecessors; and were more easily embedded into rooms and furniture. As Rachel Plotnick puts it, "*By the 1930s, push buttons had achieved status as familiar communication and control mechanisms. Buttons' popularity related in part to their design and inexpensive construction. They could blend 'flush' into walls and*

[24] My grandma was *in-service* to a wealthy family in Westcliff-on-Sea in the 1920s. While evidently a hard life, she remained on friendly terms with the family for many years afterwards.

hide in pockets, making them attractive features when the newness of electricity and 'automatic' machines threatened existing social structures and patterns. They hid wires and other 'messy' aspects of electricity that could undermine harmonious, pre-electrical environments." (Plotnick, 2018, p. 227).

Below the API - Ghost Work in the Machine

The wealthy Victorian home operated to control the visibility of labour both through the social structure of the staff, the architecture of the building and the communication technologies it employed. The system of pull-cords, and later push buttons , created an asymmetric contractual interaction, with high-status servants (such as butlers) intermediating between those above and below stairs. For some tasks simply the presence of the bell or the light was enough to initiate some predefined action. Once this contract is made, a consumer of this service need not be concerned with the complex series of interactions of people, infrastructures and resources that are invisibly set in motion. This is the nature of Ghost Work (Gray and Suri, 2019).

Stories of humans hidden inside the machine are not unfamiliar, Wolfgang von Kempelen's Turk was built in the late 18th Century and demonstrated prodigious mechanical chess-playing abilities, whilst concealing an accomplished amputee (Standage, 2002). Amazon's Mechanical Turk or MTurk, introduced in 2005, specifically alludes to von Kempelen and hides the labour of so-called crowdworkers brokered from across the Internet. Workers receive small piecemeal payments for completing well-specified short Human Intelligence Tasks (HITs) – for instance, an image recognition task. This employment is inherently precarious. The invisible crowdwork involved in the Amazon Mechanical Turk is the subject of Lilly Irani and M. Six Silberman's longstanding Turkopticon project through which workers can (and still at the time of writing) "*publicize and evaluate their relationships with employers*" and thus render their conditions visible (Irani and Silberman, 2013). The naming of Turkopticon references the panopticon (described in Chapter Two), "*pointing to our hope that the site could not only hold employers accountable, bu[t] induce better behavior*" (ibid.) – a use of surveillance to counter invisibility.

In Peter Reinhardt's 2015 article, that preceded Ghost Work, he identified a section of employment as being *below the API* (Reinhardt, 2015) – jobs so tightly specified and technologically mediated that they can be written as calls to software functions. As Irani and Silberman said, "*employers can literally access workers through APIs*" (Irani and Silberman, 2013). The API (Application Programming Interface) is the contract by which software describes to the outside world its possible functions, their required inputs and the output they will produce – a black box description of the system. So, Reinhardt's below the API casts human labour into this hidden machine world. Modern workers risk being both *below stairs* and *below the API* – unable to identify their humanity from within the machine. From above, we need not know or care if the task was completed by a human – their labour exists inside the black box. Kiwi Campus operates a fleet of seemingly self-driving delivery Kiwibots at UC Berkeley, California – yet in reality they are remotely operated by low-paid students in Medellín, Colombia (Said, 2019). The Internet's global reach distances us from the networks of people, infrastructures and resources we are complicit in exploiting.

In modern rapid software development, the concept of abstraction, modularity and reuse is paramount. Practically every piece of code is dependent on a series of software libraries developed by others to accomplish common tasks, often drawing on data and resources from across the Internet. Each library and online service will define an API, leaving the software engineer to negotiate the articulation of these parts. A smartphone app using a map likely won't store the map imagery itself, but instead request it across the network from a source like Google; often for free. Through the reuse of these cloud-dependent libraries, a software developer can then very easily create sophisticated results – yet without necessarily having a full understanding of the system with which their software participates. While Zuboff does not explicitly make this point, the use of Google and Amazon Web Services (AWS) in a wide range of third-party apps and domestic IoT devices must contribute vast quantities of behavioural surplus data (Zuboff, 2019). There is much hidden below the API – not least Ghost Work.

Ghost Work is then likely already in the smart home. MTurk is but one of the Amazon Web Services that employ human labour and many other cloud-based services the domestic Internet of Things. For example, in 2019 it was disclosed that employees at Amazon reviewed the recorded audio from the Echo assistant to train its artificial intelligence (Fowler, 2019). To critique the inhumanity of these assistants, in 2017 the artist Lauren Lee McCarthy's project LAUREN attempted to become a human version of Amazon Alexa – "*For three days, I remotely watch over the person 24/7 and control all aspects of their home. I attempt to be better than an AI, because I can understand them as a person and anticipate their needs. […] I hope that by being a real person on the end of that, I am offering something more than an Alexa AI at least."* (McCarthy, 2018).

Taken together it is easy to see how invisible work features in both the Victorian country home and modern domestic Ghost Work. Today's networked homes have complex (and often invisible) dependencies on remote web services that implicate countless people and machines across the Internet, working under conditions that are unknown and potentially exploitative.

Electrification: Services at the Push of a Button

This section discusses domestic electrification in the 20th Century and shows that through its long employment of the simple push button, the home becomes dependent on unseen remote infrastructural services and an interactional trope seen in the Victorian country home that implies forms of invisible work.

In the early years of the 20th Century, the rise of the production line, mass production and mass consumption prioritised productivity, rationality and efficiency. This was the age of Taylor's Scientific Management (Taylor, 1911), the Gilbreths' time and motion photographic studies (prolific in the 1910s and 1920s) and Le Corbusier's home as "*a machine for living*" inside (Jeanneret, 1923). These new suburban communities were the product and subject of the new industrialised processes. As the technologies of electricity, gas, water and telephony moved into the cities from the country homes where they had been pioneered, they became organised and industrialised; first at metropolitan and then national scales – cycling between periods of nationalised and privatised ownership. With suburbia came the growth of private housing and a reliance on public utilities, rather than private domestic services and servants. Homes began to consume these standardised utility services – distant from their site of production.

Electric Suburbia's Invisible Infrastructure

Domestic electrification played out slowly over the course of the 20th Century during which time a rich cultural dialogue developed. The first domestic electric light was installed in 1880 (Palmer and West, 2016, p. 86) and by 1926 96% of American homes were electrified (Nye, 1992, p. 261), but for Europeans similar levels would not be reached until the post-war reconstruction of the late 1940s and 1950s (Deschamps-Sonsino, 2018, p. 17). In the meantime films like Buster Keaton's *The Electric House* (1922), Charlie Chaplin's *Modern Times* (1936) and Jacques Tati's *Mon Oncle* (1958) developed a popular narrative around electrification and automation. From the earliest imaginings of the automated home, these technologies have been framed as domestic servants. Čapek's play *Rossum's Universal Robots* (1920), popularised the notion of the mechanical being – which was quickly translated into working demonstrations of an impending future. At the World Faire in 1939 Westinghouse's *Elektro the robot* proclaimed in a mechanical voice, "*if you use me well, I can be your slave*" – yet far from subservient or invisible Elektro was seven feet tall, enjoyed smoking cigarettes and seemingly had no immediate domestic skills, but did respond to contrived voice commands (Reichardt, 1978, p. 74).

While speculation about domestic robots was largely fanciful, a domestic modernity that embraced utilitarianism did take hold, at least in wealthy homes. Publications such as Christine Frederick's *The New Housekeeping* (1918), argued for Taylorist ideas to be applied to the home. Margarete Schütte-Lihotzky's *Frankfurt Kitchen* (1926) then embodied this through architecture, optimising common tasks according to time and motion principles. However, as Daniels notes such time and motion actually contributed to making housework more visible (Daniels, 1987).

With post-war prosperity in Western Europe and North America, electrification became the means not only to affordably light the home but also to enable a growing range of home appliances – from cookers and heaters to televisions and radios.[25] From the 1950s companies such as Braun and designers such as Dieter Rams translated these ideals into affordable mass-market domestic product design for the post-war suburban boom. The popularity of new appliances made ever more demands of the unseen national grid and began to shape aspirations of the homelife.

Figure 7. Total Electric Home. © Westinghouse, 1960. Redacted.

[25] As described in Chapter 2, at the time of my grandma's death in 1982, while her rented house had electrical lighting, there was just a single electrical socket, into which was plugged the black and white television set on which she would enjoy watching the wrestling on a Saturday afternoon.

Westinghouse's Total Electric Home (1960) is exemplary of this post-war electric consumer optimism, see Figure 7, "[…] *electricity does absolutely everything: heats, air conditions, cooks, preserves food, lights, entertains, encourages hobbies, makes it the easiest ever for you and your family to be happier, healthier, to live fuller lives. Total Electric Living has no limits*." This was the era of Hanna-Barbera's futuristic *The Jetsons* (1963) and the idea of the electrically automated home were popularly established.

Similarly, in 1956 the Whirlpool Corporation had, in collaboration with the Radio Corporation of America, launched the *RCA Whirlpool Miracle Kitchen* (Whirlpool, 1956). This exhibit demonstrated a "*laboratory of kitchen ideas*" – where, "*the things women don't like to do are done automatically.*"[26] The automation of the Miracle Kitchen revolved around the *Planning Center,* described in their short film as a "*push-button control panel*. […] *the heart and the brain of the RCA Whirlpool Miracle Kitchen.*" As the film unfolds, we learn of the "*wonderful new world of push-button cooking, cleaning and homemaking.*" Where "*merely pressing a button…*", instructs a breath-taking series of automations from an early robotic vacuum to food preparation. These showhomes were machines for living inside.

While in hindsight the Westinghouse Total Electric Home and RCA Whirlpool Miracle Kitchen seem fantastical and perhaps naive, the notion that these modern electronic gadgets and appliances were labour saving was central to their marketing and extraordinary popularity. However, Cowan argues that in reality they transformed the nature of the work for women making it more opaque and less visible, with higher standards now being demanded that actually increased the workloads (Cowan, 1983). Needless to say, the promised domestic robots failed to take the strain and to this day remain largely a performative novelty.

The new electric homes and appliances both continued to render housework invisible and were at the same time silently consuming unseen resources from far across the network – ultimately, as we understand today, with a huge environmental cost. Yet, for the designer this utility service model creates a convenient abstraction. As James Auger and colleagues point out, "*Electricity, as a form of energy, comes through sockets on the wall that deliver a seemingly endless supply. These ubiquitous and generic sockets determine the design of every electrical product, providing a neat end to the designer's role and responsibility.*" (Auger, Hanna and Encinas, 2017, p. 6).

[26] The RCA Whirlpool Miracle Kitchen toured the United Stated in 1957 and in 1959 was part of the American National Exhibition in Moscow, where Richard Nixon and Nikita Krushchev played out the Cold War through their Kitchen Debate – but that's another story.

Merely Pressing a Button

By the 1950 and 1960s, with these new electrical appliances, the push button or switch became a near-universal way to interact with services. The electrical doorbell (Joseph Henry, 1831), light switch (John Henry Holmes[27], 1884) and the television remote control remain examples of practically ubiquitous domestic push buttons to this day. Unlike the visible mechanics of the Victorian country homes' pull-cords systems, these operate by invisible electrical signals, infrared light or radio waves, which contributed to their inscrutability.

As Rachel Plotnick puts it, "*To push a button represented a particular fantasy of what I have termed digital command, where (certain) hands could direct anyone or anything to submit to their will. No longer did 'manual' refer to effort and strain; rather, the gentle or 'mere' touch of a button promised that only fingertips need engage with bells, lights, vending machines, elevators, or cameras. This 'reversal of forces' that centered on hand practices—where a small human force could put great electrical forces into motion-suggested that human beings had truly tamed nature by sublimating it to a push.*" (Plotnick, 2018, pp. 227–228).

The notion of the push button as a simple empowering interaction is prevalent from the 1950s, in the corporate domestic fantasies of the RCA Whirlpool Miracle Kitchen's Planning Center and forebodingly in the Cold War idea of armchair generals, push button warfare and the nuclear button. Merriam-Webster defines push button as, "*using or dependent on complex and more or less self-operating mechanisms that are put in operation by a simple act comparable to pushing a button.*" Simplicity is created by a gesture that triggers work of an unknown complexity in an unknown location, for some tangible outcome – the outcome of an interaction with an unfamiliar button will be uncertain. The button is the input to a black box that creates some output by processes we need not concern ourselves with – "*A black box contains that which no longer needs to be reconsidered, those things whose contents have become a matter of indifference*" (Callon and Latour, 1981, p. 285). The push button is then another means of rendering labour invisible with just the same intention as the Victorian country house.

[27] John Henry Holmes is buried less than a mile from my house in Jesmond Old Cemetery, Newcastle upon Tyne.

Figure 8. Zenith Space Command TV commercial. © Zenith Radio Corporation, 1972. Redacted.

To this day the authority of the bearer of the remote, doofah, zapper, clicker, flicker or plonker will be recognised in living rooms. The television remote control is an exemplarily push button interface first developed by Zenith Radio Corporation in 1950; it was on a long wire and called Lazy Bones. Over time the use of first visible and then invisible infrared light allowed these devices to become wireless. By the 1990s, in many homes an arsenal of push button remote controls became the most obvious expression of the automated home – but the codes used were proprietary, few interoperated and the use of infrared light limited their range. The marketing of the Zenith Space Command series (1956) makes the case for invisibility – "*You hear nothing! You see nothing! No batteries! No cords! No wires! No flashlights! No radio control waves! No transistors! The only wireless complete remote control!*" The device used inaudible ultrasonic tones that were mechanically produced by striking tuned metal bars with the action of a series of switches, each frequency operating a different function – being a mechanical device it needed no batteries. Yet the parallel to house servants is made even here, Figure 8 shows a still from a 1972 TV commercial for the Zenith Space Command in which the technology is framed as a butler in a grand home (Zenith Radio Corporation, 1972)[28].

Hobbyists also embraced the expression that electricity and the push button gave them. The past echoes too in the Popular Mechanics' article *Push-Button Manor* (Railton, 1950), featuring a reader's home in which "*hidden servants*" automate windows, doors, lights, an elevator and a burglar alarm – at the touch of a switch from a master-control room. Yet in some ways the Push-Button Manor rather complicates

[28] https://www.youtube.com/watch?v=PlgSuaIHYsY

an account of labour visibility. Unlike the corporate visions of Westinghouse and Whirlpool, this is a DIY project by the homeowner, Mr Mathias, who is both user and creator. He has devised each and every machine – necessarily engaging with the complexity of whole the system, he is not aloof from its reality but is able to modify and maintain it. At the point of action, the system might be invisible, but this does not render Mr Mathias ignorant of its operation. Furthermore, each machine addresses some specific bespoke desire, that is carefully integrated into the home over time – not a generic mass consumer product.

Push button simplicity is still compelling and remains ever-present in the modern home with the doorbell, light switch and TV remote, to name a few. The Amazon Dash Button (2015 – 2019) is a curious addition to this list, a single button WiFi device that when pressed instantaneously places an Amazon order for the specific product with which it is associated. Multiple buttons could be positioned around the home to be available at the opportune moment – a toilet roll button in the bathroom, etc. The product was marketed with the slogan, "*Place it. Press it. Get it*'. It is unclear what motivated Amazon's decision to discontinue the Dash Button, but the Echo series of devices (with the voice assistant Alexa) that survived it speak to a related domestic vision, that of the *smart home*.

The home's relationship to electricity as a utility service and its command via push button can be easily seen through the lens of invisible work – where production and consumption are removed from one another. In the case of the Amazon Dash Button, this then extends to a similar understanding of the Internet as an invisible infrastructural service and the possibility of Ghost Work in the fulfilment of the button press.

An Invisible Hand in the Smart Home

This section discussed the idea of the smart home in relation to invisible work and in doing so questions the (hidden) intentions of these systems and the implication of machine surveillance. Today *smart* is used to denote a series of network-based technologies from Amazon's Echo voice assistant to the Philips Hue – advertised as the "*smartest bulb in the room*". It can be difficult to untangle the *smart* from the *automated home,* but centrally these are concerns of agency, authority and accountability. For the purposes of this thesis, the essential experience of a smart home is a phenomenon brought about by the application of rules (learnt or otherwise) and sensor data, that goes beyond the well-specified repeated operation of a push button.

As the previous section described, networked homes are reliant on unseen services beyond their own walls and for a smart home this makes the attribution of decision-making problematic, be that by the hands of humans or machines. J. K Rowling's warning to "*Never trust anything that can think for itself if you can't see where it keeps its brain*" (Rowling, 1999) seems pertinent. Once the logics of a home become networked at scale into large communities, invisible hands have influence at scale, able to co-ordinate and control en masse. Be that an emergent benevolent force as Adam Smith (Smith, 1759) might have it, or as a centralising authority operating the much vaunted smart city, or in service to Surveillance Capitalists (Zuboff, 2019) – these are invisible hands acting in the smart home.

The smart home is also a long-told story of a near-future of as yet undelivered possibility – imagining how homes might think and act for themselves and dreaming a little of living inside a conscious entity – operating without even the inconvenience of a button press. Corporate fictions have often contributed to this promising the near-term arrival of the intelligent home – even the RCA Whirlpool Miracle Kitchen (1956) described the Planning Center as the *heart and brain*. Films such as Donald Cammell's *Demon Seed* (1977) and Ray Bradbury's *The Veldt* (1950) have also frequently returned to this proposition – often concerning the hidden dark intention of the machine. Such fictions hint at the inspiration for and can be a critical lens on, what has subsequentially been built. For instance, the degree to which a smart home's intelligence is personified and ascribed with motivations has been explored in films and fiction with such characters as Proteus IV in *Demon Seed* (1977) and HAL in *2001* (1968) – both ultimately murderous. Apple's influential speculative short film *Knowledge Navigator* (Field, 1987) has a more benevolent and subservient agent; situated in the grand home of a college professor, the bow tie wearing male virtual assistant (presumably to be read as a butler) manages communication and assists with finding research papers, although here the home environment is never explicitly manipulated. It is easy to draw comparisons between these fictions and the modern personified voice assistants of Amazon's Alexa and Apple's Siri (in contrast to Google's unnamed agent).

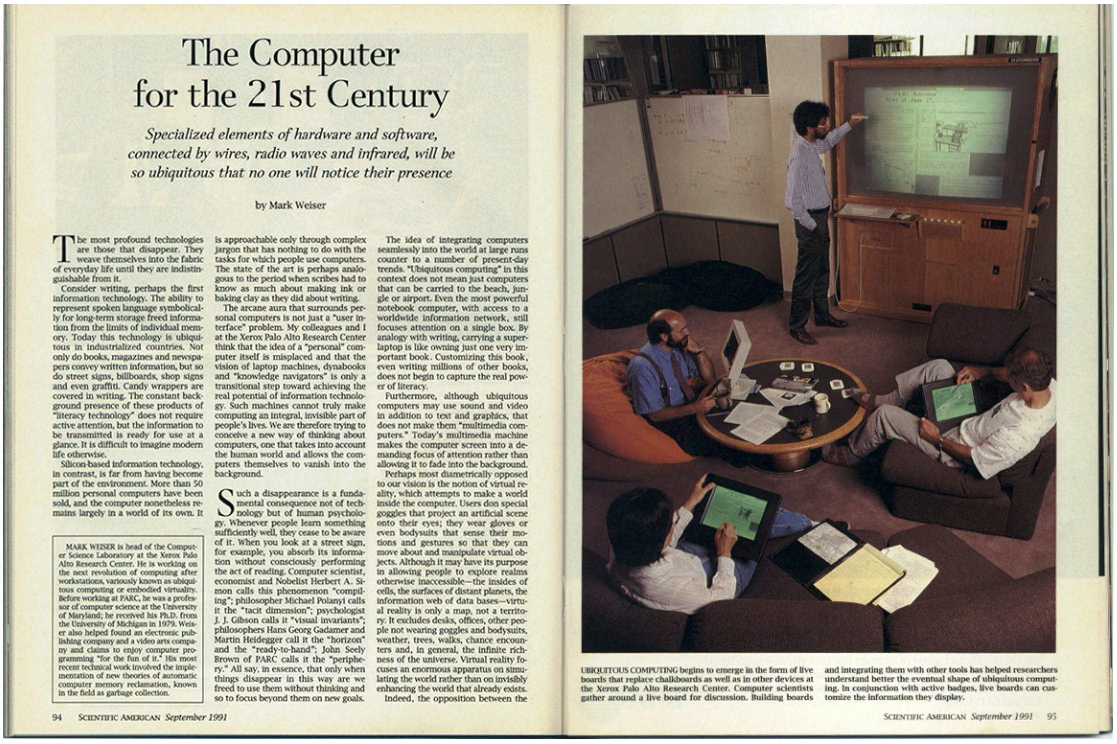
While the notion of the smart home is then to be found in fiction throughout the 20th century, the precise term *smart home* comes from the building industry, when the American National Association of Home Builders (NAHB) formed a special interest group in 1984 called Smart House and subsequently published a book of the same name (Smith, 1988). While their primary concern was with the proliferation of appliances with embedded chips and smart wiring infrastructures, the book also indulges in some light design fiction. This includes a series of cartoon scenarios in which a character is seen to intervene to keep children, the sight-impaired or elders safe from the hazards of the home – presumably enabled by some surveillant system.

Subsequentially corporate and academic efforts to prototype the smart homes of the future have frequently built living laboratories, home-like environments into which new technologies are installed and participants are invited to act out everyday life, sometimes for extended periods. Curiously the popularity of these laboratories seems to have peaked at the turn of the 21st Century (Mozer, 1998; Kidd et al., 1999; Harper, 2001; Intille, 2002; Randall, 2003) and Richard Harper's book Inside the Smart House offers some reflections on this period (Harper, 2003). These were often paternalistic smart homes, motivated to provide care or be supportive in the daily lives of occupants. Georgia Institute of Technology's Aware House (Kidd et al., 1999), aspired to: support social connections, support everyday cognition and identify potential crisis situations. Microsoft's EasyLiving environment (Shafer et al., 1998) anticipates that, "*One attractive application […] is to aid in caring for a child or a pet.*" As described in Chapter Two, such smart homes are framed in a tradition of assistive technologies where people can live independently; latterly there has been more focus on particular needs including dementia (Orpwood *et al.*, 2005) and loneliness (Austin *et al.*, 2016).

These paternalistic smart homes all require some contextual awareness of the occupants, without their explicit instruction through passive (and typically hidden) sensing. In the case of the University of Colorado's Neural Network House (Mozer, 1998) this was achieved by simple motion detection technologies and statistics like room temperature; while in Microsoft's EasyLiving (Shafer et al., 1998) cameras were processed by computer vision algorithms to understand the scene. Through such ubiquitous sensing, the machine silently and invisibly surveils the home. In contrast, Alex Taylor and Richard Harper with colleagues at Microsoft Research's Socio-Digital Systems group proposed *Homes that Make Us Smart*; "*It is this thinking, in the hearts and the minds of the occupants, that should make a home smart and not the technology embedded within.*" (Taylor *et al.*, 2007, p. 392). Ways of making such alternative speculations visible are explored in the second half of this chapter.

Meanwhile, outside academic, corporate and cinematic fantasies, bespoke smart homes were built for the extremely wealthy as signals of their power and status – in much the same way as technologies had been showcased in Victorian country homes. Microsoft's founder, Bill Gates' home, a mansion overlooking Lake Washington and completed in 1997, is a good example (Corcoran and Schwartz, 1997). Gates had previously described the project in his 1995 book *The Road Ahead* (Gates and Ottavino, 1995), which was accompanied by an interactive CD-ROM and a virtual tour of the 3D architectural computer model. According to the film's narrator, "*Another key building material is silicon. A hundred microcomputers and the software that controls them will let you experience the home without having to pay any attention to the technology at* *its heart.*" The operation of the home is to be hidden. The home function is to ensure the comfort of occupants; no domestic labour, not even food preparation, is to be seen in the film. The principle enabling technology is said to be, "*A special pin that uniquely identifies you and connects you to the home's electronic services, which will automatically adapt themselves to you and your tastes. As you move through the home the pin that you've programmed allows you to hear your choice of music on the information appliance nearest you, even as people in different rooms listen to their own favorites.*" Personal heating and lighting preferences are also matched. The design intention seems to be that each individual might experience their own isolated reality in which the lives of others are largely unseen. The smart home has no personifying character; the intentions and workings of the all-seeing home are invisible.

The smart home has then been an influential fantasy and it is hard to establish the technical reality of Gates' house or how its beta technologies have responded to change over the years. These showroom houses are a unique opportunity to envision and build a complete proprietary domestic system from the ground up, but in Brand's terms, without incremental adaption, they may struggle to learn and ultimately fail. Functional or not, the technologies of Gates' smart home, described as pins (or badges) and information appliances, reference an influential thread of HCI research, namely Ubiquitous Computing, which implicates forms of machine surveillance.



The Computer for the 21st Century

Specialized elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous that no one will notice their presence

by Mark Weiser

The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.

Consider writing, perhaps the first information technology. The ability to represent spoken language symbolically for long-term storage freed information from the limits of individual memory. Today this technology is ubiquitous in industrialized countries. Not only do books, magazines and newspapers convey written information, but so do street signs, billboards, shop signs and even graffiti. Candy wrappers are covered in writing. The constant background presence of these products of "literacy technology" does not require active attention, but the information to be transmitted is ready for use at a glance. It is difficult to imagine modern life otherwise.

Silicon-based information technology, in contrast, is far from having become part of the environment. More than 50 million personal computers have been sold, and the computer nonetheless remains largely in a world of its own. It is approachable only through complex jargon that has nothing to do with the tasks for which people use computers. The state of the art is perhaps analogous to the period when scribes had to know as much about making ink or baking clay as they did about writing.

The arcane aura that surrounds personal computers is not just a "user interface" problem. My colleagues and I at the Xerox Palo Alto Research Center think that the idea of a "personal" computer itself is misplaced and that the vision of laptop machines, dynabooks and "knowledge navigators" is only a transitional step toward achieving the real potential of information technology. Such machines cannot truly make computing an integral, invisible part of people's lives. We are therefore trying to conceive a new way of thinking about computers, one that takes into account the human world and allows the computers themselves to vanish into the background.

Such a disappearance is a fundamental consequence not of technology but of human psychology. Whenever people learn something sufficiently well, they cease to be aware of it. When you look at a street sign, for example, you absorb its information without consciously performing the act of reading. Computer scientist, economist and Nobelist Herbert A. Simon calls this phenomenon "compiling"; philosopher Michael Polanyi calls it the "tacit dimension"; psychologist J. J. Gibson calls it "visual invariants"; philosophers Hans Georg Gadamer and Martin Heidegger call it the "horizon" and the "ready-to-hand"; John Seely Brown of PARC calls it the "periphery." All say, in essence, that only when things disappear in this way are we freed to use them without thinking and so to focus beyond them on new goals.

The idea of integrating computers seamlessly into the world at large runs counter to a number of present-day trends. "Ubiquitous computing" in this context does not mean just computers that can be carried to the beach, jungle or airport. Even the most powerful notebook computer, with access to a worldwide information network, still focuses attention on a single box. By analogy with writing, carrying a super-laptop is like owning just one very important book. Customizing this book, even writing millions of other books, does not begin to capture the real power of literacy.

Furthermore, although ubiquitous computers may use sound and video in addition to text and graphics, that does not make them "multimedia computers." Today's multimedia machine makes the computer screen into a demanding focus of attention rather than allowing it to fade into the background.

Perhaps most diametrically opposed to our vision is the notion of virtual reality, which attempts to make a world inside the computer. Users don special goggles that project an artificial scene onto their eyes; they wear gloves or even bodysuits that sense their motions and gestures so that they can move about and manipulate virtual objects. Although it may have its purpose in allowing people to explore realms otherwise inaccessible—the insides of cells, the surfaces of distant planets, the information web of data bases—virtual reality is only a map, not a territory. It excludes desks, offices, other people not wearing goggles and bodysuits, weather, trees, walks, chance encounters and, in general, the infinite richness of the universe. Virtual reality focuses an enormous apparatus on simulating the world rather than on invisibly enhancing the world that already exists.

Indeed, the opposition between the

MARK WEISER is head of the Computer Science Laboratory at the Xerox Palo Alto Research Center. He is working on the next revolution of computing after workstations, variously known as ubiquitous computing or embodied virtuality. Before working at PARC, he was a professor of computer science at the University of Maryland; he received his Ph.D. from the University of Michigan in 1979. Weiser also helped found an electronic publishing company and a video arts company and claims to enjoy computer programming "for the fun of it." His most recent technical work involved the implementation of new theories of automatic computer memory reclamation, known in the field as garbage collection.

94 SCIENTIFIC AMERICAN *September 1991*

UBIQUITOUS COMPUTING begins to emerge in the form of live boards that replace chalkboards as well as in other devices at the Xerox Palo Alto Research Center. Computer scientists gather around a live board for discussion. Building boards and integrating them with other tools has helped researchers understand better the eventual shape of ubiquitous computing. In conjunction with active badges, live boards can customize the information they display.

SCIENTIFIC AMERICAN *September 1991* 95

Figure 9. The Computer for the 21st Century.

© Scientific American (text) and Matthew Mulbry (photograph) 1991. Used with permission.

The Disappearing Computer: Ubiquitous Computing

Ubiquitous Computing (Ubicomp) is a vision for interactivity that was proposed by researchers at Xerox PARC in the late 1980s and early 1990s, it has since become synonymous with the smart home and explicitly manipulates the visibility of work. Ubicomp was introduced by Mark Weiser in his article *The Computer for the 21st Century*, in the popular science magazine Scientific American (see Figure 9). Weiser starts, "*The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.*" (Weiser, 1991). The Ubicomp vision is pervasive in academia to this day – according to Google Scholar metrics, Weiser's article has been cited more than 18 thousand times since 1991 and over 500 times between 2021 and 2022. Ubicomp and Weiser have a peculiar veneration in the academic HCI community after 30 years, which Paul Dourish and Genevieve Bell first highlighted nearly 15 years ago (Bell and Dourish, 2006). Indeed by 2012, Gregory Abowd had declared that, "*ubiquitous computing, the third generation of computing, is here and no longer requires special attention, as its ideas and challenges spread throughout most of computing thought today.*" (Abowd, 2012, p. 31). Abowd is a computer scientist who initiated the previously discussed Aware Home research program at Georgia Institute of Technology (Kidd et al., 1999). He concludes, "*This spread cannot be reversed, and it results in the disappearance of ubicomp's intellectual agenda as it seeps into almost all aspects of the computing intellectual agenda.*" (Abowd, 2012, p. 38). This is extraordinary. Abowd's language of generations seeks to establish and stabilise Ubiquitous Computing, to make it disappear and remove any intellectual challenge to it – rendering Ubicomp hegemonic.

This section gives a detailed account of the domestication and popularisation of the idea of Ubicomp by identifying some of the characters who have shaped it over the past thirty years and who strikingly bear a good deal of resemblance to each other. The intention is to disclose the ways in which Ubicomp speaks directly to notions of invisible work and to develop the academic HCI landscape to which the second part of this chapter will respond with alternatives.

Mark Weiser - Ubiquitous

In introducing the vision of Ubicomp Mark Weiser described a series of early exemplars at three physical scales: boards, interactive displays approximately one meter in size; pads, hand-held devices approximately ten centimetres in size and tabs, wearable devices approximately one centimetre in size (Weiser, 1991). These were display surfaces, capable of rendering information and sensing interactions. In Ubicomp the computer was to be explicitly located and embodied in the environment; worn tabs would allow the computer to reason spatially about people too. As Weiser says, "*doors open only to the right badge wearer, rooms greet people by name, telephone calls can be automatically forwarded to wherever the recipient may be, receptionists actually know where people are, computer terminals retrieve the preferences of whoever is sitting at them, and appointment diaries write themselves."* (Weiser, 1991). The computer is then an integrated network of interoperating devices with a shared datastore – an infrastructure – a radically different world to that experienced by a typical reader of Scientific American in 1991. Very few technical details of the system are disclosed in the article and one might suggest that early descriptions of Ubicomp were published in more popular, less academic settings to allow them a degree of ambiguity and perhaps corporate confidentiality.

Ubiquitous Computing was firmly grounded in the work of Xerox PARC from the 1970s. Founded in 1969 PARC had established its reputation primarily through its demonstration to Steve Jobs of the Xerox Alto's graphical user interface in 1979, which was then adopted by the first Apple Macintosh in 1984. However, when Mark Weiser arrived at PARC in 1987 it was Alan Kay's Interim Dynabook pad computing concept (Kay, 1972) and Bob Metcalfe's invention of Ethernet Local Area Networking (LAN) in 1973 (Severance, 2013) that had the most resonance with Ubicomp – although by this time both Kay and Metcalfe had long departed PARC.

In later reflections on this period of development, accounts are clearer about the technologies the team at Xerox PARC had developed (Weiser, Gold and Brown, 1999): LiveBoard was a large interactive wall display, at the board scale; ParcPad (later called the MPad) was a book-sized device, at the pad scale; and ParcTab was palm-sized aspiring to be at the smaller tab scale (Want et al., 1995). In many ways Xerox PARC's Ubicomp program was necessarily as concerned with the construction of technical infrastructure as it was with devices. As Roy Want (Weiser's colleague) states, "*Attaining the goals of Ubiquitous Computing will require a highly sophisticated infrastructure. In the ideal system, a real-time tracking mechanism will derive the locations and operational status of many system components and will use that context to deliver messages more intelligently.*" (Want *et al.*, 1995, p. 3). The indoor location system, through which boards, pads and tabs (and so people) were tracked in the building, was a development of Want's earlier Active Badge system at Olivetti (Cambridge, UK) (Want *et al.*, 1992). Wireless networking used a bespoke infrared system of beacons in known fixed positions, interconnected via a wired Ethernet backbone. The experience of the Ubicomp vision made considerable infrastructural demands of the built environment; indeed, Ubicomp fundamentally seeks to be infrastructure. In Weiser's first internal articulation of Ubicomp at Xerox

PARC in 1988, he said, "*It is invisible, everywhere computing that does not live on a personal device of any sort, but is in the woodwork everywhere.*" (Weiser, 1996b). In Shearing Layer terms, this vision is beyond merely the Stuff of electronic gadgetry and intervenes in the slower layers of the built environment.

The function of this ubiquitous infrastructure is then ubiquitous surveillance, the more context that is known to the system the more functionality the system can provide; Ubicomp is then predicated on an invisible infrastructure that surveils people and stuff. Weiser understood the potential consequences of this from the start, "*overzealous government officials and even marketing firms could make unpleasant use of the same information that makes invisible computers so convenient.*", (Weiser, 1991).

While the early demonstrations of Ubicomp were focused on the office and productivity, Weiser's Scientific American article of 1991 offers some speculations about domestic ubiquitous computing. The piece included a short fictional account of the life of Sal; who wakes up in her Ubicomp home, before commuting to work. The scenarios are scarcely described in a few words, with glimpses of tangible interactions with unseen devices – it seems Weiser's vision is deliberately kept at a low fidelity to make it open to interpretation. At home Sal's interactions orchestrate her family, maintain the home and accomplish microtasks of work; with the exception interestingly of the neighborhood map, which shows electronic trails "*of neighbors coming and going during the early morning*" and "*let[s] Sal feel cozy in her street*" (Weiser, 1991). Later Weiser wrote an article for New York University's Interactive Telecommunications Program's Review Magazine that applied a Ubicomp agenda to the home, in which he said, "*the 'Smart House' of 2005 will have computers in every room. But what will they do? […] We will dwell with these computers, whose presence we will ignore most of the time, and they will provide us with constant clues about our environment, our loved ones, our own past, the objects around us and the world beyond our home. […] A house that is true to its house nature must have a certain quiet, even stolidness. Through a thousand subtle cues, computers will help turn our houses into homes.*" (Weiser, 1996a).

Ubicomp is today commonly understood by the apparent *ubiquity* of computing resources (and network technologies). "*The first wave of computing, from 1940 to about 1980, was dominated by many people serving one computer. The second wave, still peaking, has one person and one computer in uneasy symbiosis, staring at each other across the desktop without really inhabiting each other's worlds. The third wave, just beginning, has many computers serving each person everywhere in the world. I call this last wave 'ubiquitous computing' or 'ubicomp'."* (Weiser, 1996a). Yet, this insistence on everything, everywhere, all the time seems to deny scarcity and the realities of struggle.

Weiser's conceptualisation of invisibility is then also slippery; at once he suggests the troupe of invisible labour, "*…like the wires in the walls, these hundreds of computers will come to be invisible to common awareness. People will simply use them unconsciously to accomplish everyday tasks.*" and then, "*disappearance is a fundamental consequence not of technology, but of human psychology*", citing Heidegger's *ready-to-hand* – which frames visibility as a question of attention (Weiser, 1991). Writing subsequentially in an ACM Interactions magazine article, he clarifies, "*A good tool is an invisible tool. By invisible, I mean that the tool does not intrude on your consciousness; you focus on the task, not the tool.*" (Weiser, 1994b) and "*the most powerful things are those that are effectively invisible in use"* attributed to (Weiser, 1994a). The notion of being invisible in use was subsequently developed by Peter Tolmie and colleagues as *Unremarkable Computing* (Tolmie et al., 2002) and reflects the experience of Mr Mathias' Push-Button Manor (Railton, 1950).

Matthew Chalmers reports that by 1994 and 1995 Weiser was advocating for seamful systems with "*beautiful seams*" rather than simply being seamless and invisible (Chalmers and MacColl, 2003). Chalmers' conceptualisation of seamful design, applied to the seams of wireless data networks and location technologies like GPS (Broll and Benford, 2005), would later be considered by Kristina Höök and Jonas Löwgren as one of HCI's *strong concepts* (Höök and Löwgren, 2012). Weiser's vision of ubicomp has a degree of ambiguity that constructs these seeming contradictions and yet continues to recruit devotees.

Donald Norman - Invisible

In Donald Norman's book *The Invisible Computer* (Norman, 1998), he outlines the ways in which computers can be made convenient, easy to use and pleasurable through interaction design; by rendering their complexities invisible. While this book is often read as a ubicomp text, it curiously contains no reference to Ubiquitous Computing or Mark Weiser, with which it seems in clear dialogue. Instead, Norman draws exclusively on Jef Raskin's earlier conception of the *Information Appliance* – a narrowly defined device as easy to use as a home appliance.

Norman reports that Raskin had originally coined the term Information Appliance in an internal document at Apple in 1978; this at about the same time he conceived the original Macintosh project, which he saw as an exemplar of this vision. Norman's retrospective definition of an information appliance is given as, "*An appliance specializing in information: knowledge, facts, graphics, images, video, or sound. An information appliance is designed to perform a specific activity, such as music, photography, or writing. A distinguishing feature of information appliances is the ability* *to share information among themselves.*", (Norman, 1998, p. 53). In regard to sharing information, appliances are then not existentially reliant on network infrastructure but do reach beyond themselves to some useful effect. As noted, Bill Gates would also adopt the term information appliance to describe the domestic terminals in his mansion, but here the network is essential (Gates and Ottavino, 1995).

While Norman's book concludes with a speculation of how computing will become embedded into the fabric of everyday life, in the walls, as objects, in our clothes and in our bodies – it is principally concerned with computing appliances as an alternative to then-dominant desktop PC. Contemporary examples of commercial information appliances might include the Apple Newton (1993) and latterly the Apple iPod (2001). It is not the computer that is invisible, but the complexity of its work. In Shearing Layer terms, an information appliance is Stuff, rather than the infrastructural Services of Ubicomp. Norman's influential popularisation of J. J. Gibson's ecological account of visual perception (Gibson, 1979; Norman, 1988), describes the affordances of everyday things and with Bill Gaver's application to technological things (Gaver, 1991), offers a way to design such tangible digital Stuff.

Hiroshi Ishii – Tangible

In 1995 Hiroshi Ishii moved from NTT (Nippon Telegraph and Telephone Corporation) in Tokyo, where he had become established in the research field of CSCW (Computer Supported Cooperative Work), to the MIT Media Lab where he founded the Tangible Media Group. At MIT he became (and remains) one of the most enthusiastic proponents of Weiser and his vision. After Weiser's early death in 1999, Ishii offered him a tribute by way of an installation of bottles that were containers of sound, "*The bottles illustrates Mark Weiser's vision of the transparent (or invisible) interface that weaves itself into the fabric of everyday life.*" (Ishii, 2004, p. 1299). Ishii's framing of Ubicomp emphasizes the invisibility and seamlessness qualities of the interaction, whilst being focused on the manipulation of things in the physical world entangled with Tangible Bits (Ishii and Ullmer, 1997).

Around 1998, Ishii's Tangible Media Group adopted the word ambient to describe their technologies as a way too to negotiate this tension in their work; between what is tangible and physical, what is digital and what is invisible. The ambientROOM (Ishii et al., 1998) was a system of devices that instrumented a room and displayed ambient media: lighting, sound, graphical displays and phicons (or physical icons); that rendered real-time sensor data drawn from beyond the workspace. Ambient also describes the defused ubiquity of these technologies. The visual and aural qualities of this ambient media suggest the influence of the ambient music genre, popularised in the 1970s by Brian Eno, Stewart Brand's long-term collaborator[29]. Other projects from Ishii's group described as ambient include: Ambient Fixtures (Wisneski et al., 1998), Water Lamp and Pinwheels (Dahley, Wisneski and Ishii, 1998), Personal Ambient Display (Wisneski, 1999) and LumiTouch (Chang et al., 2001). While the majority of the group's work was focused on tangible computational Stuff, projects such as ambientROOM and John Underkoffler's Luminous Room (Underkoffler and Ishii, 1999), explored ways of embedding infrastructural intelligence into the architectural space.

By 1997 Weiser had become uncomfortable with the ways in which Ubicomp and ubiquity were being understood. In a private message to Hiroshi Ishii and Brygg Ullmer at MIT, responding to their CHI paper *Tangible bits: Towards seamless interfaces between people, bits and atoms* (Ishii and Ullmer, 1997), Weiser wrote, "*My request is that you help me stop the spread of misunderstanding of ubiquitous computing based simply on its name. Ubicomp was never just about making 'computers' ubiquitous. It was always, like your work, about awakening computation mediation into the environment. […] I have started to talk about Calm Technology as a theme, but it better names a goal than a research project. 'Tangible Bits' is very nice, and maybe could serve as an overall umbrella*" (Ishii, 2004, p. 1310). Weiser's use of calm attempts to reconstrue invisibility, which he had previously coined in an article for the PowerGrid Journal written with John Seely Brown (Weiser and Brown, 1995). Calm is a matter of attention rather than of absence – their example of Natalie Jeremijenko's Live Wire (1995) is present and occupies space, it is not invisible but calm and undemanding.[30] Calm is articulated with reference to Norman, "*For us the term 'affordance' does not reach far enough into the periphery where a design must be attuned to but not attended to.*" (Weiser and Brown, 1995). However, for Yvonne

[29] Brian Eno and Stewart Brand have worked together through projects such as the Long Now Foundation (01996). The slow calm ethos of Eno's ambient music has resonances in Brand's Shearing and Pace Layers.

[30] Live Wire (also known as Dangling String) wiggles a long suspended wire with a motor to indicate the volume of network traffic; it was built by Natalie Jeremijenko in 1995 while she was a visiting researcher at Xerox PARC in collaboration with Weiser (Ishii and Ullmer, 1997). It is hard to know how calm the experience really was – how violently the string could move or how loud it was. Similarly, at Xerox PARC in 1999 Weiser's collaborator Roy Want built the Internet Stock Fountain, which indicated stock prices by controlling the height of water columns (Simanowski, 2011). While Live Wire is often cited as one of the earliest things on the Internet, neither contribute to the network, they only observe it.

Rogers calm is a misstep and Ubicomp should instead be about "*engaging rather than calming people*", where there is a move from "*proactive computing to proactive people*" (Rogers, 2006) – a clear rebuke to the paternalistic smart home.

In 2000, Underkoffler left the MIT Media Lab to become the science advisor for Stephen Spielberg's film *Minority Report* (2002), where he would define one of the most popular contemporary visions for gestural computing (Beaumont, 2003). This was a necessarily a large-scale cinematic system, using gloves for hand tracking to manipulate multimedia data on large displays; Weiser's Ubicomp concepts of boards, pads and tabs are clearly recognisable[31].

Neil Gershenfeld – Thinking

The Things that Think Consortium was formed in 1995 at the MIT Media Lab as a means to share intellectual property, including the work of Ishii's Tangible Media Group, with corporate sponsors.[32] The research agenda was articulated by the consortium's co-director Neil Gershenfeld's book *When Things Start to Think* (Gershenfeld, 1999) and describes a world where everyday things are invisibly embedded with computation. However, there is no mention of Weiser's Ubiquitous Computing, nothing of Raskin's Information Appliance or even Ishii's tangible bits or ambient media. Despite a forward written by PARC's John Seely Brown, Calm Technology is also absent. It is a very curious book. Rather than speculating about large scale networks of things, it is much more orientated towards wearables and Personal Area Networks (PANs). Nevertheless, Gershenfeld would prove to be influential in the conceptualisation of the Internet of Things.

Kevin Ashton – Sentient

In 1999, Kevin Ashton of Procter & Gamble co-founded the Auto-ID Center at MIT, one of a global federation of research groups exploring applications of RFID (Radio-Frequency IDentification) tags – a compact technology for proximate wireless identification, that needs no batteries and can be inexpensively produced at scale. That same year Ashton had started to popularise the term Internet of Things (IoT) in relationship to RFID, describing it as a way by which the network could capture data about things in the real world and by which the Internet could achieve some sentience

[31] From the success of Minority Report, Underkoffler founded a company called Oblong to develop working versions of these technologies, which became known as the g-speak spatial operating environment. However, g-speak did not find a mass market, due in part perhaps to its demands on the architectural space (Boutin, 2011).

[32] The Things that Think Consortium ran until 2014.

(Ashton, 2009). Ashton's Internet of Things was primarily a tool for multinational companies (such as Procter & Gamble) concerned with managing large highly complex international supply chains of valued commercial goods. The technology of RFID allowed the flow of things through a corporate supply chain to be tracked in minute detail and in real-time; it is a technology for disclosing the complexity of a system down to its individual components. However, it was conceived as a logistics technology, not a domestic technology.

Ashton's RFID-based IoT is fundamentally a thing-oriented technology where things are responsible for identifying themselves by producing on demand a unique identity number, and perhaps some sensed quality about their environment. Things are made sense of by a technical assemblage of tag readers, databases of ID codes and a telecommunication network. Things cannot reason or make connections for themselves and can only see the world from their own perspective. Without this assemblage the tag has little utility, but the thing's integrity is not reliant on the network's presence.

In reflecting on this period Ashton makes explicit the connection between both Gershenfeld's Things That Think and Weiser's Ubiquitous Computing, "*Neil's work at that time was not especially focused on networking, but he had a good early take on the potential value of embedding computers and sensors into everyday devices, as did other researchers working in a field then called embedded computing, and now more commonly known as ubiquitous computing.*" (Ashton, 2016). However, while Ubicomp and IoT are both predicated on tagging and tracking to observe the reality of the world, they differ in their orientation to and dependence on infrastructure.

Over the past twenty years Ashton's Internet of Things has come to be collectively imagined commercially and academically quite differently than first intended – frequently in a domestic context. The term has come to evoke things that interact and actuate, as well as sense – things that are on the Internet and typically existentially dependent on the network. It is difficult to assert exactly when IoT became synonymous with Weiser's infrastructural Ubicomp, but by 2009 Ashton was acknowledging that his concept was becoming misunderstood (Ashton, 2009) – just as Weiser had complained before him.

David Rose - Enchanted

In 2001 Hiroshi Ishii's concept of ambient and related projects was spun-out of the MIT Media Lab as the company Ambient Devices by David Rose (Felberbaum, 2004). In 2002 the company launched their first consumer product the Ambient Orb; a sphere that was lit with a coloured light reflecting a configurable real-time data source obtained by the cellular data network – for instance displaying a warmer colour for warmer weather. Ambient Devices still trades twenty years later, with a range of information displays, principally concerned with home energy use; Ishii remains an adviser to the company (Ambient Devices, 2020). In early press interviews Rose explicitly referenced the vision of Weiser's Ubicomp (Felberbaum, 2004) with the moniker of the Internet of Things being adopted much later (Rose, 2014).[33]

In 2003, the French company Violet launched the DAL lamp, similar to Ambient Devices' orb, but with WiFi connectivity (Rojas, 2004). The lamp retailed at €800 and was described as calm – it sold in but in small numbers (Violet Dal, the first "emotional lamp", 2004). However, in 2005 Violet had initial commercial success with the launch of the Nabaztag, *the Internet connected rabbit*, followed by the Nabaztag:tag in 2006 (Turi, 2014). The original Nabaztag made considerable innovations beyond the previous ambient lamps; it could communicate by the position of its actuated ears and through a speaker with a synthesized voice or music, as well as with coloured lights. By *marrying* pairs of rabbits, moving of the ears of one would be mechanically reflected by the other across the network – by which means a kind of intimate semaphore language might develop between separated partners. The later Nabaztag:tag could be instructed by voice commands and interact with objects tagged by RFID. In 2009, despite early commercial promise, Violet filed for bankruptcy and when the servers shut down Nabaztags everywhere stopped working (Le Meur, 2009). Ambient Devices' Ambient Orb and Violet's Nabaztag created the first wave of commercially available domestic things on the Internet.

[33] As briefly noted in Chapter One, Ambient Devices' first products used the mobile pager network, giving it robust and easily configured wireless Internet connectivity (Feder, 2003).

In 2014, David Rose of Ambient Devices, published a book called *Enchanted Objects: Design, Human Desire, and the Internet of Things* (Rose, 2014). The prologue describes Rose's nightmare of what he characterises as a Corbusian Utopia with "*no furniture and no objects*". The book makes an equivalence between the tradition of Weiser's calm, Ishii's ambient and Ashton's Internet of Things; which was doubtless by then commonly understood. However, Rose's use of enchantment renders complexity not as invisible or even simply outside of our attention, but as magical and inscrutable. Furthermore, Rose claims that this enchantment can uniquely satisfy human desires. Citing Aristotle, Hobbes, Darwin, Freud, Maslow and Myers-Briggs, he claims to have identified, "*a set of human desires that I believe are fundamental and universal, and that deserve the focus of product designers and entrepreneurs and companies*" (Rose, 2014, p. 66). These being:

> **Omniscience**. This is the desire to have great knowledge. We have a voracious appetite to know as much as possible and to know about things that go beyond facts and information. We would love to be able to predict what will happen in the future.
>
> **Telepathy**. We have a powerful desire to connect to the thoughts and feelings of others, and to be able to communicate with ease, richness, and transparency. We want to know others and to feel known by them.
>
> **Safekeeping**. We fervently wish to be protected from harm. To feel comfortable, safe, and at ease.
>
> **Immortality**. We want to be healthy, strong, fully capable. We dream of living long lives, vital to the last moment.
>
> **Teleportation**. We crave movement, to be transported easily and swiftly and joyfully from one place to another, and to live unconstrained by physical limits or boundaries.
>
> **Expression**. We all wish to be generative, to fully express ourselves in many forms and media—acting, music making, art, writing, cooking, dancing, documenting our lives.

Enchanted Objects (Rose, 2014, pp. 66–67)

While this may be hyperbolic, it also seems a genuine attempt to disclose the priorities and assumptions embedded in these connected comercial products. Furthermore, those domestic IoT products with sustained popularity, do seem to address at least some of these desires or drives; consider the Amazon Echo assistant (omniscience) or the Google Nest security camera (safekeeping). Rose's book is not a rigorous academic argument; indeed, these desires do not seem to necessitate enchantment. Instead, the book is an articulation of something nonetheless present, a hegemony of cultural imagination adopted by many engineers – who in turn build with these values. Rose is clear about this too, "*What's the secret to creating technology that is attuned to the needs and wants of humans? The answer can be found in* *the popular storeys and characters we absorb in childhood and that run through our cultural bloodstream; Greek myths, romantic folktales, comic book heroes, Tolkien's wizards and elves, Harry Potter's entourage, Disney's sorcerers, James Bond, and Dr. Evil. They all employ enchanted tools and objects that help them fulfil fundamental human drives. In this book I link the fictions and fantasies that so beautifully expressed these desires and the role of modern inventions."* (Rose, 2014, pp. XI–XII). Not to mention endless allusions to Roddenberry's Star Trek (1966).

While Rose's enchantment is seemingly engaged in a rich cultural dialogue, on closer inspection there is very little criticality, and this becomes problematic. The heroic individual empowered by these tools is easily read through a lens of Ayn Rand's amoral objectivism or Friedrich Nietzsche's superman – James Scott made this parallel clear in his article *UbiComp: Becoming Superhuman* (Scott, 2005). Rose's case for enchantment relies on the tirelessly repeated crux of Arthur C. Clarke's "*Any sufficiently advanced technology is indistinguishable from magic.*" (Clarke, 1962). Yet at its heart there is a logical contradiction – the desire for omniscience or "*to know as much as possible*" implies that a magical explanation of enchantment is insufficient. With a magic trick there is a sleight of hand and a secret to be understood, but not with enchantment. Omniscience should disclose the hegemony making work visible, but enchantment makes it not just unseen but unknowable.

Conclusion

Through this account of the Disappearing Computer and Ubiquitous Computing, some of the divergent ways it has been used to speak about invisibility in HCI has been shown; be that ambient, calm, unremarkable or even enchanted. Some render work with greater invisibility than others, but there is little questioning of the necessity for machine surveillance and its aspiration for these technologies to become home infrastructure – which is problematic. Overall, this first part of the chapter has taken an inclusive historic perspective on the automated home, from the 19th Century country homes to modern times. In doing so it has demonstrated how work has been rendered invisible by the technologies of the pull-cord, push button, utility service, computer and network. The desire to make the complexities of the home invisible or at least at the periphery of awareness, for the sake of simplicity has been the implicit theme of this section and yet as the feminist Invisible Work discourse shows this can be extremely problematic. The second part of this chapter will respond with alternative ways to approach domestic design that instead makes work visible.

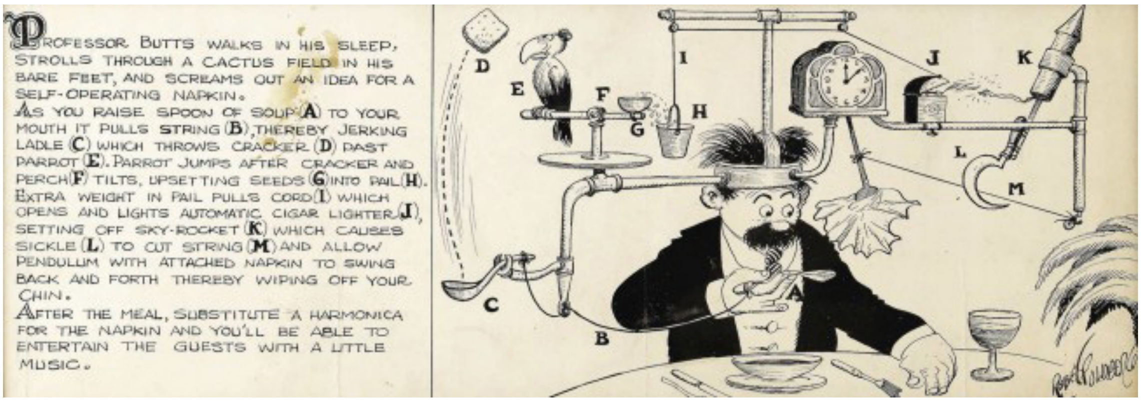
Part Two: The Visibility of Alternatives

This final part of the chapter suggests some starting points for design alternatives – as Anderson puts it to open the *play of possibilities* (Anderson, 1994). These alternatives should make struggles with the networked home visible, challenge an uncomplicated narrative and make the work on which the home relies more apparent. As a comic counterpoint the machines of Rube Goldberg are first discussed, then I have selected three influential texts (Dunne, 2006; Bell, Blythe and Sengers, 2005; Taylor and Swan, 2005) as jumping-off points to discuss a wider range of theories that are relevant to developing design tactics. These tactics relate to current speculative HCI and design research discourses that describe material and ecological exploratory methods to make the invisible visible – to see alternatives that were previously unseen. These methods will be refined and elaborated in Chapter Four for the purposes of this thesis. Unfamiliar outcomes will likely require unfamiliar methods.

This is not a comprehensive academic literature review of HCI's involvement in the home, for which the reader should turn to works like Desjardins, Wakkary and Odom's seven genres of domestic technology research (Desjardins, Wakkary and Odom, 2015).

Goldberg Variations

While the automated home has been largely imagined and experienced through invisible work, a different kind of automation has also been part of the popular discourse – those of the illustrated mechanisms of Heath Robinson (1912) and Rube Goldberg (1928) and their cinematic counterparts (often curiously as breakfast-machines) that include: *Chitty Chitty Bang Bang* (1968), *The Goonies* (1985), *Pee-wee's Big Adventure* (1985), *Ferris Bueller's Day Off* (1986), *Wallace and Gromit: A Grand Day Out* (1989) and *Home Alone* (1990). These whimsical DIY contraptions have served as comic relief to the corporate industrialised domestic narrative; but also seem to demonstrate an alternative relation to complexity. These are visible systems of chain-reaction networks, set in motion by some simple action (see Figure 10).



PROFESSOR BUTTS WALKS IN HIS SLEEP, STROLLS THROUGH A CACTUS FIELD IN HIS BARE FEET, AND SCREAMS OUT AN IDEA FOR A SELF-OPERATING NAPKIN.

AS YOU RAISE SPOON OF SOUP (A) TO YOUR MOUTH IT PULLS STRING (B), THEREBY JERKING LADLE (C) WHICH THROWS CRACKER (D) PAST PARROT (E). PARROT JUMPS AFTER CRACKER AND PERCH (F) TILTS, UPSETTING SEEDS (G) INTO PAIL (H). EXTRA WEIGHT IN PAIL PULLS CORD (I) WHICH OPENS AND LIGHTS AUTOMATIC CIGAR LIGHTER (J), SETTING OFF SKY-ROCKET (K) WHICH CAUSES SICKLE (L) TO CUT STRING (M) AND ALLOW PENDULUM WITH ATTACHED NAPKIN TO SWING BACK AND FORTH THEREBY WIPING OFF YOUR CHIN.

AFTER THE MEAL, SUBSTITUTE A HARMONICA FOR THE NAPKIN AND YOU'LL BE ABLE TO ENTERTAIN THE GUESTS WITH A LITTLE MUSIC.

Figure 10. Self-operating napkin. © Rube Goldberg Institute, 1931. Used under license.

While these machines might typically rely on cartoon or cinematic physics[34], one thing by inspection intuitively and predictably leads to the next. These are collectives of pulleys, flames and feather dusters; there is the occasional well-understood mechanical clock or instinctual pet, but otherwise there are no black boxes – everything is visible, nothing is smart. As Goldberg said, "*An illogical bunch of things which are put in a logical sequence*" [as reported by (Adelson, 2019)]. In DiSalvo's terms they are articulated networks of objects; a tangle of humans, stuff and other non-humans (DiSalvo, 2012). Indeed, the Victorian Country houses were mechanically articulated in much the same way as Goldberg's illustrations, with pulleys and cables; they are also not unlike the contraptions of Mr Mathias' Push-Button Manor, but nothing is hidden away behind the walls. Goldberg's machines start to suggest some ways to understand ecosystems of these things.

Making by Making Strange

To ground this discussion in relevant academic discourses, the first influential text is Genevieve Bell, Mark Blythe and Phoebe Sengers' *Making By Making Strange* (Bell, Blythe and Sengers, 2005). As they observe, "*Everyone is an expert on the home*" (Bell, Blythe and Sengers, 2005, p. 150) and such familiarity creates a tendency to "*passively propagate the existing politics and culture of home life*" through design (Bell, Blythe and Sengers, 2005, p. 169). Furthermore, ways of talking about home often emphasise its stability and permanence, as described in Chapter One, with Weiser stating, *"A house that is true to its house nature must have a certain quiet, even stolidness.*" (Weiser, 1996a). From this common-sense perspective then homes are

[34] There are many examples of these assemblages that do operate for real; for instance, in the film *The Way Things Go* (Fischli and Weiss, 1987), yet here the complexity and fragility of the system makes a single continuous shot of the action impossible – it too is made to work through skilfully edited film clips.

places in which the moral order of things is already established and understood, not where change is enacted.

In this paper Bell, Blythe and Sengers propose that unthinking design assumptions can be challenged by processes of defamiliarisation – specifically by engaging with comparative ethnographies of mundane domestic technologies and ecologies. Ethnography is then a means by which the hegemony can be (partially) revealed, made strange and so made visible. The authors make twelve statements outlining the challenges and strategies for designing strange home technologies, defamiliarised through their own ethnographic accounts of domestic life in international homes during the early years of the century:

> (1) Efficiency is overrated.
> (2) All tomatoes are not alike (and neither are users).
> (3) I am not my wallet.
> (4) Technology or user: Who's in charge?
> (5) No Home is an Island.
> (6) Homes are in communities; homes resist communities.
> (7) Gendered design legacies may be past their sell by-date.
> (8) The user is plural.
> (9) Not everyone has broadband.
> (10) There is an elephant in the room – pornography.
> (11) There is a ghost in the machine – spirituality.
> (12) Play is not the same as entertainment.

(Bell, Blythe and Sengers, 2005, pp. 166–169)

My reproduction here of this list of headings titles give these statements a quality somewhat like a manifesto for the strange; they can also be read in parallel to the struggles described in Chapter Two. For instance, *efficiency is overrated* speaks directly to *struggles to be productive*. However, making by making strange is concerned with the doing of design and suggestive of alternative perspectives. For my purposes, I find three strong resonances with ecologic, ludic and heterogenic discourses and methods. Each of these is first justified and then expanded in turn.

Ecologic

Making By Making Strange argues that, "*A historical and cultural analysis of American domestic technologies and ecologies is one way to defamiliarize the home*" (Bell, Blythe and Sengers, 2005, p. 157) and it can be straightforwardly read as making an ecological account of the home as a way of revealing the familiar. The science of ecology has developed over the past 100 years, pioneered by botanist Arthur Tansley and who defined the term *ecosystem* as a way of studying the interdependency of biological networks in the wild (Tansley, 1935). Ecological methods offer an alternative to traditions of scientific work where the subject of study is removed from the world and the phenomena isolated in the laboratory – instead, an ecological account will maintain a degree of necessary complexity, through a multiplicity of interactions in the network between entities in the environment that form the ecosystem. I shall first layout some broad ways to understand ecological philosophy and history, before returning to consider it domestically and in the context of HCI.

An ecological perspective necessarily requires a change of scale from the immediate and proximate, to the slow and interconnected – an act that makes the big picture visible. Indeed, the Blue Marble photograph of the whole earth, taken by the crew of Apollo 17 in 1972, is associated with the growth of the ecological/environmental movement in the 1970s and contributed to popular understandings of global ecosystems; it remains possibly the most reproduced photograph in history (Petsko, 2011; Reinert, 2011). By this time ecologies had become an influential way to talk about the nature of nature – that natural systems naturally seek balance and maintain stable equilibrium – for instance, in populations of predators and prey or global climate. Ecologists were routinely modelling the natural systems they observed as networks of formalised relationships between interconnecting entities. However, the notion of self-organising networks of free individuals, able to find stability without authoritarian power structures, demonstrated an alternative to the status quo that had a wide political influence; especially in the American countercultural hippie commune movement of the 1960s and 70s (Curtis, 2011a, 2011b).

One such free individual was Stewart Brand. Brand had studied biology and ecology at Stanford University graduating in 1960; it was he who had petitioned NASA in 1966, asking "*Why haven't we seen a photograph of the whole Earth yet?*", anticipating the popular impact it would have. Subsequently, NASA first published a whole Earth image taken by the ATS-3 weather satellite in 1967 and then the so-called Earthrise image was taken on the surface of the moon by astronaut Bill Anders in 1968; prior to the Blue Marble in 1972. Brand was active in the commune movement and in 1968 had published the first edition of the *Whole Earth Catalog* – with the ATS-3 photograph used as its cover. The Whole Earth Catalog was "*a how-to manual, a compendium, an encyclopaedia, a literary review, an opinionated life guide, and a collection of readers' recommendations and reviews of everything from computational physics to goat husbandry.*" (Cadwalladr, 2013). It was infused with ecological thinking from its use of whole Earth images to the inclusion of complex ecosystem diagrams. John Markoff, of the New York Times, would later describe it as, was "*the internet before the internet. It was the book of the future. It was a web in newsprint.*" (Cadwalladr, 2013). The Whole Earth Catalog became a countercultural bible for an alternative way of living.

Adam Curtis' argues in his documentary television series *All Watched Over by Machines of Loving Grace*, that ecological and countercultural thinking also profoundly shaped 20th Century computing and networking; from Wiener's cybernetic feedback loops in the 1940s and 50s, Engelbart's desktop computing of the 1960s and 70s and Berners-Lee's World Wide Web in 1989 (Curtis, 2011a). However, he claims that this ecological grounding was flawed. From the 1970s experimental work began to expose that, "*Tansley's idea of a underlying pattern of stability in nature was really a fantasy, not a scientific truth."* (Curtis, 2011b) borne out of gross simplifications of the observed natural world and with consequences for the stability of man-made self-organised systems – not least architecture. Brand's subsequent Shearing Layers model (Brand, 1995) addresses directly this question of the stability and adaption to change in buildings and draws on the work of other ecologists including architect Christopher Alexander (Alexander et al., 1977; Alexander, 1979). The Shearing Layers is an ecological idea, but one that explicitly acknowledges instability and struggle.

In the context of domestic HCI, it is easy to see the academic roots of Ubiquitous Computing and the Internet of Things in the ecological tradition. As Carl DiSalvo comments, "*The design of ubicomp is the design of connectedness. More than just exchange and expression between objects, this connectedness extends outward to enrol people, other entities in the environment, and even the environment itself.*" (DiSalvo, 2012, pp. 92–93). However, it is hard to see ecological thinking as being dominant more generally in the field of HCI. The ACM Special Interest Group on Computer-Human Interaction conference (or simply CHI) in particular has a tradition grounded in information processing models of cognition and laboratory-based ergonomic studies – where complexity is deliberately excluded to isolate phenomena and where *ecological validity* is then a concern. Nevertheless, a thread of ecological thinking has been long present at CHI. The *Ecological Perspectives in HCI* workshop at CHI 2015 dealt directly with this question and the call for participation reminded the community that, "*The concept of affordances, originating from the Gibsonian ecological psychology, is one of the first, and most central, HCI concepts.*" (Blevis *et al.*, 2015, p. 2402). This refers to Donald Norman and Bill Gaver's accounts of affordance (Norman, 1988; Gaver, 1991), drawing on J. J. Gibson's ecological concept of visual perception (Gibson, 1979). However, affordance here attends to the mind of the perceiver, rather than the ecological network. In Jodi Forlizzi's conception of *product ecologies* (Forlizzi, 2008) the ecology is rather more present. Previously in collaboration with Carl DiSalvo, they used an ecological approach to describe how a Roomba vacuum fitted into the ecology of the home (Forlizzi and DiSalvo, 2006).

Later at the Georgia Institute of Technology, DiSalvo's student Tom Jenkins introduced the notion of *object ecologies* both as a way to develop interrelated design spaces for everyday IoT, which he notably grounds in a Latourian understanding of objects and networks (Jenkins, 2015). In subsequent work, Jenkins applies this approach to the design of alternative IoT for cohousing, but here the ecological angle is more implicit (Jenkins, 2018). While the mainstream HCI community, Ubicomp and IoT in general have an uneasy ecological footing, some relevant work does acknowledge its ecological foundation and make some methodological waypoints.

The ecologic perspective is useful in making visible the uniqueness of each home – a reminder that *all tomatoes are not alike*. This inspires alternative designs that participate in and are accepting of these ecosystems, rather than attempting to impose some new externally defined logic.

Ludic

Making By Making Strange is acknowledged to be in ongoing dialogue with a tradition of critical and speculative work with its origins at the Royal College of Art's Computer Related Design Studio, that might be characterised as having a ludic outlook. In 2000, Bill Gaver and Heather Martin's *alternatives* workbook was a critique of domestic information appliances that "*tend to represent a narrow range of cultural possibilities, reinforcing a simple dichotomy between work and play*." (Gaver and Martin, 2000, p. 209). By 2005 and the formation of Interaction Research Studio at Goldsmiths, Gaver had been working with Andy Boucher, Sarah Pennington and Brendan Walker on the Equator project[35] since 2000. This six-year collaborative project culminated in the *Curious Home*, a series of workbook proposals and highly resolved research products installed in participants' homes over several months. All suggested alternative values for domesticated technologies, that "*do not have to reproduce our culture's preoccupation with work, consumption and entertainment*" (Beaver, Boucher and Pennington, 2007, p. 4). This sentiment is echoed in Making By Making Strange's statements that, *efficiency is overrated* (1) and *play is not the same as entertainment* (12) (Bell, Blythe and Sengers, 2005, pp. 166–169).

Drift Table is arguably the most iconic of these ludic designs; a coffee table presenting a porthole through which the British landscape appears to drift below, as if on a balloon ride (W. Gaver *et al.*, 2004). Gaver articulated this alternative design space as *ludic*

[35] The Equator Project was a six-year Interdisciplinary Research Collaboration (IRC), supported by the UK's EPSRC focussed on the integration of physical and digital interaction, running between 2000 and 2006.

design and through the Equator project and subsequent work at the Interaction Research Studio (Gaver, 2002, 2011, 2012; Beaver, Boucher and Pennington, 2007) demonstrated how it could be explored by Research Through Design methods, including through the production of workbooks – which he describes as "*collections of design proposals and related materials, both as a method for design and as a design methodology*" (Gaver, 2011, p. 1551).

The production of a design research workbook then both documents an alternative design space of speculative proposals and may serve as a resource of inspiration in subsequent more highly resolved design work. The related *annotated portfolio* and pictorial publication formats allow such design work to be given form as research without being resolved as a studied artefact (Bowers, 2012; Gaver, 2012; Gaver and Bowers, 2012; Pierce, 2014). James Pierce's counterfunctional things project (Pierce and Paulos, 2014) is a good example of such a research outcome; his proposal for a wireless derouter (Pierce, 2016) and alternative design metaphors for networking (Pierce and DiSalvo, 2018) are highly relevant here and share some method and intention with the *Heterogeneous Home* (Aipperspach, Hooker and Woodruff, 2008) to be discussed next.

The ludic perspective is useful in challenging the utilitarian logic of the automated home, exposing forms of work by validating playful alternatives.

Heterogenic

Like Making By Making Strange, *The Heterogeneous Home* by Ryan Aipperspach, Ben Hooker[36] and Allison Woodruff seeks to problematises the homogenised, normalised domestic space that they find implicit in Ubicomp (Aipperspach, Hooker and Woodruff, 2008). The paper proposes ways of boundary making to differentiate domestic space through a series of design proposals, presented as sketches from a workbook. In particular, they explore the boundary between home and work activities, defining spaces where work email is accessible and those where it is not[37]. These sketches consider the home at multiple scales and particular attention is paid to architectural interventions at Brand's Space Plan layer – to define the characteristics of individual rooms. The Heterogeneous Home also resonates with prior work on

[36] Previously, Ben Hooker was a member of the Computer Related Design studio at the Royal College of Art, where he worked with Bill Gaver and Tony Dunne on the Presence Project (Gaver, Hooker and Dunne, 2001).

[37] It is important to acknowledge that work is narrowly defined here, and these proposals tend to privilege kinds of paid employment over housework.

domestic video spaces at the Royal Institute of Technology's ComHOME that explores how the gaze of cameras create unequal spaces and thresholds of public visibility; this was materialised as a living lab (Junestrand and Tollmar, 1999). These projects echo Dourish and Bell's critique of Ubicomp that, "*The rhetoric of seamlessness is often opposed to the inherently fragmented nature of social and cultural encounters with spaces; we need to be able to understand how pervasive computing might support rather than erase these distinctions.*" (Dourish and Bell, 2007, p. 15).

Like the ecologic perspective, the heterogenic perspective calls for designs are prepared to encounter the uniqueness of a home and its work. Making By Making Strange then helpfully connects a series of tactics and methods for making ecological, ludic and heterogenic accounts of the home that oriented to alternative (and somewhat strange) design landscapes.

Artful Systems

The second influential text is Artful Systems in the Home (Taylor and Swan, 2005), in which ethnographers Alex Taylor and Laurel Swan present their fieldwork on the everyday use of organisational systems (calendars, paper notes, to-do lists, etc.) in managing a family at home. In doing so they make visible a form of domestic labour and demonstrate an alternative domain for home technology, when "*arguably disproportionate attention [is] given to leisure and entertainment*" (Taylor and Swan, 2005, p. 641). Through their analysis it is suggested that, "*technologies must be designed to accommodate the rich and diverse ways in which people organize their homes, providing them with the resources to artfully construct their own systems rather than enforcing ones that are removed from their own experiences.*" (Taylor and Swan, 2005, p. 641). While this is a critique of homogeneity, it is not directed at Ubicomp. Indeed, they conclude, "*Generally, the implications of what has been presented outlines a vision of multiple and heterogeneous information technologies operating within the home, a vision that is closely aligned with the ubiquitous computing project.*" (Taylor and Swan, 2005, p. 649).

Taylor and Swan's emphasis on heterogeneous collections of artefacts and ecological habitats, revealed by a process of ethnographic defamiliarisation, can be easily seen as a tactic to make strange. *Ecological habitats* was coined by Andy Crabtree and colleagues to talk about the "*places [in the home] where communication media reside*" (Crabtree, Hemmings and Rodden, 2003). As well as taking an ecological perspective for alternative making, Taylor and Swan also emphasise the *material properties* of the systems they ethnographically encounter and the *material artefacts* that might be made in response – *to produce the home's social order* (Taylor and Swan, 2005). Here material is understood in terms of its affordances; for instance, the "*ubiquitous, pliable and free-form properties of paper-based artifacts"*. Material exploration is well-established in art and design as a practice-led approach through which a material's affordances, its interactions and ways it may be worked become apparent – this is not an abstract engagement but highly specific and inherently situated. It is quite a different tradition from the engineering disciplines that value well-understood material properties and reproduce established patterns through industrialised processes. In the HCI literature material understandings are often coupled with Research Through Design methods intended to reveal alternatives and these tend to be offered by those with a design school training – through what might be broadly described as Critical Making.

The term Critical Making was defined by Matt Ratto (Ratto, 2011) to describe material and participatory practices and has been influential in recent HCI discourses. "*Critical making organizes its efforts around the making of material objects, devices themselves are not the ultimate goal. Instead, through the sharing of results and an ongoing critical analysis of materials, designs, constraints, and outcomes, participants in critical making exercises together perform a practice-based engagement with pragmatic and theoretical issues.*" (Ratto, 2011, p. 253). Garnet Hertz's later adoption of the term for a handmade book of the same name (Hertz, 2012), featured works and interviews from practitioners who, through their making and material engagement, offer some critical reflection on technology and society (Hertz, 2012). Contributors include Matt Ratto, Dunne & Raby (Critical Design) and Julian Oliver (Critical Engineering); as such it offers a rather more inclusive definition of what might constitute material engagement, while still emphasising the importance of the act of making. Another related influential thread is that of Phil Agre's Critical Technical Practice, in which close technical work allows a "*rigorous reflection upon technical ideas and practices*" (Agre, 1997, p. 3), that unpacks a system's values and assumptions.

Building on Critical Making, Ron Wakkary's notion of *material speculation* also has a concern with mindful practices of design and making, but shifts its attention to the reality of living with physical material artefacts that embody some *counterfactual* alternative (Wakkary *et al.*, 2015). The work of Wakkary's Everyday Design Studio has since developed a series of domestic counterfactual material speculations including Hook (Odom *et al.*, 2016), Morse Things (Wakkary *et al.*, 2017), table-non-table (Hauser *et al.*, 2018), the Olly radio (Odom *et al.*, 2018) and Slow Game (Odom *et al.*, 2018). In their 2015 paper on *Investigating Genres and Perspectives in HCI Research on the Home*, Audrey Desjardins, Ron Wakkary and Will Odom identify two complementary perspectives that, "*help expand the HCI community's attention to new* *areas of domestic technology research: the material perspective and the first person perspective* ." (Desjardins, Wakkary and Odom, 2015, p. 3073). Subsequently, the Everyday Design Studio and alumni have demonstrated these perspectives in use in their papers: *Designing for an other Home* (Oogjes, Odom and Fung, 2018) and *Alternative avenues for IoT: Designing with non-stereotypical homes* (Desjardins et al., 2019).

These Artful System perspectives broadly complement the Making by Making Strange collection and helpfully expose some of the necessary organisational work of the home. These material responses to ethnographic encounters inform my methodological approach in Chapter Four.

Hertzian Tales

The final influential text is Anthony Dunne's Hertzian Tales (Dunne, 2006) through which the concept of materials is extended to immaterials – those without physical form. Implicit in a material approach is that the material is both visible and manipulable. This is straightforward for physical materials such as wood, paint, mechanics, etc, but less clear for largely invisible software, electronic circuits, networks and radio waves. It is not without contention that material understandings be applied to technologies such as these, but this thesis shall later argue that it can (Franz and Papert, 1988; Löwgren and Stolterman, 2007; Vallgårda and Redström, 2007).

In Hertzian Tales Anthony Dunne describes a Hertzian space of radio and invisible radiated properties of electrical devices and the concept of radiogenic objects, that "*allows this invisible world to be understood and modeled in terms of material reality, it provides a starting point for a design approach that links the immaterial and the material so as to open up new aesthetic and conceptual possibilities.*" (Dunne, 2006, p. 112). Dunne explored this space, often in collaboration with Fiona Raby, through a body of work that includes: the Faraday Chair – in the permanent collection of the V&A (1995), Pillow (Dunne and Gaver, 1997) and the book Design Noir (Dunne and Raby, 2001) which documented the Placebo project and designs such as the Compass Table and the Electro-draught excluder. Perhaps with the exception of the Compass Table, all expose the Hertzian space obliquely – their highly resolved finish and function are designed to communicate through photography and gallery show; in the main, they do not function technically. Instead, they are speculative responses to the invisible.

A rather more literal, but nonetheless fictional, rendering of the Hertzian space is made by Semiconductor in their film Magnetic Movie (Jarman and Gerhardt, 2007). Through interviews with scientists at NASA's Space Sciences Laboratories (UC Berkeley) the film visualises the invisible magnetic fields that are described using video footage of the laboratory overlaid with animation. The viewer (and perhaps prospective designer) is left with an imagined experience of the invisible.

Through the *Immaterials* project Timo Arnall describes a rather more direct approach to working with the invisible material of the Hertzian space. Arnall at BERG and then at the Oslo School of Architecture and Design, demonstrated how to design with RFID (Martinussen and Arnall, 2009) and WiFi (Arnall, Knutsen and Martinussen, 2013) in material terms. Long-exposure photography and light painting are used to reveal the complex electromagnetic fields that shape the interactions with these wireless technologies, a form of exposition that harks back to the time and motion work of the Gilbreths. Arnall shows that, in the case of RFID, once revealed these immaterial qualities can be matched by physical affordance in the design of tokens and readers – resulting in interactions that are well understood, where the visible and invisible are reconciled. However, electromagnetic fields are but one of the invisible technical materials in the home – how might computation and global connectedness also be considered in material terms?

A Hertzian perspective is fundamentally about finding tactics to make the invisible visible, producing designs that engage with immaterial realities – not least with the home WiFi network.

Conclusion

This final part of the chapter has suggested some starting points for domestic design alternatives that make struggles with the networked home visible, challenge an uncomplicated narrative and make the work on which the home relies more apparent. From these influential texts the following strageies are suggested: defamilarisation through ethnography, Research Through Design practised through the production of design research workbooks, material/immaterial engagements and taking a first-person perspective. These tend to furnish the designer with ecologic, ludic and heterogenic understandings of the home, which seem rather well realised in the diagrammed machines of Rube Goldberg. These methods will now be refined and elaborated in Chapter Four.

Taken together these two parts of the chapter have presented a broad account of the domestication of new technologies, their social implications, and ways to seek alternative paths. This has necessarily drawn on a variety of scholarly and popular sources over an unusually wide span of recent history. Significantly, this chapter has shown how the concept of Invisible Work can be used to critique network technologies and HCI’s vision of Ubiquitous Computing with its implication of machine surveillance.

Chapter Four: Designerly Hacking in Response to Surveillance Capitalism

This chapter describes the methods I shall employ in seeking to design alternative networked homes; homes that prioritise a network of one's own and respond to the challenges of domestic Surveillance Capitalism. In the broadest terms, this is a practice-based Research Through Design inquiry and as such the first section offers this essential framing. The second section outlines the two empirical studies that constitute this inquiry: Hack My House and the Home Network Study. Each builds on the existing methods for alternative domestic design described in the previous chapter; they also illustrate the use of a new method of designerly hacking that discloses new technical possibility in complex systems – hacking being a direct way to open black boxes. The third section situates ways of hacking in general terms, allowing the fourth and final section to unpack how Designerly Hacking operates through close technical work that incorporates the products and methods of hacking, but with designerly intent. The combination of these studies and methods employed are designed to socially and technically reveal the struggles and invisible work of the networked home and then offer alternatives – first as a resource for the process of design and then as inspiration for designs themselves.

The final two sections situate designerly hacking in broader historic and theoretical framings, with the intention of contributing a more widely applicable research design method for dealing with technical complexity. So, the third section offers a brief history of hacking, such that the fourth section can characterise some features of designerly ways of hacking. From this methodological foundation, the subsequent chapters describe each study in turn.

Research Through Design

Over the past fifteen years my design practice can be characterised as an Research Through Design (RTD) inquiry – first at BT Labs, then the Royal College of Art, at Newcastle University and now at Goldsmiths – although I have only latterly identified it as such (Kirk et al., 2016). My education and experience prioritise practice and reference to the prior art, over theory; I am clear that theory alone can never capture all the nuances of a successful design. The individual human mind is by no exaggeration the most complex and diverse structure on earth, when operating outside the laboratory in domestic social groups the reductive, generalising thrust of the scientific method and resulting theories struggle to make useful predictions – especially as it pertains to the subtleties and details of successful design. So, the RTD that I practice implies designerly (rather than scientific) things to know, ways of knowing and ways of finding out that can be applied to the practice of design– this is the use of designerly articulated by Nigel Cross (Cross, 1982). Philosophically these concerns are pragmatic, in the sense of John Dewey's approach to knowledge, which focuses on specific situated experiences (Dewey, 1929).

As someone primarily focused on design practice, it takes a change of perspective to understand how theory shapes my work – often implicitly. My understanding and practice of Research Through Design is rooted in the traditions of the Royal College of Art, where to some degree RTD was in the air, encoded in the everyday activities of the college. More directly I have been profoundly influenced by Bill Gaver and Anthony Dunne through their tutorage, but for neither is theory prioritised over practice. So there is then a degree of further archaeological and genealogical work necessary to surface my position with respect to theory and so method[38]. My simple designation of this thesis as an inquiry with concerns including precarity and stability creates resonances with Dewey that I was simply not expecting – namely his consideration of existence as precarious and as stable (Dewey, 1929, p. 40). This also comments on the value of design theory in design practice; it is almost never explicitly in play.

So then to Research Through Design. In the article Research in Art and Design (Frayling, 1993) Christopher Frayling describes three modes of research in art and design: research into art and design, research through art and design, research for art and design. Fraying's paper is foundational for constructing practice-based art and design as research, distinct and valid, rather than a degenerate form of the scientific method. At the time Frayling was a senior professor at the Royal College of Art and would become the college's Rector in 1996. Meanwhile, Gillian Crampton Smith, leading the college's Computer Related Design (CRD) studio, was exploring these ideas in the context of the computer, which she articulated with her partner Philip Tabor (at the Bartlett School of Architecture) in the book section The Role of the Artist-Designer (Smith and Tabor, 1996). By now, Anthony Dunne and Bill Gaver were together in the CRD studio (Crampton Smith, 1997) and at CHI 1997 they presented

[38] The previous chapter was similarly motivated in attempting to disclose such implicit attachments in Ubicomp.

Dunne's Pillow as Research Through Design to the HCI community, "*an example of our ongoing attempt to understand how we can do research while respecting the methods and perspectives of designers.*" (Dunne and Gaver, 1997, p. 362) – thus building on the concept of artist-designer. With the same intent, this collaboration would later invent cultural probes (Gaver, Dunne and Pacenti, 1999). Gaver, in particular, has subsequentially shaped the ways in which Research Through Design is understood and practised in HCI over the past twenty years (Gaver and Martin, 2000; W. Gaver *et al.*, 2004; Gaver *et al.*, 2010, 2013; Gaver, 2012).

In recent years an alternative understanding of Research Through Design has also been influential in the HCI community, one that draws on a tradition of Herbert Simon's Design Science at Carnegie-Mellon University (CMU) (Simon, 1969)[39]. Design science attempts to make design rigorous and systematic, indeed scientific – in marked contrast to Crampton Smith's artist-designer. In a series of publications John Zimmerman (CMU) and colleagues, including Jodi Forlizzi (CMU), attempt to recast RTD as a design science method to be known as [pragmatic] Constructive Design Research (CDR) (Zimmerman, Forlizzi and Evenson, 2007; Zimmerman, Stolterman and Forlizzi, 2010; Koskinen et al., 2012). This seems epistemologically incongruent to me and Gaver makes this same challenge in his paper *What should we expect from research through design?* (Gaver, 2012). Forlizzi and Zimmerman have stated that they believe these differences to be irreconcilable and have gone so far as to call for an academic divorce from those they characterise as practising Critical Design (Forlizzi *et al.*, 2018). Yet these categories seem uncomfortable, conflating design science and pragmatism, set in opposition to a broad spectrum of speculative and critical work[40]. Perhaps, in part, this is why the proposal has had little traction in the HCI and design communities, with few studies identifying as CDR.

[39] It is notable that relevant deisgn researchers including: Carl DiSalvo, Will Odom and James Pierce are products of the design and computer science programmes at Carnegie Mellon University and this provides an interesting way of seeing their work through a Design Science lens.

[40] This dichotomy is strained further in acknowledging the contribution of Zimmerman's co-authors to the ideas I present in this thesis; Jodi Forlizzi, Eric Stolterman and Johan Redström are cited on multiple occasions in broadly affirmative ways (Forlizzi, 2008; Stolterman, 2008; Davoli and Redström, 2014).

How then should I frame my own Research Through Design? Here I turn back to Gaver and the Interaction Research Studio's account of the Prayer Companion, "*in which design practice is brought to bear on situations chosen for their topical and theoretical potential, the resulting designs are seen as embodying designers' judgments about valid ways to address the possibilities and problems implicit in such situations, and reflection on these results allow a range of topical, procedural, pragmatic and conceptual insights to be articulated.*" (Gaver *et al.*, 2010, p. 2055). My inquiry is precisely about offering richer, complications of simplistic attempts to homogenise the home.

Critically then, what are the activities and outcomes of my Research Through Design? The Family Rituals 2.0 project (Kirk *et al.*, 2016; Chatting, Yurman, *et al.*, 2017) shaped the ways I came to this inquiry; defined by a process of participant engagement through interviews and Culture Probes, followed by the design, fabrication and deployment of bespoke Research Products (Odom *et al.*, 2016), here to disclose attitudes to separation in families due to remote work. This thesis and Family Rituals both attempt to unpack some of the complexity of multioccupancy homelife and so both are embedded in complex technical and social networks; however, this inquiry is more explicitly concerned with technical infrastructures. While, more improbable design speculations might be deliberately insulated from the world at large, enclosed within a magic circle (Huizinga, 1955; Andersen and Wilde, 2012); the design of this RTD needs an inquiring power that will reveal these networks in the home and in the world.

The inquiring power of a Research Product can be expressed both in the process of its making and in its subsequent deployment– in Stolterman's terms operating as an *ultimate particular* (Stolterman, 2008). A working product demonstrates that through the process of design the networks that constitute this reality have been (at least) partially understood – especially when it operates for a prolonged period. In Research Product terms: finish, independence and fit are all designed attributes of the product that integrates with (or deliberately disrupt) the reality of the world once deployed. This has a similar intention to Sanders and Stappers' notion that prototypes necessarily confront and change the world; although theirs is less concerned with working prototypes and more narrowly focused on experimentally instantiating some theoretic position (Sanders and Stappers, 2014).

For good pragmatic reasons, many domestic Research Product studies develop novel computational Stuff – in the sense of Brand's "*the things that twitch around daily to monthly*" and implying a physical scale. Smaller devices are typically easier to fabricate and easier to install in the participant's home, intense interactions are quicker to study, and a technical independence of operation is more likely to work. Yet without deeper entanglements in the network, the inquiring power of this Stuff seems diminished; both in what can be learnt in the process of its design and in its deployment. While my inquiry is also necessarily stuff-orientated, the network (by way of hacking) opens up an unusual degree of entanglement with the world and so magnifies its inquiring power. Lorenzo Davoli and Johan Redström illustrate this point through their probe-based exploration of logistic infrastructures (Davoli and Redström, 2014).

Family Rituals is a good methodological waypoint for designerly hacking, in that it begins to articulate some of the ways in which hardware hacking can be used in RTD, specifically how the mobile telephone can be considered as a material for Research Products (Chatting, Kirk, *et al.*, 2017). However, my new inquiry is more concerned with the process of design than Family Rituals. As such the outcomes of this Research Through Design have forms that are intended to be generative and illustrative of alternative design spaces, rather than the highly resolved (critical) exemplars of the Family Ritual machines. The literature dealing with this disclosure of alternatives using RTD, as it might be applied to networked homes, was described in the previous chapter. The next section outlines how my RTD will proceed in this inquiry and how it relates to this previous work.

Seeking Alternative Networked Homes

This thesis seeks to complicate accounts of the home and the domesticated Internet that would otherwise characterise them as a simple, settled and uncontested; then to offer alternatives – new possibilities for design that knowingly participates in domestic struggles. To this end, the Home Network Study and Hack My House contribute social and technical understandings of existing networked homes. This section outlines these two studies. Each builds on the existing design research methods suggested in the last chapter for seeking domestic alternatives, namely: defamilarisation through ethnography, a first-person (autoethnographic) perspective, a material/immaterial engagement in a practice of Research Through Design and the production of designerly forms. The studies straightforwardly apply these: the Home Network Study creates a defamilarisation of the home and the network, Hack my House is a first-person material engagement and in Chapter Eight design patterns will be articulated that are intended to generate alternatives and make these insights apparent for a wider audience. The complexity of the home network ecosystem requires some innovation in these methods to make a better account beyond what is visible, local and instantaneous – what goes on in the network. Typically forms of RTD and its documentation (such as the pictorial publication format) are well suited to situated inquiries of physical artefacts but lack the same resolution for software, networks and distributed ecologies. Designerly Hacking is my response to this challenge and is applied in these studies.

Home Network Study

The Home Network Study is intended to offer an account of the domesticated Internet as it is currently configured in some homes. Domestication here is understood through the lens of Brand's Shearing Layers, which pulls into focus rates of change and the liberties of individuals to make change in the home – which speaks directly to the aspiration of a network of one's own. To magnify this, the participants of the Home Network Study are renters and so to some degree struggle with precarity, in that they do not own the spaces in which they live. The study of renters is both personally relevant, giving a motivation to my work and widely experienced, making it easy to communicate to a wider public. By working with renters, the study can then disclose ways that participants make change in their homes in general and with their home networks in particular. This is broadly intended to deliver a defamilarisation of the networked home through ethnographic methods.

The Home Network Study takes the familiar form of a cultural probes package (Gaver, Dunne and Pacenti, 1999) in which the activities are designed to give glimpses of everyday life and promote some reflective behaviour too; generating response materials to inform then inspire the design process. These studies tend to include a collection of both paper-based and technically mediated probes, for instance maps, listening glass, dream recorder (digital memo-taker) and disposable cameras (Boehner, Gaver and Boucher, 2012). The Home Network Study continues in this tradition by using a set of provocation cards that are styled after Peter Schmidt and Brian Eno Oblique Strategies (Schmidt and Eno, 1975) and suggest captions for photographic responses. The disposable camera no longer needs to be provided as the availability of a smartphone can be reasonably assumed. However, to allow participants to witness and make accounts of their networks requires some uncommon instruments. The Home Network Study includes three bespoke WiFi instruments that measure invisible qualities of the network: the signal strength of the home router, the dynamics of an individual device's use of the data and an overview of the network. These allow both directed explorations and reinforce fundamental concepts – for instance, the invisible qualities of WiFi as a radio broadcast. The cards also promote these questions.

While technically mediated probes have always been a feature of cultural probe studies, I deliberately use the designation of instruments here. This reflects Dewey's writing on pragmatism (or indeed instrumentalism) which Peter Dalsgaard develops in his conceptual framework for instruments of inquiry (Dalsgaard, 2017). This helpfully provides a vocabulary of five qualities: perception, conception, externalisation, knowing through action and mediation; which I will define and use in Chapter Five on the Home Network Study.

Hack My House

Hack My House is a series of technical explorations of my own home network, where access and permission are uniquely available, and I can freely explore the implications of a network of one's own. Being a rented home, this also develops reflections on struggles with precarity. Hack My House is the clearest expression of my designerly ways of hacking and this activity is framed through periods of self-directed hacks, making, documentation, public demonstration and hackdays . This then necessarily takes a first-person (autoethnographic) perspective and makes a material/immaterial engagement in the networked home, in a technically engaged practice of Research Through Design.

Hack My House responds to the complexity of the network with close technical work that incorporates the products and methods of hacking, but with a designerly intent. This has some a parallels with Agre's Critical Technical Practice (Agre, 1997), but with perhaps with a less explicitly critical agenda and more as a means to seek technical alternatives. This produces a series of software and hardware experiments, prototypes and interventions in my home. These self-directed hacks and consequent making, allow an exploration of prototyped forms and documentation, that facilitate myself and others to make alternative design proposals for the networked home.

Hacking is close technical work that enables a material engagement in the networked home, but it is typically rather slow, concentrated, and antisocial – albeit the constant referral to online forums in the hope of striking gold. Hacking is a risky activity in which time invested can frequently not be rewarded and as a solitary endeavour motivation can wax and wane, or you can become hopelessly lost in the detail. As such it is difficult to manage in the context of a resource-limited directed inquiry. It is notable that in one of the few papers that consider hacking and Research Through Design, William Goddard and Robert Cercos hack together playfully, "*not driven by the expectation of research outcomes*" and for defined time-limited periods (Goddard and Cercos, 2015). Hack My House addresses these challenges through a regular series of hackdays at my house that constructs a small (trusted) public for the products of my hacking, then makes an invitation to work with these materials and suggests some pliable forms they may take to facilitate this. In Audrey Desjardins and Aubree Ball's discussion of autobiographical design they identify five tensions: need, participation, privacy, contemplation and authorial voice (Desjardins and Ball, 2018). Chapter six on Hack My House will reflect on the challenges of this inquiry in these terms and contribute to an ongoing discussion of autoethnographic methods in HCI.

Ways of Hacking

This section is intended as a brief history of hacking that will next enable such practices to be considered in designerly ways, as such it constructs a working definition of hacking that implies close technical work with computers and networking. With this established the next section will characterise some features of designerly hacking, drawing on these examples.

MIT Hacks

Steven Levy's book Hackers (Levy, 1984) situates the word hacker in the early computer labs of MIT from the late 1950s. At the time hack was already in use at MIT to describe a series of audacious night-time pranks – a tradition that continues and included the placement of a police car on top of the campus' Great Dome in 1994 (Peterson, 2003). In these earlier days, the monolithic computers were disconnected from the world and communities of hackers worked (often in the small hours of the morning) to demonstrate ever more elaborate mastery of the machine at hand. The products of this included Steve Russell's graphically sophisticated Spacewar game on the PDP-1 in 1962, around which larger groups gathered to play (Brand, 1972). This hacking was transgressive in the sense that vastly expensive computers were used for seemingly trivial applications, but not in the sense of hacking-in to gain some unauthorised access. However, by 1963 these MIT hackers were beginning to probe the number ranges of the telephone network with these same machines and hacking became a means to explore the outer world – an idea that was already familiar to the Phone Phreakers (Lichstein, 1963).

Phone Phreakers

By the 1950s the telephone network had grown to be a complex interconnection of exchanges, trunk lines and manual routing, with some automatic control signalling through tones – crucially using the same audio channel as the speech. Long-distance calls had to be routed (manually to start with) across the network – from exchange to exchange. With an attentive ear, one could hear the properties of the network through the way it shaped sound. The telephone network was a beguiling global electro-mechanical-social system that could be accessed from home or the street corner and those who were drawn to explore it became known as Phone Phreakers. Phil Lapsley's Exploding the Phone describes the practices and cultures of the phreakers from the 1950s to the 1970s in America (Lapsley, 2013).

The phreakers motivations were various; at the start they tended to act alone probing the telephone numbers on each exchange, mapping the interconnection of exchanges, finding the operator codes and finding special numbers used by the phone companies and the government. The first phreakers were typically teenagers and college students; overwhelming male and disproportionately blind – many found the telephone network a way to reach out from their isolation at home and act through sound in the world. Their tools were rudimentary, a sharp ear, a toy whistle and some ramshackle electronics – orders of magnitude more available than the tens of thousands of dollars of computing resources at MIT.

Through a series of observations, explorations and the discovery of detailed technical documentation in university libraries, communities of phreakers came together to unpick both the topology of the network and the control mechanisms that increasingly automated it. Central to this was the production of a 2600Hz tone, which the network used as a practically universal control signal. The phreakers learned to make this tone for themselves, discovering that a Captain Crunch cereal packet toy whistle produced it perfectly, building electronic Blue Box circuits and in rare cases pitch-perfect whistling. By understanding the signalling protocol of the network, it became possible to exert a level of control over it with just the access granted by a standard telephone handset. It was realised that payphones signalled the value of the coins inserted through a sequence of tones, others indicated that a call had begun and charging should start. By producing these tones at prescribed times anyone could make free phone calls, without the detailed technical understanding of the original phreakers. With such a popular motivation, a wider audience was drawn to phone phreaking and the Blue Box circuits became commodified – being sold by individuals that included the Apple founders, Steve Jobs and Steve Wozniak.

By the early 1970s, Blue Boxes tone generators were widely (and cheaply) available. Phreaking had become popularised notably by an article in Esquire Magazine (Rosenbaum, 1971), groups like the Homebrew Computer Club, newsletters like TEL (Telephone Electronics Line) and inclusion in the underground publication of the Anarchist Cookbook (Powell, 1971). Along with the ability to make free calls so-called party lines numbers were discovered in the network that would connect people in large conference calls. Over time these party line numbers became social meeting spaces that amongst other things supported the new political discourse of the growing countercultural movement; exemplified by Brand's Whole Earth Catalog. One such notable group were the Yippies or the Youth International Party who established the YIPL (Youth International Party Line). The curiosity and isolated exploratory hacking of the original phone phreakers had driven an understanding of the telephone that became embedded in artefacts like the Blue Box and enabled a series of cultural reappropriations, which were now challenging the intended logics of the network.

Throughout this period Bell fought with varying degrees of success the activities of the phreakers. While the legal status of phreaking and the tactics Bell used to detect and prosecute users of Blue Boxes were contested, over time the law responded to the new phenomena of the network and ultimately, phreakers such as John Draper (known as Captain Crunch), served prison terms for phone fraud.

There is a pleasure in retelling these stories, but there are also some important lessons as I attempt to historically situate designerly hacking. Such hacking consumes and produces forms of knowledge in particular ways that construct different publics who bring meaning to the hack, while there is a struggle with existing structures of power. Phreaking in particular frames hacking as low-cost DIY or even guerrilla action – by which some inequity can be addressed, or a curiosity satisfied and this complicates simple criminality.

The Hacker Ethic

By the 1980s the popular view of the hacker was of one who gains unauthorised access to some remote mainframe system, over the telephone network from a home computer. Two interesting films that construct popular perspectives on hacking in this period are WarGames (1983) and Ferris Bueller's Day Off (1986). In both teenaged Matthew Broderick is a playful male hacker, who in WarGames accidentally brings the world close to global thermonuclear war from his bedroom and as Ferris Bueller his computer hacking is far more mundane, but intentional, as he harasses the teacher by altering his high school database. Broderick's characters are playful and a little devious, but not politically or criminally motivated. Through the discussion that follows I want to establish some of the ways hacking (and portrayals of hacking) struggles with existing structures of power and question its ethics; designerly hacking is to a degree adversarial.

With this level of popular recognition, efforts were mobilised to establish hacking's morality. In 1984, Steven Levy argued in his book Hackers that a hacker ethic had been informally established by the early MIT hackers and which had subsequentially positively influenced the direction of computing (Levy, 1984). The British hacker Peter Sommer (writing under a pseudonym) described the techniques of hacking as a recreational and educational sport in the Hacker's Handbook (Cornwall, 1985). At the same time, Loyd Blankenship (also pseudonymously) published The Conscience of a Hacker (popularly known as the Hacker Manifesto) on a bulletin board in 1986 – which framed the criminality of hackers as an expression of intellectual and moral superiority, "*My crime is that of curiosity*" (Blankenship, 1986). Yet it is

Levy's articulation of five moralising tenets of the hacker ethic that has been the more influential:

1. All information should be free.
2. Mistrust authority – promote decentralisation.
3. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
4. You can create art and beauty on a computer.
5. Computers can change your life for the better.

(Levy, 1984, pp. 27–38)

The hacker ethic has a clear rhetorical purpose, and as Levy recalls, in 1984 "*the media was starting to define the word as 'evil little grub who breaks into computers'.*" (Levy, 2014). Levy is neither an impartial nor untroubling narrator. In reflecting the demographics of MIT students in the 1950s and 1960s his book describes an exclusively white, male and wealthy culture, which he glorifies through the language of the priesthood, monastic orders, the brotherhood and the Catholic church – its subtitle, heroes of the computer revolution, has a Randian tone. Furthermore, Levy's writing casually and unreflectively describes students as their professor's *coolies*.

However, it is perhaps the first tenet, *all information should be free* or rather Stewart Brand's rephrasing that *information wants to be free* that has been the most consequential and has come to define hacking's moral purpose to reassert access and openness when it is restricted. Brand coined the phrase in an exchange with Steve Wozniak at the first Hackers Conference in 1984; a conference he was inspired to convene in Marin County to bring together the characters from the pages of Levy's book (Brand, 1985; Levy, 2014). In total there were 125 attendees, many meeting for the first time, including: Bill Atkinson, Steve Capps and Andy Hertzfeld from the recently triumphant Macintosh team at Apple; Richard Stallman of MIT; and renowned phreaker John Draper aka Captain Crunch.

The original exchange between Brand and Wozniak concerned intellectual property and copyright. "*On the one hand information wants to be expensive, because it's so valuable. The right information in the right place just changes your life. On the other hand, information wants to be free, because the cost of getting it out is getting lower and lower all the time. So you have these two fighting against each other.*" (Levy, 2014). So, in context Brand's words reflect an economic tension, but in use they resonant as an ethical imperative; writ large in Stallman's Free Software Foundation (FSF) (1985), Tim Berners Lee's World Wide Web (1989), Linus Torvalds' Linux (1991) and codified in so-called *copyleft* software licenses, like the FSF's GNU General Public License. These mechanisms of sharing enable much of the free exchange of tools and data on which designerly hacking relies and then wishes to contribute.

By the 1990s, with films such as Sneakers (1992), Hackers (1995) and The Net (1995), Hollywood's attention shifted to networked national infrastructures that it saw conceivably within a hacker's grasp. In each there is some adversarial struggle between good and evil with cyberterrorists or some state-level conspiracy. Hackers and The Net are both explicitly situated on the Internet, a technology of which the audience would have been largely ignorant. As the Internet grew in the late 1990s, the booming security industry took Hollywood's lead and began to make the distinction between the ethical white-hat-hackers and their adversaries the criminal black-hats. Designerly hacking is not intended to be white-hat, in the sense that it can propose (potentially disruptive) alternatives, but it is also not black-hat, in that plural alternatives are intended.

Hacktivism

Around 2003 the term hacktivist began to be used to describe hackers with explicitly politically motivations, who disrupted the activities of their opponents through online protests, pranks, and hacks. It particularly relates to the Anonymous group an international hacker collective of whose targets have included the CIA, Sony and the Sun newspaper – public statements justifying their actions were anonymised by the wearing of the Guy Fawkes mask from the film V for Vendetta (2006) and the use of voice changing technology (Cadwalladr, 2012). This is probably the dominant view of hacking today, not of isolated curious teenage boys, but of orchestrated criminality and state-sanctioned cyber warfare, targeting individuals, organisations and critical infrastructure – this is the world portrayed in the television drama series Mr Robot (2015). Hacktivism is an extremely adversarial form of hacking, attempting to enact political change, whilst refusing to be identified and so accountable. Designerly hacking can be politically motivated, but as design work positionality needs to be acknowledged at least through authorship – it should not be anonymous.

Hardware Hacking

So far this discussion of hacking has been limited to gaining unauthorised access to some remote system, but the concern of designerly hacking is more materially at hand. Electronic devices have always offered the potential for modification and maintenance to those with sufficient technical know-how. However, as circuitry became more complex and embedded with software, simple repair becomes less feasible. Furthermore, manufacturers have actively worked to prevent this access, both with physical barriers to the circuity and with the absence of comprehensive documentation. This is an attempt to control the repair market, limit the ways in which devices can be used and ensure future revenues through planned obsolescence. In reaction, Peter Vermeren (aka Mister Jalopy) wrote the Maker's Bill of Rights for Make Magazine, in which he declared, "*If you can't open it, you don't own it.*" (Vermeren, 2005). This makes 17 demands on manufacturers to ensure their products are repairable and hackable; including, "*Screws better than glues*" and "*Circuit boards shall be commented*". Being able to access the contents of the closed box is fundamental to repair, hacking depends on being able to break open a system. Some 16 years later, the *Right to Repair* was enacted in British law (in July 2021) and similar legislation was being drafted by governments across the globe. The British law requires manufacturers of some electrical appliances provide spare parts for consumers to make "*simple and safe*" repairs (Speight, 2021). However, while it covers dishwashers, washing machines, washer-dryers, refrigerators, televisions and "electronic displays"; it excludes, smartphones and computers, and even cookers, microwaves, hobs and tumble dryers. It is unclear how these rather simplistic laws will respond to the dependencies and complexities created by information appliances.

With the introduction of information appliances, like cameras, music players, and electronic toys; domestic devices from the 1990s became routinely embedded with microprocessors running software that defined their behaviour, rather than being defined by the physical wiring. Over the past 15 years these appliances have become connected to the Internet and existentially dependant on the cloud, with their behaviour constantly redefined by over-the-air updates. Running embedded software these appliances are a draw for hackers and tinkerers, especially when they are accessible via the network.

Traditionally hardware and software systems might be developed in-house through an entirely bespoke process – leaving them relatively closed and inaccessible to reconfiguration. However, today the complexity and ambition of these systems necessitate the reuse of common black boxes and toolchains. For hardware this means that devices are often overprovisioned for the task at hand, using common components manufactured inexpensively in high volumes. For software then a device's operating system will likely be composed of well-understood and documented subsystems. The Amazon Echo has at its core a Linux kernel, itself built on a series of open-sourced software libraries and technical standards. While this facilitates rapid commercial development, it also allows the decomposition of complex systems using familiar tools and suggests avenues for hacking that once cracked can be widely shared and reproduced via the Internet. This is the realm in which designerly hacking operates.

Open-source hardware, in the guise of computers like the Arduino (2005) and Raspberry Pi (2012), further allows the orchestration of hacked parts – either directly in an electronic circuit or over the network. The pliable software and the availability of GPIO (General Purpose Input/Output) hardware make the function of these boards ultimately unresolved and open for appropriation by the designerly hacker.

The potential of open-sourced software and overprovisioned hardware is perhaps best demonstrated by the series of hacks in which DOOM, id Software's groundbreaking 3D first-person shooter game from 1993, is shown to run on an unlikely set of devices – most recently an IKEA smart lightbulb (Maloney, 2021). This was spawned in 1997 when the DOOM source code, written in the popular C language, was publicly released under a non-profit licence. Using the *gcc* tool (Richard Stallman's GNU General Public Licensed C compiler) executable binary code can be generated for almost any microprocessor – including those now in lightbulbs!

Canny Hacks – Hackerspaces and Hackathons

Finally, while hacking is popularly understood as a technical practice in adversarial and access terms, the hack is also commonly used in the sense of a quick fix or reconfiguration. Sometimes this denotes a bodge, especially a bad but functioning technical solution – other times it refers positively to a shortcut or clever (canny) use of resources; as with Mind Hacks (Stafford and Webb, 2004), Life Hacks (O'Brien, 2004) and Ikea Hackers (Yap, 2006). This is the sense intended by the phenomena of the hackerspace/hackspace and hackathon/hackday; each offers some community scaffolding for the hack – which designerly hacking can employ too.

The notion of the hackerspace as a community initiated-space with shared tools to support a diverse set of broadly technical practices, gained global popularity after members of the Chaos Computer Club Cologne presented their catalogue of hackerspace design patterns at the Chaos Communication Congress (24C3) in 2007 (Haas, Weiler and Ohlig, 2007). These were practically orientated recipes for starting and running hackerspaces, clearly inspired by Christopher Alexander's Pattern Language (Alexander *et al.*, 1977) which delegates subsequentially used to found their own spaces – notably across North America.

Hackathons grew in popularity at about the same time – notably at Facebook in 2007 where the *like* button is said to have been invented (Chang, 2012). These corporate hackathons were framed as competitions in which teams conceived and hacked-together Web 2.0 (O'Reilly, 2005) service prototypes. These events typically spanned multiple days in a single location, at which the Silicon Valley machismo of coding, energy drinks and sleep deprivation were celebrated – not unlike Levy's original hackers. The Hack Day Manifesto (Knell, 2012) is an interesting document that codifies some of these qualities in practical advice for organisers. The Web 2.0 technologies were socially oriented and multimedia-rich, but they also crucially defined a series of well-defined public web APIs and datasets that allowed existing components to be easily *mashed up* in novel combinations – this might typically render some new dataset in Google Maps (Zang, Rosson and Nasser, 2008). These mash ups are the currency of these hackathons and this is hacking in the sense of the canny reconfiguration of prescribed units. However, in doing so these hacks tend to offer rather superficial combinatorial innovation, that shuffles unopened black boxes, leaving their logics and corporate interests wholly intact. Designerly hacking is intended to be more critically engaged.

The Silicon Valley hackathon has since become an endlessly appropriated format for rapid inexpensive solution-orientated innovation in corporations and public organisations. By 2010 civic hackathons began to be seen, which were constituted around newly available public data sources and framed as a new kind of democratic participation (Hogge, 2010; Schrock, 2016a). Doubtless, these events constructed more diverse publics (Lodato and DiSalvo, 2016) than their corporate counterparts, drawing together representatives of public organisations, citizen experts and some coders – most unpaid. However, in doing so these events became less focused on the demonstration of some technical feat; to the extent that Andrew Schrock reports participants describing, "*hackathons with no hacking* at which there is merely the *performance of innovation*" (Schrock, 2016b). In their article, The Trouble with White Hats, Melissa Gregg and Carl DiSalvo assume there is some technical innovation, but question how well "*the Silicon Valley model of public good enacted by hackathons provides technical solutions to social problems*" (Gregg and DiSalvo, 2013). Similarly, Evgeny Morozov argues the civic hacker seems apolitical, whilst unthinkingly enacting Silicon Valley's scientism (Morozov, 2013). Both advocate for more adversarial politically engaged hackers. I share this, having grown weary of hackathons, of weekends given up with no pay, working on dubious identikit projects, where your technical skills are seen as a resource for others to plunder. In recent years HCI has managed to reframe the hackathon as a form of Participatory Design (Taylor and Clarke, 2018) – where, in my experience, pipe-cleaners might be reconfigured, but not hegemonies.

Yet despite the hackathon's embedded Silicon Valley values, endless recombination of critically underexamined technologies and awkward relations to technical competency, they are still interesting; if only for the community scaffolding of canny hack, the forms of knowledge that facilitate it and the public that gathers. It is these aspects that inform designerly hacking.

This section has acknowledged the plural ways in which hacking has been understood historically and it has begun to make commitments for designerly hacking that relate to these. Designerly hacking implies both close technical work and a degree of adversarial work – in that it first unsettles systems, such that an alternative can then exist. However, it isn't just about breaking open; it is also about putting back together – to make an alternative with some designerly intent that gathers a newly engaged public. Nick Taylor and colleagues make a similar observation in their discussion of deconstructing and reconstructing technologies, "*individual deconstructed units became a building block for more complex conversations and which participants could use to build their own stories around.*" (Taylor *et al.*, 2021, p. 1814). Spacewar, the Blue Box and DOOM on an IKEA lightbulb are all examples of putting back together. In this context, the next section finally articulates designerly hacking as a method.

Designerly Ways of Hacking

This chapter has described the Research Through Design that I practice, then outlined my inquiries that seek alternative networked homes and apply a new method of designerly hacking. The previous history of hacking surfaced a degree of adversarial motivation and two phases of activity: breaking up and putting back together. With these identified this final section attempts to articulate designerly hacking in methodological terms. This is accomplished through two perspectives on adversarial practice, Carl DiSalvo's Adversarial Design (DiSalvo, 2012) and Peter Lamborn Wilson's Temporary Autonomous Zones (TAZ) (Bey, 1991).

Adversarial Design frames the adversarial nature of hacking that breaks up as "*revealing the hegemony*" and helpfully situates it in terms of Callon and Latour's Actor-Network Theory (ANT) (Callon and Latour, 1981). However, while DiSalvo offers an agonistic account of putting back together to "*reconfigure the remainder*", it is Wilson's TAZ that better captures the intended pluralistic outcomes of designerly hacking. Importantly, TAZ allows a return to my themes of visibility through its concept of the *pirate utopia*. Designerly hacking synthesises these two perspectives and the understanding of hacking developed in the previous section. This account then is intended to ground my studies with sufficient theory and methodological description to allow others to apply designerly hacking beyond the networked home.

Adversarial Design

Carl DiSalvo's Adversarial Design (DiSalvo, 2012) is grounded in Mouffe's politics of agonism (Mouffe, 2007), in which all matters are being openly contested. As such Adversarial Design engages in a kind of speculative alternative making in which the design outcome is intended to struggle, as an adversary, with the hegemony. DiSalvo describes the hegemonic state of the world in the terms of Callon and Latour's Actor-Network Theory (ANT) (Callon and Latour, 1981) which attempts to make explicit the complex ecology of humans and non-humans in which all design necessarily participates.

Adversarial Design also speaks directly to Ubiquitous Computing, as DiSalvo comments, "*The design of ubicomp is the design of connectedness. More than just exchange and expression between objects, this connectedness extends outward to enrol people, other entities in the environment, and even the environment itself.*" (DiSalvo, 2012, pp. 92–93). The network technologies of ubicomp then further expand the reach of these collectives, entangling them in further degrees of complexity. The constituents of these collectives are then not altogether obvious and are articulated together to particular effect – this is where the invisible labour is to be found in the system – and where the hegemonic things are.

While surprisingly DiSalvo's Adversarial Design does not explicitly consider the practices of hacking in these ways, the instruction to "*reveal the hegemony"* and then "*reconfigure the remainder*" are straightforwardly mapped to phases of breaking up and putting back together. Each is now considered in turn.

Reveal the Hegemony

DiSalvo's "*reveal the hegemony"* might be reinterpreted as: to *break-up*, *hack-open*, *disassemble*, *lay out*, *disarticulate*, *unpick*, *unpack* or *unsettle* a system, making its constituent parts visible and so (partially) revealing its operation. While DiSalvo's examples of this in action typically take the form of a visualisation of an otherwise hidden dataset, such as the Million Dollar Blocks project (2006)[41], it can also be straightforwardly read as a practice of hacking. This is the argument Cally Gatehouse and I make in our DIS 2020 paper on *Inarticulate Devices* (Gatehouse and Chatting, 2020).

The phone phreakers have a particular relevance to this inquiry in that they worked with the network as a whole to reveal its articulation – they recognised the network itself had properties and was not simply an abstract technology for collapsing distance.

[41] In which the cost of incarcerating individuals from city blocks in Brooklyn is mapped and made visible.

Adversarial Design usefully accommodates both this technical definition of the network and the interconnected ecology described by Actor-Network Theory. Of its human elements, it is clear that phone phreaking constructed different publics as it played out: the original phreakers who explored the network, gained access to forms of documentation, and shared what they discovered; those who commodified the tone making Blue Boxes; those who participated in making free telephone calls; and Bell, their adversary. This notion of publics is John Dewey's and was developed by DiSalvo (DiSalvo, 2009) prior to Adversarial Design, where it is only implicitly present. Publics is a helpful concept because it highlights how different audiences gather around different (designed) material forms.

Our Inarticulate Devices paper also productively reacquaints the ANT concept of the black box with Adversarial Design, which DiSalvo does not use (Gatehouse and Chatting, 2020). "*A black box contains that which no longer needs to be reconsidered, those things whose contents have become a matter of indifference.*" (Callon and Latour, 1981, p. 285). In this sense, black boxing is a practical approach to managing complexity. As Latour comments, "*The word black box is used by cyberneticians whenever a piece of machinery or a set of commands is too complex. In its place they draw a little box about which they need to know nothing but its input and output.*" (Latour, 1987, pp. 2–3). It is easy to consider that it is the black box that is opened or revealed by the process of hacking.

In a technical system the black box can be considered at multiple scales – from the very literal black boxes of the smartphone and the software modules to the data networks and other human and non-human actors. Black boxing can then be helpfully applied to the previous chapter's discussion of visibility, invisible labour and the specific engineering practices of modality and API definition. In describing our hardware hacking for the Family Rituals project, we explicitly attempt to break up, enumerate and publicly document with examples the technologies of the phone; although we only hint at the supply chains, agreements and infrastructures on which it existentially relies (Chatting, Kirk, *et al.*, 2017).

For designerly hacking, the objective of this is not to disarticulate every connection and reveal each black box in every respect, which is likely practically futile – there are black boxes within black boxes. Instead, it is enough to offer some partial understanding to suggest some new alternative reconfiguration. Indeed, the comprehensive disarticulation of a system will threaten its very stability and integrity.

Reconfigure the Remainder

DiSalvo's "*reconfigure the remainder"* seems more slippery. I interpret this as: to *put together*, *articulate*, *make finished*, *stabilise*, *settle*, *close-up* or to *enclose* something that has previously been disarticulated; reconfigured with a new intention. Reconfiguration is meant here in the sense of sociologist Lucy Suchman's Human-machine reconfigurations (Suchman, 2007) and the remainder refers to the work of feminist legal theorist Bonnie Honig (Honig, 1993). DiSalvo's examples of reconfiguring the remainder have a speculative or critical design quality, such as Kelly Dobson's Blendie (2004) which reconfigures the co-evolution of people and machines, here with a kitchen blender. DiSalvo's relatively insubstantial examples seem a little mismatched with a well-articulated theory. From a hacking perspective, the phone phreaker's Blue Box might again be a better alternative example of such a settlement; the use of tones for control was discovered, before a partial understanding was settled in an enclosure of commodified electronics and usable instructions written for a new audience to obtain free telephone calls (Rosenbaum, 1971).

In essence, this reconfiguration is a process of making new black boxes, enclosures that hide and expose alternative possibility – with appropriate annotation. Our Family Rituals account of hardware hacking takes this rather literally, enclosing the phone by "*selecting from an abundance of material properties (technologies and affordances), purposing and making them coherent and stable, and rendering those we disregard invisible.*" (Chatting, Kirk, *et al.*, 2017, p. 444). These techniques include masking the screen and extending the power button through the new case – in ways that are paralleled in James Pierce and Eric Paulos' Inaccessible Digital Camera (Pierce and Paulos, 2014). However, in some Family Rituals machines the black box was deliberately destabilized from the perspective of the participants. Notably in the telescope the family built the machine themselves from a set of flat-packed parts and were knowingly enclosing an iPhone. The cardboard construction material of the telescope contributed to this, making it somewhat provisional and open to adaption with everyday tools (Chatting, Yurman, *et al.*, 2017). Despite reasonable efforts, these hacks tend to create rather leaky black boxes with glimpses of the enclosed system – where a smartphone splash screen is visible for a moment as the device boots up. I have since come to think of our Family Rituals process as being a matter of putting *phones in [black] boxes*.

Daniel Weil's *Radio in a Bag* is an interesting play on the stability and inscrutability of the black box – where the radio's electronic components are unanchored (presumably risking short circuits) and visible through the transparent bag (Weil, 1981).

Designerly hacking is intended as a means of making alternatives beyond existing probable futures – some of those alternatives will be outright improbable, but more likely this is an exploration of the possible, assuming some slightly reconfigured conditions. This puts it at odds with Adversarial Design's more agonistic or counter-hegemonic framing. Designerly hacking is unlikely to inflict a fatal blow, to say Surveillance Capitalism, or even to engage in an open struggle with its adversaries; and for professional practitioners, legality constrains possibility further. Designerly hacking is then less adversarial and might create more plurality in mass-produced affirmative design, operate publicly as Critical Design or enable some private DIY-built response. If a military analogy needs to be made, then it is of guerrilla warfare. So while it is tempting to describe designerly hacking attempts to putting back together as reconfiguring the remainder, instead I shall next argue its intentions are better captured by Lamborn's outlying pirate utopias (Bey, 1991).

Temporary Autonomous Zones

The anarchist author and poet, Peter Lamborn Wilson, writing under his pseudonym Hakim Bey, describes TAZ: Temporary Autonomous Zones, in his book of the same name, as a tactic of disappearance (Bey, 1991). He depicts the pirate utopia; an autonomous enclave at the edge of the known world, outside the gaze of existing structures of power and its impositions – which can exist at least temporarily. This then is not freedom obtained through an adversarial struggle or even a guerrilla skirmish; it is a tactic to render oneself invisible and live freely. Domestically TAZ resonates with the castle doctrine's things that go on *behind closed doors* and Virginia Woolf's requirement for a door with a lock . While TAZ is a useful concept, Wilson is nonetheless a troubling figure, whose writing on paedophilia contextualises his own desire for invisibility.

Wilson's communique on the Temporary Autonomous Zones is penned in 1990 and while it refers to the Net and the Web, they are not meant in their modern sense. Net is the totality of all communication and information transfer, frequently embedded with hierarchical power structures, including the telephone, the postal system, public databanks, etc. The Web is a subset of the Net, but these are systems without hierarchy that afford freedoms; they include marginal zine networks and the nascent Internet technologies of the dial-up Bulletin Board System (BBS) networks. Like designerly hacking Wilson is looking for reconfigurations of these technologies and the counter-Net is the rebellious use of the Net – for say hacking and phone phreaking.

Wilson's discussion of the temporality or precarity of these zones is interesting as it acknowledges the dynamic nature of the world in which they seek to exist. The priority of the TAZ is to live in the moment, to exist rather than to wait for the revolution and some unobtainable utopian state. In so doing they can exploit rather short-term conditions, but that makes them a little precarious. There are clear resonances here with Brand's Shearing Layers in which superficial interventions will come and go – built as they are on shifting sands[42]. While more permanent change can only become established by a shearing process that carves its way into the status quo – probably rather visibly and slowly. Despite this seeming contradiction, by 1993 Wilson was contemplating the PAZ (Permanent Autonomous Zones), "*not all existing autonomous zones are 'temporary'. Some are (at least by intention) more-or-less 'permanent*" (Bey, 1993). Designerly hacking is often temporary, as it seeks to publicly demonstrate an alternative in the moment, but it can also inspire more permanent alternative (pluralistic) settlements, on which mass-produced design could be built.

The Family Rituals project illustrates this temporality; while the telescope worked for the deployment, it no longer works today. An iOS update was delivered automatically over the air, that required the home (rather than the power) button to be pressed to activate the screen. This button is inaccessible through the enclosure and so there's no way to turn it on once built. The attempted imposition of a new black box works for a moment but ultimately becomes itself unsettled by the network.

While designerly hacking as a method is ambivalent about the visibility (to the user) of technologies that are subsequently designed; this inquiry is explicitly concerned with the visibility and the TAZ tactic of disappearance as it is relevant to domestic struggles to be private. Specifically, it suggests possible responses to Surveillance Capitalism, enabled by Ubiquitous Computing, tactics to be invisible under the gaze of the system. It becomes clear that ubicomp's invisible computer demands a visible user. In ANT terms, the truly invisible utopian life of a pirate requires a severing or balkanization of the networks in which one exists; it is to be the cat inside Schrödinger's [black] box[43], whose actions and indeed existence has no consequences for the outside world and so is peculiarly free – at least temporally.

With respect then to *putting back together* Wilson's TAZ captures the intended pluralistic and temporary outcomes of designerly hacking, which speaks directly to my themes of visibility.

[42] Which in turn begins to sound very much like the *Parable of the Wise and the Foolish Builders*, Matthew (7:24–27).

[43] Minus the death inducing radioactive source!

Designerly Hacking: a methodology

Designerly hacking is a method that discloses new technical possibility in complex systems. It operates through close technical work that incorporates the products and methods of hacking, but with designerly intent. In essence it transforms hackerly forms into designerly forms to be manipulated in one's own design process or made public for the use of others. Hackerly here implies a set of technical competencies and aesthetic commitments, distinct from a (typical) designerly practice and distinct from a (typical) software engineering practice. As previously argued, hacking (and so designerly hacking) has two phases of activity: breaking up and putting back together[44] – and the previous discussion offered some theoretical framings for these. Crucially each phase consumes and produces different forms of knowledge and constructs different publics as they progress.

Pragmatically the activity of breaking up is likely to start with found hackerly forms, rather than original close technical work of one's own. These forms are likely to describe electronic circuits, software tools and libraries – rich in the technical details sufficient to allow one to reproduce and experience the hack. This process of reproduction is not always straightforward and may assume a degree of domain expertise and specialist tools – or the detail may simply be underspecified. Found hacks like these may be found and shared by the open-source community on the Internet – some are abstract technical demonstrations, others resolved for an often somewhat contrived use case. Instructables.com (2005) is a popular and useful example – a catalogue of curiosities, DIY projects and *outsider design*[45]. The activity of breaking up then first requires one to identify potential in these eclectic found forms, beyond perhaps what their authors envisaged. This may be achieved through first-hand experiences of the system in operation – through which one might expect to glean some material insight to direct some incremental deconstruction.

I consider computation/software/data to be a design material, but that is not uncontended (Franz and Papert, 1988; Gaver, 1991; Blevis, Lim and Stolterman, 2006; Vallgårda and Redström, 2007; Dourish, 2017) and this account is inevitably complicated by the ecology of the network (Ingold, 2012). Pragmatically, as a designer (and so a worker of materials) as I work with, in and through technical networks (as I have in my day-to-day practice over the past twenty years) I experience them as having material

[44] This breaking-up then putting back together also represents phases of diverging and then converging possibility, that is present in more familiar methodologies, like the Design Council's Double Diamond.

[45] By *outsider design* I mean design that seems to operate without the conscious referential practice taught in design schools.

qualities. In much the same way perhaps as the phone phreakers saw the telephone network. Furthermore, I suggest that any black box (whether or not it contains elements of the network) exhibits such material qualities when it is worked; how it transforms apparent inputs to outputs, how it acts temporally and in combination with others – perhaps sometimes unpredictably. From this perspective, one can then make an essentially behaviourist account of a black box or a found hack, without further decomposition.

So as a methodological activity breaking up some system one might initially create a collection of found hacks, then experience and document their material properties. This was intended by the taxonomy of exemplar phone hacks in the *phones in boxes* Family Ritual's paper, which drew from a diverse set of sources and once published was itself intended to be a public resource of found hackerly forms (Chatting, Kirk, *et al.*, 2017). Such a taxonomy itself offers a kind of temporary settlement, in which the relationships between hacks are identified, named and mapped.

Once some fruitful hack has been selected, there is then the process of putting back together; the material process of transforming hackerly forms into designerly forms. This should make new specific offers that shift a designer's conception of what is possible. It is likely that a different set of designerly tools and (new) higher-level representations are then implicated. In terms of technical work, it becomes a question of black box interface design, what is visible and legibly represented and what is hidden and inaccessible – what goes in and what comes out. Legibility implies the use of clear and consistent language, that supports the imposition of some new mental model, addressed to a designerly public. With this new settlement there is an implied stability. However, as previously discussed this may be necessarily temporary or deliberately be partially unsettled to allow some further modification, but now with designerly tools and competencies. This pliability might be a physical affordance for change – whether a cable is attached by a connector or soldered directly to the circuit board. It might be the ways in which the artefacts are annotated and documented or the functions that are provided through the API, that then shape how a public reacts to this possibility.

Beyond the internal technical settlements of what is put back together, its higher-level forms and representations have an important function, especially when this designerly hack seeks to operate publicly. These forms may be text, imagery or film – supplemented with code examples and circuitry. Made public through self-publishing (e.g. YouTube), journalism or academic writing. For the dissemination of Research Through Design annotated portfolio (Gaver and Bowers, 2012) and the pictorial publication format are useful forms. Similarly, Audrey Desjardins and colleagues have previously discussed the creation of DIY plans for documenting RTD inquiries (Desjardins *et al.*, 2017). DIY forms are appealing for designerly hacking in that they retain the technical detail, create an opportunity for use and suggest somewhat open-ended outcomes. Publications like the Whole Earth Catalog (Brand, 1968) and Nomadic Furniture (Hennessey and Papanek, 1973) add further historic waypoints for the popularisation of DIY responses.

To offer a short account of designerly hacking in action what follows is a short case study of where there are multiple phases of breaking up and putting back together and through which there are multiple transformations of hackerly into designerly forms – with at times large publics.

A Case Study: BT Balance

This is a brief story of BT Balance – a prototype I developed at BT Labs in the Broadband Applications Research Centre during 2006 and which received some public attention through coverage by the BBC and WIRED Magazine. While designerly hacking is a label retrospectively applied, it illustrates the method well, demonstrating transformations of forms.

In late 2005, on the pages of MAKE Magazine volume three, I found an article written by Tom Owad on a Tilt Interface (Owad, 2005). This described a hack of the Sudden Motion Sensor (SMS) in Apple's newer PowerBooks and MacBooks – a triaxial accelerometer used to detect falls and prevent damage to their electro-mechanical hard drives on impact. The hack allowed the raw values from this sensor to be read using a command-line tool called Amstracker (Singh, 2005) and interpreted as a motion controller in a game called Bubblegym (Berglund, 2005). I was able to run and experience the data produced by Amstracker, seeing how the values changes as I moved my PowerBook.[46]

I was curious to explore these interactions and worked on a way of getting the accelerometer sensor data into my own code. Amstracker was distributed as a binary file, without its source code. However, through online searches, I found Christian Klein's Motion tool for which the C code was freely available (Klein, 2005). At this time the language in which I was most proficient was Java and I converted Klein's code to run as a Java Native Interface (JNI).

At this point my friend Craig McCahill and I were discussing what we might exhibit at the newly formed Curiosity Collective's first public show. Craig had recently developed a puppet animation for his MA at Goldsmiths in Adobe Flash and we speculated that we could combine this with gestures from the laptop. By creating a socket server in Java, we collaborated to stream the sensor data into Flash which manipulated the animation accordingly. The Powerbook Puppet was born and we

[46] Gestural interactions would later become popularized with the launch of the Nintendo Wii (2006).

shared it on YouTube (Chatting and McCahill, 2005) with over thirty thousand views, showed it at the Curiosity Collective's Show One (August 2006) and distributed code for a simplified Java/Flash example online. Our project was covered by MAKE magazine, amongst others.

Back at BT Labs, our colleague product designer Martin Trimby had seen the Powerbook Puppet and made a connection with a brief for a broadband Etch A Sketch for older customers. Adam Oliver, Head of Age and Disability Research, wanted to build an Internet tablet device that would be, *as easy to use as an Etch A Sketch*. This would not be an Apple tablet[47] and so an external accelerometer would need to be found. Through the CHI conferences I was aware of Saul Greenberg's Phidgets (Greenberg and Fitchett, 2001); USB sensors (including accelerometers) and actuators that were straightforwardly integrated with code with well-defined APIs. I incorporated the Phidget library into my Java code and started building a new Flash environment in which to prototype interactions. These sketches included a book with flippable pages and a slippery map[48]. My Java code now added simple gesture annotations like left, right and shake to the data stream read by Flash – these prelabelled events made the interactions easier to code.

While Martin developed designs for the case, my first demos were given with the accelerometer board simply Blu Tacked on the front of the PC tablet. The first product renderings were of an integrated enclosure, but with a limited budget we decided that instead the accelerometer would remain separate. The resulting design referenced the desirable Zippo lighter – a little back box that plugged into the tablet to make it motion-sensitive. We called it BT Balance.

In April 2007, we issued a press release through the BT Press Office and the story was covered by the BBC and WIRED websites. In June the BBC Click programme featured BT Balance and for a morning we were on the front page of the BBC website. I subsequently published a short study of the interactional qualities of the map interface at Tangible and Embedded Interaction (Chatting, 2008).

[47] The Apple iPad would not be introduced until 2010.

[48] Inspired by the Tilty Tables I had seen at the Xerox PARC exhibition *XFR: Experiments in the Future of Reading* (Back *et al.*, 2001) and the Interaction Research Studio's *Drift Table* (W. Gaver *et al.*, 2004).

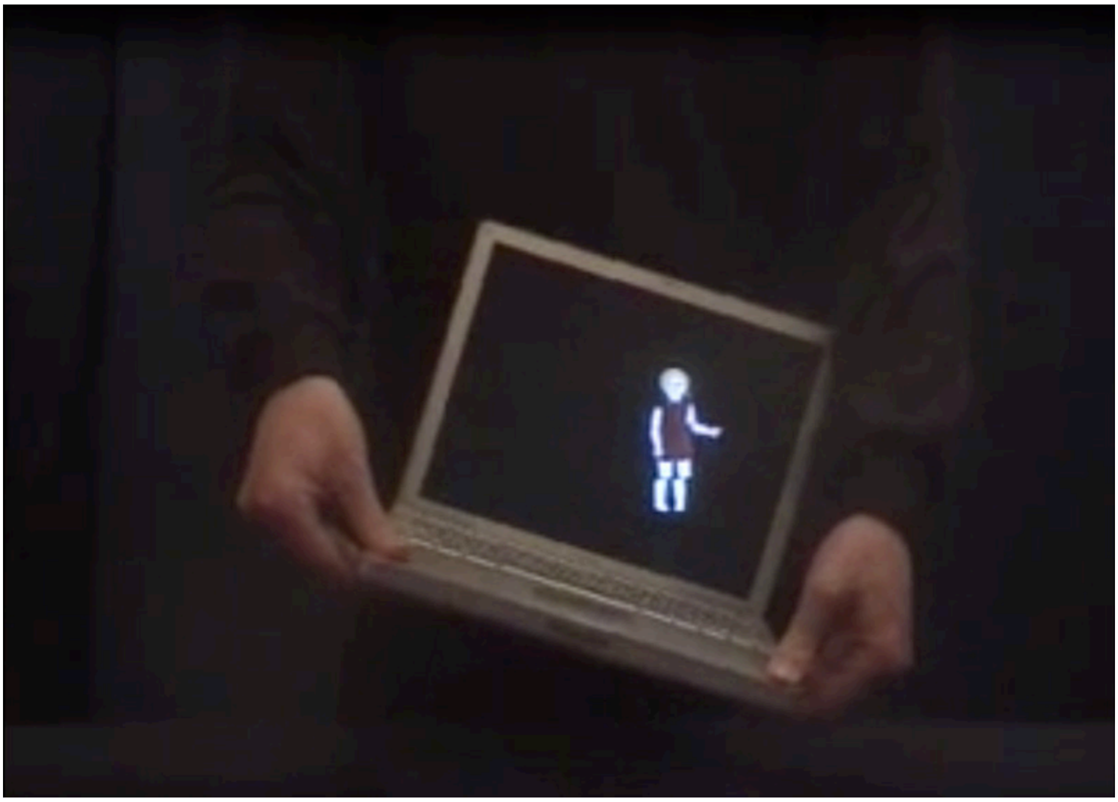


Figure 11. Powerbook Puppet. © David Chatting and Craig McCahill, 2005. Used with permission.

Figure 12. Andy Oliver using BT Balance. © BT, 2007. Redacted.

A Response to Surveillance Capitalism?

This chapter has also situated hacking in broader historic and theoretical framings, which has allowed designerly hacking to be positioned with respect to adversarial practices (Adversarial Design and Temporary Autonomous Zones) and to draw productively on Actor-Network Theory. Designerly hacking is not intended to be a prescriptive method, it is intended to surface pragmatic issues, tensions and opportunities when engaged in close technical work in a practice of Research Through Design. This chapter has described the methods I shall employ in seeking to design alternative networked homes. Two Research Through Design inquiries will constitute this work: Hack My House and the Home Network Study. Each builds on the existing methods for alternative domestic design and makes use of a new method of designerly hacking that discloses new technical possibility in complex systems and has been described at length here. Importantly this includes activities of breaks up systems to reveal something previously unseen (often as private close technical work) and then putting it back together in a public designerly form for the use of others.

Specifically, the alternative designs I seek respond to Surveillance Capitalism. The practice of designerly hacking should, by way of its close technical engagement, expose and disrupt what is hegemonic and otherwise unseen in complex sociotechnical infrastructures. For home networked stuff, this is the otherwise unwitting use of Cloud services, their collection of data and enablement of behavioural change, in the service of Surveillance Capitalists. Designerly hacking's production of public forms is intended to inspire other less technical designers and enable DIY responses by individual users alike.

This chapter has also situated hacking in broader historic and theoretical framings, which has allowed designerly hacking to be positioned with respect to adversarial practices (Adversarial Design and Temporary Autonomous Zones) and to draw productively on Actor-Network Theory. Designerly hacking is not intended to be a prescriptive method, it is intended to surface pragmatic issues, tensions and opportunities when engaged in close technical work in a practice of Research Through Design.

Chapter Five: Hacking my House

This chapter describes the first of the two studies in which I seek to reveal the struggles and invisible work of the networked home. This study, Hack my House, intends to disclose new technical alternatives in the networked home, specifically in my networked home. As it unfolds this initially solitary activity enrols others through a process of designerly hacking (described at length in the previous chapter) in which private hackerly forms are transformed into public designerly forms.

While a small network testbed would be a convenient site for my inquiry, it would lack the vital context and complexity of homelife that is the essence of the study. An autobiographical approach in my own home network is then a natural choice; where access and permission are uniquely available for extended periods of time – here for over three years. Significantly, living alone I can reasonably give my express consent for the interception of my own messages on my network, in ways it would not be possible in a participant's home. This is then a legal endeavour with respect to UK law and the Investigatory Powers Act (IPA) of 2016. Further being a rented home, this also gives me a first-person perspective on ways to assert a network of one's own, when one does not own the home.

While an autobiographical approach is uniquely well suited to studying the home network, it is not without its challenges: methodologically, practically and personally. The early phases of this study illustrate this point, challenges I then attempt to address through a regular series of hackdays at my house. These hackdays construct a small public for the products of my hacking and make an invitation to work with these materials in playful ways.

As an activity of designerly hacking this study starts by breaking up in private and finishes by putting back together in public – it transforms hackerly forms into designerly forms. However, in between these endpoints there is a long period where both activities occur in iterative material/immaterial engagements with the home to explore new configurations, both in private and in public, and when nothing is yet settled. This chapter charts such a transition of activity, offering a broadly chronological account of the Hack my House study. In doing so it is divided into six sections: the first describes early attempts to break up the home, materially and immaterially; the second gives an account of my private attempts to enact a hack of my Kindle's wallpaper; the third describes the series of designerly hackdays at my house with a small, trusted public and the artefacts we produced; the fourth documents the ways in which some of the products of these hacks were put back together in public and then reflects on the success of these forms; the fifth offers a discussion and the sixth finally makes some concluding remarks. In sum, this approach develops new technical alternatives in the networked home, which complements the Home Network study (that follows in the next chapter) which is then revealing of contemporary social struggles in the home.

Breaking Up My Networked Home: Early Explorations

Hack My House intends to reveal the networked home's struggles with technologies, in particular by showing the invisible work it implicates. Designerly hacking suggests a way to approach this by breaking up the system and opening its black boxes; however, the home is so complex it is still difficult to know where to begin and how to operate at an adequate scale and pace. Here again Brand's Shearing Layers offers a useful lens, especially with respect to the home's Services, Space plan and Stuff – the fastest-changing layers of analysis (Brand, 1995). This gives me some terms in which to make a first material account of the status quo, that might capture some of my home's complexity and create a domain for an immaterial account. So, this section first considers what is material and then what is immaterial about my networked home. While this could be seen as a straightforward act of accountancy, I intend something a little more evocative and poetic, in the spirit of Georges Perec's Species of Spaces (Perec, 1974).

My Material Networked Home

My Space Plan

Working with a tape measure and using an estate agent's document (found online) of an adjacent property, I created this map of my flat – see Figure 13. It shows the individual rooms, doors, windows and semi-permanent fixtures like the bath and cooker; in Brand's terms, this is predominately the space plan (Brand, 1995). It is reduced to two dimensions and does not show the heating, lighting, electrical or network services, nor does it show any of the Stuff or my life within. However, this plan does establish a material framework to view this domain and its limits – allowing me to reason about the whole and locate information within it. Drawn to scale in a vector file format (Abode Illustrator) it is conceivable that this digital form may be at some later stage be interpreted by a machine, perhaps employed by an algorithm to locate devices within the home given known locations of WiFi beacons that models the signal attenuation through walls.

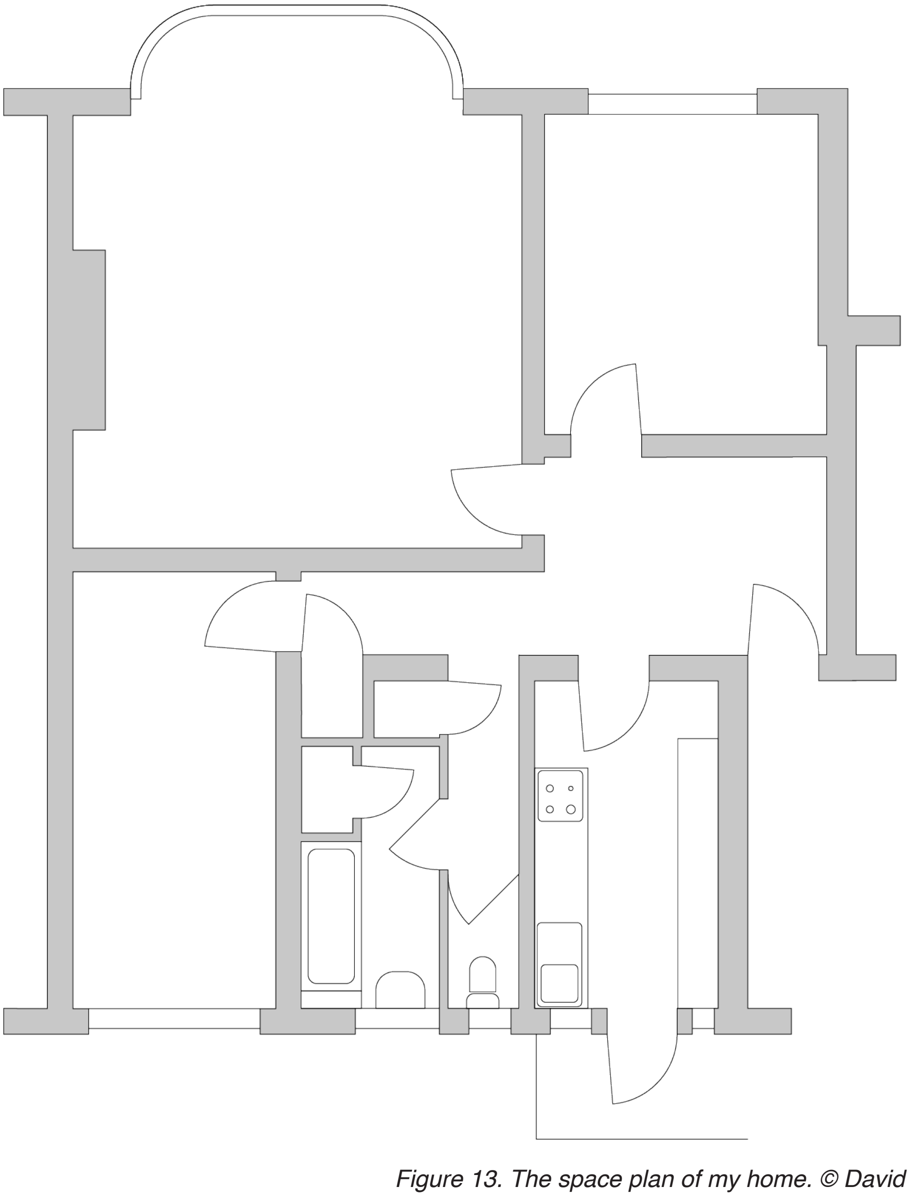


Figure 13. The space plan of my home. © David Chatting.

My Telephone Line

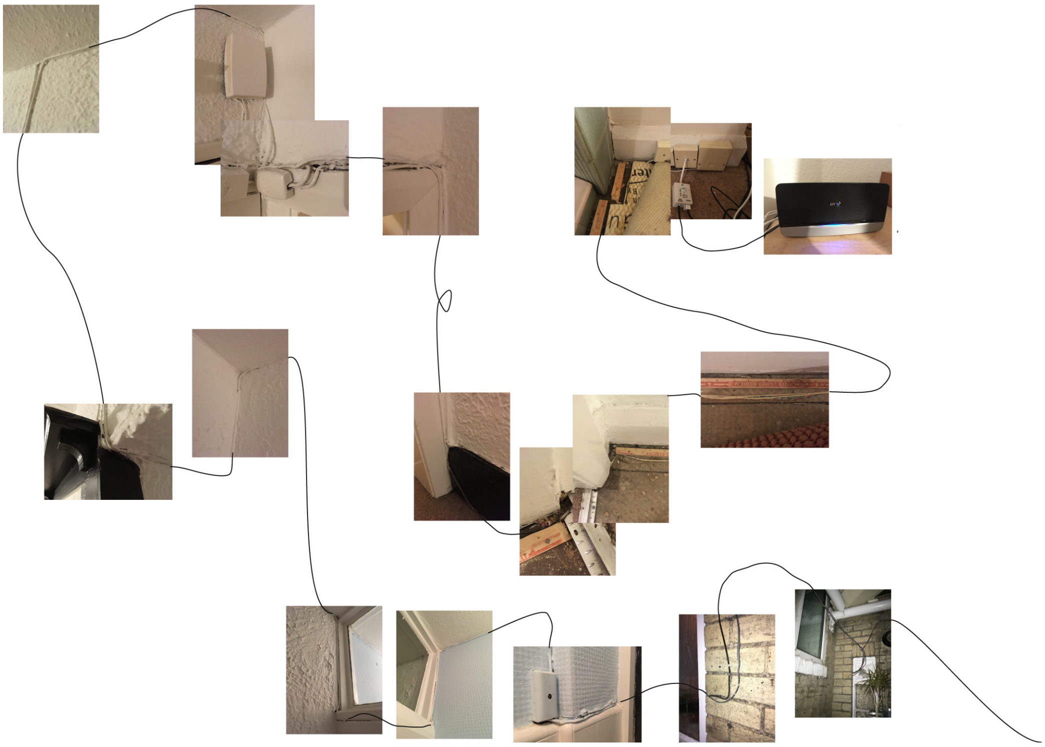


Figure 14. My telephone line. © David Chatting.

The Internet in my home is delivered over the telephone line and its reliable operation is crucial to my work and leisure; this is especially true as I write this during the time of the UK coronavirus pandemic lockdown in April 2020. I made this map of my telephone line as it enters and routes its way across my flat to my broadband router, it was created to understand a little better one of the critical material infrastructures of my home – see Figure 14. In Brand's terms, the telephone line is a service (Brand, 1995).

This activity is somewhat inspired by Ingrid Burrington's *Networks of New York - An Illustrated Field Guide to Urban Internet Infrastructure* (Burrington, 2016). In this book, Burrington walks New York to document the street furniture and road markings that can be interpreted to make the city's Internet infrastructure legible. She demonstrates that New York's modern networks are shaped by the networks and centres of power that preceded them; how its infrastructure uses the cable ducting and city architecture of the telegraph and telephone.

My telephone line starts on my balcony, outside my kitchen door, where it is found haphazardly flung across the rubbish chute. It is tacked lightly into the brickwork, before tunnelling through the wall to emerge above the toilet to enter a junction box, where there is evidence of an older cable that has simply been cut off. The line then heads off across the ceiling, over the toilet door and towards the hall. It does a circuit of the hall, passing as it goes a long disconnected external telephone bell (the 59D-1 bell component identifies this as dating from January 1980[49]), it is at all times ad hocly strung and has become painted into the fabric of the room over the years. Leaving behind yet more severed cables, it heads towards the floor and follows the line of the skirting board towards the living room. Coming through the door, it lays unprotected under the carpet where worn by years of footfall it has become unsheathed. Undeterred it finally emerges by the fireplace into a BS 6312 wall connector, bearing the post-privatisation logo of British Telecom (1980-1991). Through a DSL filter, the line is split between the landline telephone and the ADSL modem which then makes the Internet available wirelessly. My Internet as it turns out has an unexpected and unsettling precarity.

My Networked Stuff

Amazon Dash Button
Amazon Kindle
Apple iPhone SE
Apple MacBook Pro
Brionvega algol 3 12” Television
BT Home Router
Bush Radio
Cannon Printer
Dell Desktop PC
DIY Kyoto Wattson Energy Meter
Google Chromecast (Audio)
Google Chromecast (Video)
Google Home Mini
GPO Rotary Telephone 746F
Ikea Trådfri lightbulb (3 off)
JVC Hi-Fi and remote control
Nintendo Switch
Philips Clock Radio
Philips Digital Radio
Samsung TV and remote control
Sonoff Wireless WiFi Switch
Sony Playstation 4
Tivoli Audio Radio
UE Roll Speaker
Line-us – *the little WiFi robot drawing machine*
Violet Nabaztag – wireless rabbit
Wilko wireless doorbell
Withings WiFi Scales
Wolseley RF Programmable Room Thermostat

This is an inventory of all the devices in my home that somehow reach beyond

[49] https://www.britishtelephones.com/

themselves, that are in Brand's sense networked Stuff. This includes all the Internet connected devices, televisions and radios; but also, those that span shorter distances, such as the wireless thermostat control and TV remotes. Over the past three years of this work there have been some additions to this list (e.g. the Nintendo Switch), but several are unchanged for almost twenty years (e.g. the JVC Hi-Fi). While some devices are relatively new in my possession, they are older again (e.g. the GPO Rotary Telephone, a design from 1967 and working today). Some are in daily use, some are ignored; some like the Amazon Dash Button and Nabaztag have been made obsolete. Some others seem to have lost potential and lay abandoned in drawers – an old laptop, a broken printer and the like are excluded from this list.

This inventory then constitutes the technologies of my networked home. My struggles in this space will attempt to create new logics by which these devices coexist and relate to the world beyond the home and into the cloud. Some ways of struggling will modify the devices themselves, others will reconfigure the ways they exist in the network through their interaction with services. An enactment of such hacks will later require a more detailed understanding of each device's operation, but for now, it is sufficient to name, list, and wonder about them.

My Immaterial Networked Home

Having considered some of the material aspects of my networked home, I now turn to what is immaterial, to its Hertzian Space (Dunne, 2006) – notably to the radio signals of its WiFi network.

My WiFi Availability

Perhaps the principal way I experience my immaterial WiFi radio network is through its availability and reliability. Anecdotally, I could have told you that I can't make video calls on my balcony or that the Playstation needs to the wired via Ethernet to the router for online games to be responsive. The wireless router's signal strength is a good metric for understanding these observations and WiFi devices will generally make this available as the RSSI (Received Signal Strength Indicator) value. RSSI measures received power, such that near the transmitter the loss approaches zero and as the receiver moves further away it will decrease. RSSI is measured in decibels (or dBm) on a logarithmic scale; a value of -40 dBm is a good signal, with -70 dBm being much less reliable.

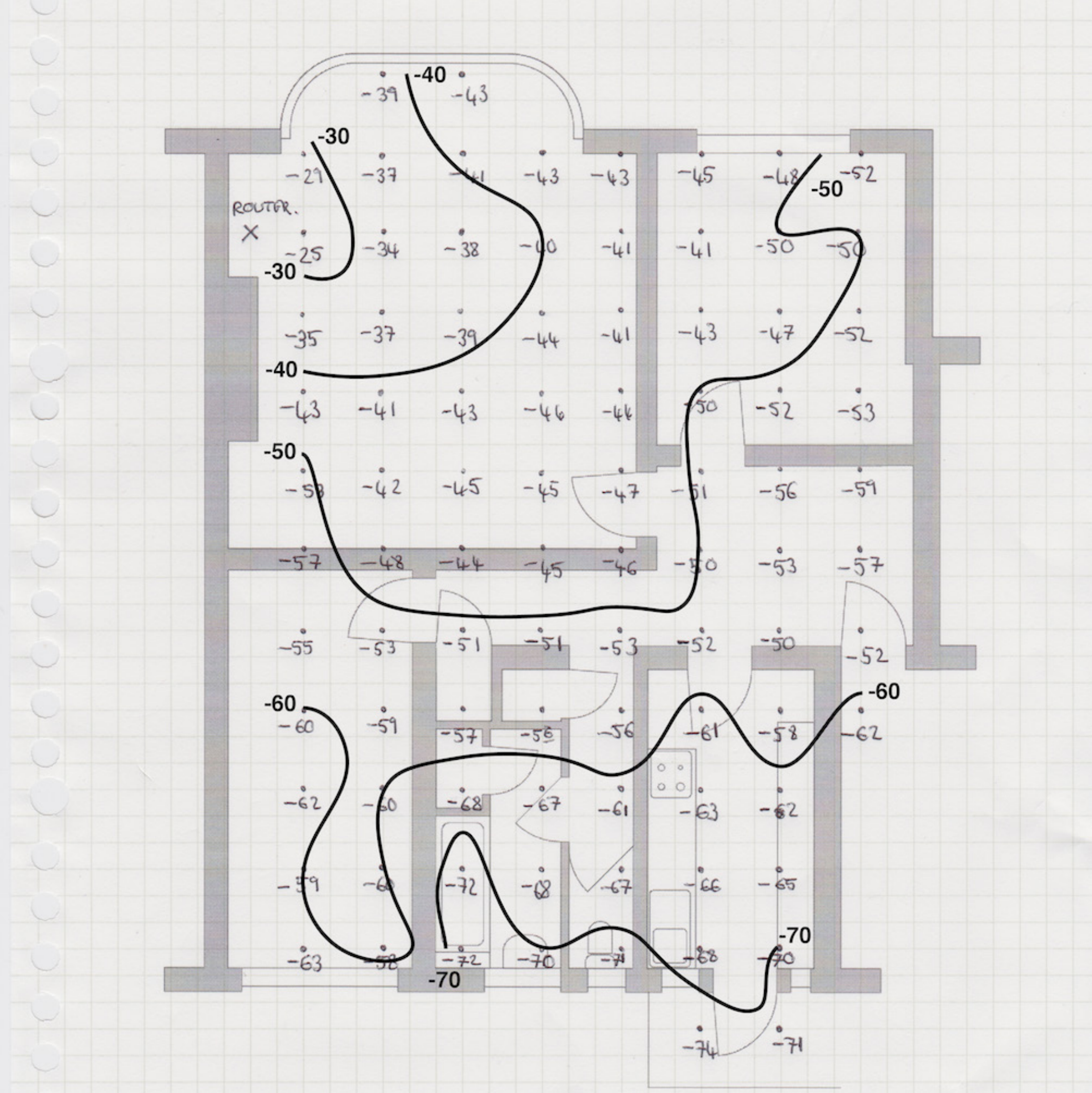
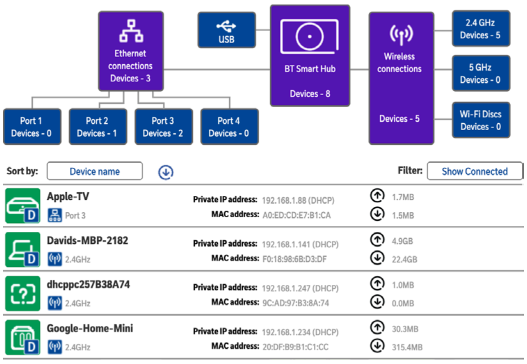


Figure 15. The RSSI landscape of my WiFi network. © David Chatting.

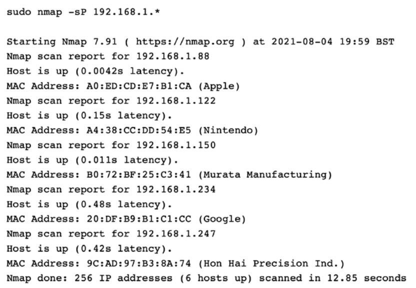
Using the space plan map I had drawn and measuring RSSI with my laptop, I surveyed the landscape of my WiFi network throughout my flat – see Figure 15. The contour lines begin to reveal how the physical building interacts with the radio signal and shapes my experience of the network.

My WiFi Network



Apple-TV Port 3	Private IP address: 192.168.1.88 (DHCP) MAC address: A0:ED:CD:E7:B1:CA	↑	1.7MB
		↓	1.5MB
Davids-MBP-2182 2.4GHz	Private IP address: 192.168.1.141 (DHCP) MAC address: F0:18:98:6B:D3:DF	↑	4.9GB
		↓	22.4GB
dhcppc257B38A74 2.4GHz	Private IP address: 192.168.1.247 (DHCP) MAC address: 9C:AD:97:B3:8A:74	↑	1.0MB
		↓	0.0MB
Google-Home-Mini 2.4GHz	Private IP address: 192.168.1.234 (DHCP) MAC address: 20:DF:B9:B1:C1:CC	↑	30.3MB
		↓	315.4MB

From the BT Smart Hub



```
sudo nmap -sP 192.168.1.*

Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-04 19:59 BST
Nmap scan report for 192.168.1.88
Host is up (0.0042s latency).
MAC Address: A0:ED:CD:E7:B1:CA (Apple)
Nmap scan report for 192.168.1.122
Host is up (0.15s latency).
MAC Address: A4:38:CC:DD:54:E5 (Nintendo)
Nmap scan report for 192.168.1.150
Host is up (0.011s latency).
MAC Address: B0:72:BF:25:C3:41 (Murata Manufacturing)
Nmap scan report for 192.168.1.234
Host is up (0.48s latency).
MAC Address: 20:DF:B9:B1:C1:CC (Google)
Nmap scan report for 192.168.1.247
Host is up (0.42s latency).
MAC Address: 9C:AD:97:B3:8A:74 (Hon Hai Precision Ind.)
Nmap done: 256 IP addresses (6 hosts up) scanned in 12.85 seconds
```

From the nmap tool

Figure 16. Views of my network.

Used under license, GNU GPL and Nmap Public Source License.

Having surveyed the immaterial availability of my WiFi, I next questioned exactly what was using this network. With access to the router this is quickly established via its administration webpage – see Figure 16. As well as enumerating the devices, it crucially provides the IP and MAC addresses of each. The IP (Internet Protocol) address is the Internet's underlying addressing scheme and is a string of four one-byte numbers (0-255), such that my Google Home's address is 192.168.1.234[50]. These addresses belong to the network 192.168.1.* – which are allocated and managed by the router and are unique only in this private network. To the wider Internet these devices are addressed through the router which has its own globally unique IP address. The MAC (Media Access Control) address is a globally unique identifier that is permanently assigned to the network hardware of the device. Typically it is shown as a string of six two-digit hexadecimal numbers – here my Google Home is 20:DF:B9:B1:C1:CC. The network operates to translate between these addresses so that data is routed to the correct recipient. Knowledge of these immaterial connections and specifically these two addresses allows one to consider ways to interact with these devices over the network – enabling a potential hack.

However, while the router page is informative it does not afford much further exploration. Instead, I turned to the abundance of free Unix command-line interface (CLI) tools, published under the GNU public licence, which enable one to explore the network in fine detail and accomplish close technical work. With these tools, there

[50] Strictly speaking this is a IP version 4 address, version 6 addresses are also used on my network.

are several ways to scan the devices on a network with nmap (Lyon, 1997) being a powerful option. In its most straightforward use, nmap will report the IP and MAC addresses of each device it encounters, it can be run on any client of the network and does not require privileged access to the router, unlike the previous administrative method. In more advanced use nmap can discover the individual services that a device offers to the network, perhaps a webserver that might then be exploited by a hack. I started by making a simple nmap scan of my network – see Figure 16.

In the Home Network Map project, I previously began to explore the use of these Unix CLI tools to create ways to experience the network – see Figure 17 (Chatting, 2017). The LED display creates a representation of the output of nmap (Lyon, 1997) and tcpdump (Jacobson, Leres and McCanne, 1989), running on a Raspberry Pi computer. The nmap tool is used to make periodic scans of the active devices on the network and tcpdump monitors or sniffs their real-time network activity. When a device is seen to be active the corresponding LED flashes[51]. Over time it is intended that these rhythms disclose some quality of the network's normal behaviour and the appearance of new devices and new patterns of interaction become remarkable.

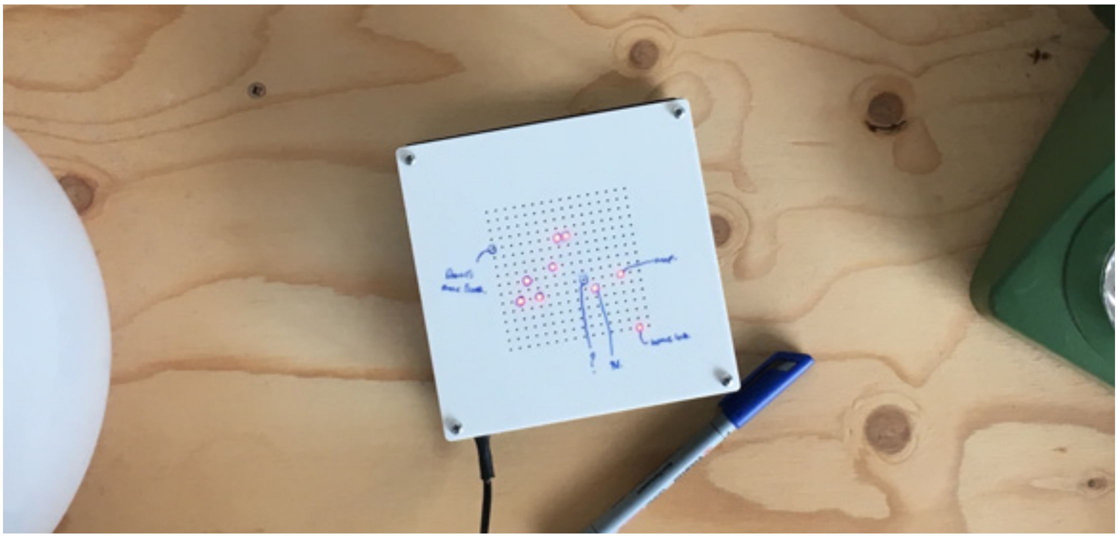


Figure 17. The annotated Home Network Map. © David Chatting, 2017.

The technique of packet sniffing used by tcpdump is analogous to radio frequency scanning. By operating the WiFi dongle in the *promiscuous mode* in which all network messages on this WiFi channel are received, whether or not this machine is the intended recipient. While in most circumstances the payload of these messages will be encrypted and inaccessible, the destination and source address may still be

[51] The final byte of the device's IP address, e.g. 192.168.1.141, determines which of the 256 LEDs is lit – in this case, number 141.

extracted, and this is sufficient to construct this kind of flight map. Packet sniffing is a useful technique in that it allows individual clients of the network to create unseen parasitic relationships with other clients.

```
sudo tcpdump

tcpdump: data link type PKTAP
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on pktap, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
14:35:32.798006 IP6 fe80::66cc:22ff:fedc:88f2 > ff02::1: ICMP6, router advertisement, length 88
14:35:32.916685 IP 192.168.1.141.mdns > 224.0.0.251.mdns: 0 PTR (QU)? 2.f.8.8.c.d.e.f.f.f.2.2.
c.c.6.6.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
14:35:32.916723 IP6 davids-macbook-pro-2182.local.mdns > ff02::fb.mdns: 0 PTR (QU)? 2.f.8.8.c.d
.e.f.f.f.2.2.c.c.6.6.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
14:35:33.209942 IP ec2-3-10-95-11.eu-west-2.compute.amazonaws.com.https > 192.168.1.141.52159:
Flags [.], ack 1858524223, win 13, options [nop,nop,TS val 31723888 ecr 2338599173], length 0
14:35:33.209991 IP 192.168.1.141.52159 > ec2-3-10-95-11.eu-west-2.compute.amazonaws.com.https:
Flags [.], ack 1, win 2048, options [nop,nop,TS val 2338609156 ecr 31718874], length 0
14:35:33.594764 IP 192.168.1.141.59978 > bam-8.nr-data.net.https: Flags [.], ack 2423043065,
win 65535, length 0
14:35:33.701237 IP bam-8.nr-data.net.https > 192.168.1.141.59978: Flags [.], ack 1, win 65535,
length 0
14:35:33.707913 IP 192.168.1.141.56452 > 192.168.1.234.8009: Flags [P.], seq
4278307968:4278308078, ack 1457318569, win 2048, options [nop,nop,TS val 2338609652 ecr
4426056], length 110
14:35:33.720022 IP 192.168.1.234.8009 > 192.168.1.141.56452: Flags [P.], seq 1:111, ack 110,
win 294, options [nop,nop,TS val 4426559 ecr 2338609652], length 110
14:35:33.720057 IP 192.168.1.141.56452 > 192.168.1.234.8009: Flags [.], ack 111, win 2046,
options [nop,nop,TS val 2338609664 ecr 4426559], length 0
```

Figure 18. Network traffic as seen by the tcpdump tool.

Used under license, BSD license.

The Home Network Map transforms the immaterial hackerly forms of the Unix CLI software tools (Figure 18) into a designerly material form – here represented as a short description text and a photograph of the device in vivo (Figure 17). In doing so much is hidden with the display rendering just the essential properties. The fundamental question of which LED represents which device demands exploration for which the white acrylic surface affords mark-making with a semi-permanent marker pen. This then allows a material annotation of the immaterial, a little like the Interaction Research Studio’s listening glass probe (W. W. Gaver *et sal.*, 2004; Boehner, Gaver and Boucher, 2012).

The Unix CLI tools allow me to materially engage with my home network in close technical yet open-ended ways; the Home Network Map is suggestive of ways of transforming such hackerly forms into designerly forms.

My Tuneable Reality

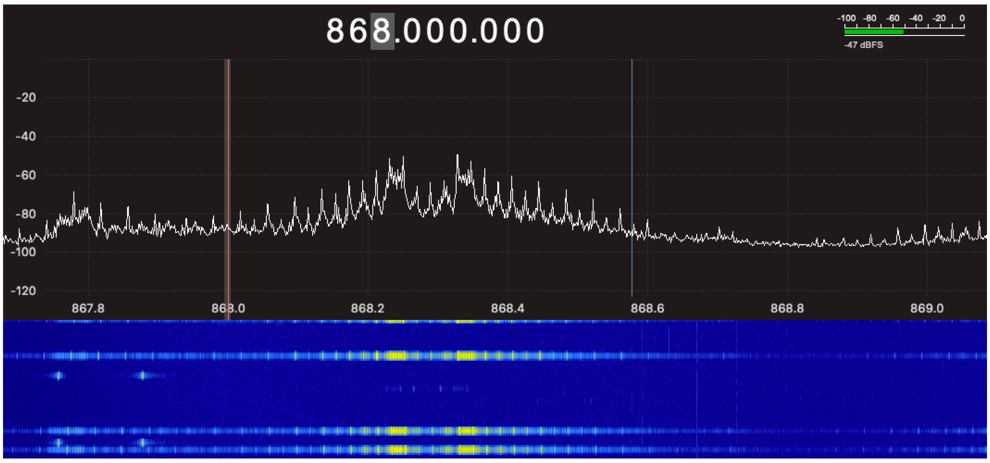


Figure 19. Waterfall visualisation of boiler activity, recorded by the gqrx tool. Used under license, GNU GPL.

Besides WiFi, my networked home is defined by an immaterial landscape of radiated radio and light waves. Each has a frequency along the electromagnetic spectrum, with broadcast FM radio between 88 to 108 MHz, terrestrial television from 45 to 215 MHz, mobile telephony from 800 MHz to 2.6 GHz, WiFi at 2.4 or 5 GHz and infrared light in excess of 300GHz. Perhaps less obviously, there are frequencies (notably at 433 and 868 MHz) for low power domestic data use, for instance used by wireless doorbells. In Dunne's terms, this is the home's Hertzian Space, that can be experienced through a Tuneable Reality (Dunne, 2006).

The technology of Software Defined Radio (SDR) makes the exploration of the tuneable home possible. In contrast to an inflexible hardware radio, an SDR can be tuned and the signal decoded by simply changing software commands, rather than electrical components. This then allows one to semi-automatically scan a wide band of frequencies and survey the electromagnetic landscape. With a full SDR transceiver, a signal may also be transmitted under software control at a specified frequency.

Until recent years SDR has been prohibitively expensive for the student or hobbyist. However, in 2012 it was realised that the cheap ($25) mass-produced TV tuner USB dongles, based on the RTL2832U chipset, could be hacked to receive any broadcast between 64 and 1700 MHz (Nardi, 2019). The online RTL-SDR community[52] quickly grew and began to share the software tools they had developed and their experiences of receiving and decoding the signals that they found. These included tools for decoding satellite imagery and aircraft ADS-B broadcasts, but significantly also tools for the domestic data frequencies.

[52] https://www.rtl-sdr.com/

Using an RTL2832U USB dongle and the RTL-SDR software I was able to partially map my home's Hertzian space; my boiler, wireless doorbell and energy meter all operate at these domestic data frequencies (433 and 868MHz). Using the gqrx (Csete, 2012) tool I confirmed the periodic broadcast from my boiler at 868.292MHz and the waterfall visualisation shows this in time running vertically and frequency horizontally – see Figure 19. Using rtl_433 (Larsson and Zuckschwerdt, 2012) I was able to extract data from these signals – if not determine precisely the meaning of the message. However, with this hardware it is impossible to transmit, so the interaction is only one way.

In running these tools, it became apparent how busy these frequencies are in an apartment building like my own and how my walls do not define the territory. Intriguingly my neighbour's cars are regularly broadcasting their tyre pressures and temperatures!

The Loneliness of a Designerly Hacker

Having revealed some of the material and immaterial aspects of my networked home, I started to enact some private hacks within it; this section describes my attempts to change my Kindle wallpaper and reflects on the challenges of such autobiographical work.

Changing my Kindle Wallpaper

As an early deliberated hack, that informed my conceptualisation of designerly hacking, I was drawn to the Amazon Kindle, the electronic book reader with an e-ink display from the online retail giant. The Kindle exemplifies nicely a notion of domestic networked Stuff: small, battery-powered and wirelessly connected to the Internet – with the mobility to seamlessly move from inside to the outside of the home. The infrequently changing non-emissive e-ink display is at one with the environment of the object and the room, it does not create its own artificially lit reality – the object seems materially changed by the display. When on standby the Kindle becomes an advertisement. To me this seems a greater intrusion than the ephemeral flicker of a TV ad; an object I own has become changed in ways I do not control and runs counter to my sense of home, to William Morris' maxim, "*Have nothing in your houses that you do not know to be useful, or believe to be beautiful*" – described in Chapter One. So, it became my desire to digitally replace the Kindle adverts with wallpapers from Morris' cornflower series. I assumed this would be a relatively trivial and quick demonstration of my inquiry's values. Instead, as it turned out, over several ad-hoc months of struggle it slowly began to glean understandings of the network beyond the Kindle and suggested alternative possibilities for the Internet of Things (IoT). A version of the account given here was published in the paper *Inarticulate Devices: Critical Encounters* *with Network Technologies in Research Through Design* at the DIS (Designing Interactive Systems) conference (Gatehouse and Chatting, 2020).

So, with a degree of chutzpah, I made my initial Google searches. These showed that from the introduction of the Kindle with Special Offers in 2011, the first model with WiFi at a discounted price for carrying adverts, people had devised ways to block or replace these adverts. Two broad routes were suggested; to modify the Kindle itself or to modify the network of linked resources in which it exists. To modify the Kindle would likely require that the device become rooted (a hack that allows root administrative full access to the filesystem) that would likely need the case to be opened and some hardware modification to be made. The modification of the network would require some hacking of the local WiFi network, making changes to the local router to trick the Kindle into taking William Morris wallpapers rather than Amazon advertisements. It is the network that defines my interest in this Stuff and so I looked at ways to hack the local router.

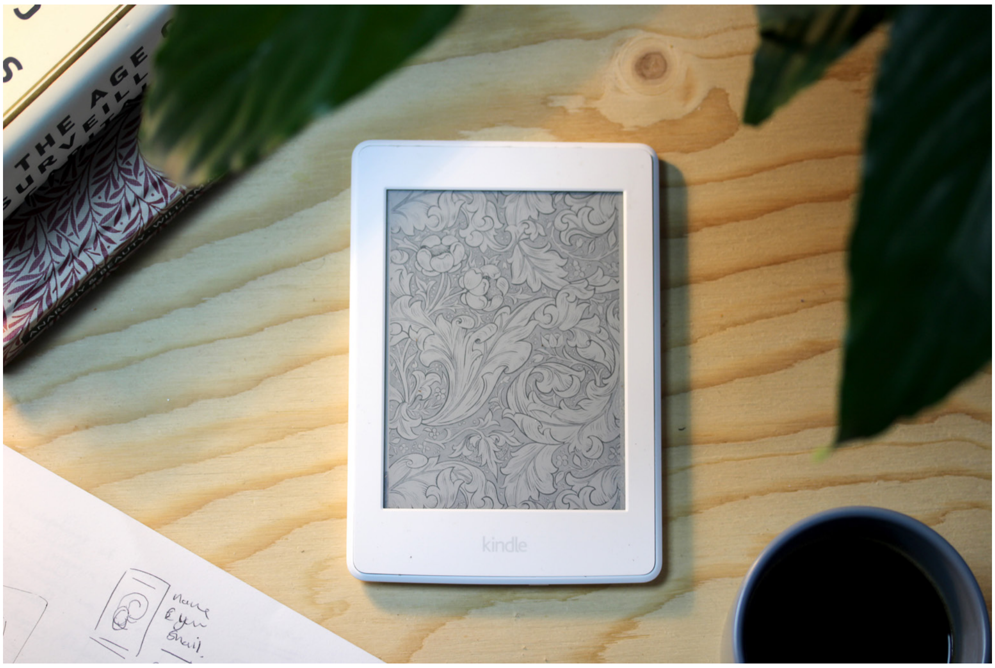


Figure 20. Kindle with William Morris wallpaper. © Cally Gatehouse, 2020. Used with permission.

Through my online searches, I discovered two pieces of software that were quickly written and shared in 2011 to replace the advertisements delivered to the Kindle with any image saved in the common gif format – these being pwnazon by Michael Shepard (Shepard, 2011) and k4freeserver by Piero Toffanin (Toffanin, 2011). They were distributed as source code, in the well-known PHP and Ruby languages respectively; copies of both are currently still available on the popular GitHub platform. The scripts are short and with some programming knowledge one can gain an understanding of their operation through simple inspection.

Pwnazon and k4freeserver operate in identical ways, the Kindle proactively makes HTTP (Hypertext Transfer Protocol) web requests for image content from the identifiable server adpublisher.s3.amazonaws.com which returns an image in gif format. This transaction is intercepted, and an alternative image is delivered. The HTTP web request is the same mechanism by which an image is delivered to a web browser and is an extremely common way by which data of all kinds is transferred by all manner of connected things.

This intercept of advertisement images relies on a key infrastructure of the Internet, that of DNS (Domain Name Servers). DNS is the means by which a computer's domain name is translated into its associated IP (Internet Protocol) address – the Internet's underlying addressing scheme. This is how for instance www.amazon.com is resolved to 13.32.69.252. A DNS request will be made at the start of a communication; initially with the local router and then if unknown there, with well-known DNS machines at the heart of the Internet. Pwnazon and k4freeserver both rely on changing the local DNS server on the home router, such that when the Kindle makes a request for adpublisher.s3.amazonaws.com it is returned with the IP address of a local machine running a spoof website serving alternative imagery; thus circumventing Amazon's servers. In a similar approach, specific domains can be effectively blocked by rewriting the local DNS record for a domain as unknown, this is how network-level ad-blocking software such as Pi-hole works (Salmela, 2014) by preventing devices on the network from contacting a list of well-known advert-serving websites. I had a good understanding of this mechanism as I began this exploration.

My home router's DNS log showed a long list of the servers my Kindle was interacting with. Even the domain name amazonaws.com – the AWS (Amazon Web Services) – hints at the enormity of the Amazon cloud-based collective on which the Kindle invisibly hangs and contributes its data. The DNS entries included those for time, software updates and messaging services – as well as a regionalised advert service for Europe. A little more of the infrastructure was revealed to me. I could block all the adverts from adpublisher-eu.s3.amazonaws.com by simply rewriting the router's DNS record. However, when I tried to use pwnazon and k4freeserver to replace the imagery I was frustrated, they no longer worked. By reading articles on Stack Overflow and other online forums, it became clear that in around October 2013 Amazon had changed the firmware on the Kindle, in an Over-the-Air software update, so that rather than using HTTP it now used HTTPS (Hypertext Transfer Protocol Secure). The Kindle's web requests were now secure. The consequence of this, which I had not previously understood, is that the device verifies the identity of the server it is talking to and then encrypts its messages such that only that recipient can read the data. As such the Kindle rejects the local machine's attempt to impersonate the Amazon server. A different strategy was required, which would need me to develop some deeper understandings of HTTPS.

With an HTTP exchange the source destination and data payload of every message sent by any device on the network is inspectable by all on the local network or at any point between the server and client – using tools such as Wireshark (Combs, 1998). This includes the full URL of the resource, any parameters – including usernames and passwords and the contents of the reply – for instance HTML or image data. Everything in the HTTP exchange is readable and could be modified or stored in transit, without the knowledge of either server or client. Further, the client is offered no guarantees on the authenticity of the server's identity – all of which was exploited by pwnazon and k4freeserver.

While I knew that HTTPS was in some cryptographic sense secure and to be trusted for bank details and the like, I had no detailed understanding of it as an exchange of messages. Some rudimentary reading offers that, HTTPS implements TLS (Transport Layer Security) a cryptographic protocol that authenticates the identification of the remote server and then encrypts all the traffic between the two[53]. So, requesting a resource from a server becomes a multi-stage process as these details are negotiated and certificates exchanged and verified. As I discovered, this means that in inspecting the HTTPS traffic between the Kindle and Amazon only the destination hostname and destination IP address are visible – with an encrypted payload only simple statistics like length and rhythm can be discerned from the exchange (Amar et al., 2018). Modification of payloads becomes impossible, and as a result, I cannot change the wallpaper.

With a so-called man-in-the-middle (MITM) attack it seemed I could, perhaps, intercept and decode the Kindle's HTTPS traffic, but to do that I needed to get the Kindle to accept a modified Certificate Authority (CA) certificate. Such certificates are issued by a set of well-known trusted Certificate Authority servers. However, with access to the device's filesystem, these CA certificates can also be locally installed and so they will verify the false identity of the MITM machine. This required a change to the device and not just the network in which it finds itself. A bewildering set of forum posts documented how this might be achieved; each dependent on a slightly different model of the device and version of the operating system. Nothing worked for me. It was a deeply frustrating experience. There seemed to have been a window of time in past when the wallpaper hack had been possible, but no more.

Running out of options it was with some reluctance that I finally opened the Kindle's case to reveal the circuit board[54]. It seemed that with the right wires soldered to the PCB

[53] TLS is commonly but strictly incorrectly referred to as SSL (Secure Sockets Layer), the protocol it succeeded.

[54] Indeed, I slightly damaged the screen in doing so.

and through the right USB adapter I could open a teletype terminal with the Kindle, that Levy's MIT hackers would have found very familiar. This revealed the Kindle's Linux kernel and gave me my last shot at installing a CA certificate on the filesystem. However, once I had this view, a curious thing became apparent: the downloaded ad images were actually stored in a hidden directory that would be accessible to my laptop when the Kindle was connected as a USB drive. I plugged my Kindle in, navigated the filesystem, and then replaced all the image files; lo and behold William Morris' cornflowers filled the screen. However, the blooming was temporary and 20 minutes later the Kindle had downloaded new adverts in their place. Amazon's hegemony was rapidly restored. Ultimately, I was able to modify the Kindle's behaviour from the outside, but only through knowledge gained from the inside by breaking open the black box.

My encounters had revealed a tangle of online infrastructure and authority; and questions of on whose behalf security operates. Similarly, Hill and Mattu had found, "*all the connected devices [are] constantly phone home to their manufacturers*", but many of these conversations are encrypted. So, while it is possible to see that there is an exchange, it isn't easy to tell what is being sent. The security, ostensibly for privacy, has the effect of excluding us from a knowledge of the operation of our own devices. Hill and Mattu commented, "*When you buy a smart device, it doesn't just belong to you; you share custody with the company that made it*" (Hill and Mattu, 2018).

Through my interventions, I had begun to witness how this network resisted and enabled my efforts. Seen retrospectively as a process of designerly hacking, the inquiry did operate through found hacks and tools, that developed my private critical understanding of secure protocols for domestic networked Stuff and produced public imagery (Figure 20) and a commentary by way of a publication (Gatehouse and Chatting, 2020), however it did not substantially deliver new public designerly forms. Furthermore, the outcome was too temporary to enact any lasting change in my home. All in all, it had been a long and at times lonely trudge.

Autobiographical Challenges

While I have argued an autobiographical approach is uniquely well suited to studying the home network, it is not without its challenges: personally, practically, and methodologically. In this section I have necessarily imposed a logical narrative on my activities, but this has largely been apparent in retrospect. In the moment, it could be confusing, frustrating, and seemly unproductive. The sheer open-endedness of hacking a complex system like a networked home can become quite overwhelming and difficult to manage in a timely way. Much of what was done stays undocumented and unfinished, and so hard to articulate in later design work or even acknowledge as being work. As an autobiographical solitary pursuit, this close technical practice was self-resourced and self-directed – reliant on my own skills, materials, and time. While the triumphs were then personal, so were the setbacks.

While autobiographical or first-person methods are known to HCI, they are somewhat unusual. Audrey Desjardins' ongoing practice has perhaps the most relevance to this thesis in this regard. Desjardins' thesis describes her experiences of *living in a prototype*, a van she designed and then lived in with her partner (Desjardins, 2016; Desjardins and Wakkary, 2016). Subsequentially with Aubree Ball, through Ball's development of a domestic ludic communication system for her family, Desjardins identified methodological tensions in autobiographical design studies (Desjardins and Ball, 2018). These tensions are synthesised with respect to the few explicitly autobiographical HCI works and scholarship from the previous decade (Cunningham and Jones, 2005; Gaver, 2006; Neustaedter and Sengers, 2012; Desjardins and Wakkary, 2016) – furthermore, they argue that implicit autobiographical aspects of work have been historically under-documented in HCI.

Desjardins and Ball's summary of autobiographical design and identification of five methodological tensions (genuine need, participation, privacy, co-shaping design and research, and authorial voice) helps me to reflect on my own inquiry in these terms and is suggestive of ways of alleviating some of the challenges my early explorations faced. Critically for Hack my House, design and research can be co-shaped over an extended time with periods of contemplation in one's own home. Yet this can result in tensions with homelife and this needs to be approached mindfully. There are also several significant points of divergence which recalibrate the importance of their five tensions in my work. Hack my House seeks to generate unresolved technical alternatives rather than working prototypical solutions and it does so in a private single-occupancy home. My inquiry is more concerned with exploring a valid ecology, rather than studying how new designs are lived with – so the questions of genuine need, participation with designs, and authorship are then somewhat diminished in importance. Furthermore, Desjardins and Ball's concern with the participation of others and their privacy is moderated where autobiographical work (as here) is conducted in private. However, considering my attempts to hack the Kindle wallpaper, it suggests the presence of this tension might be productive – that a public might create some constraints and focus the open-endedness.

So, while the Kindle hack was resolved to a degree and does offer insights that shape my thinking – its shortcomings have perhaps more significantly informed the way I have subsequentially conceived designerly hacking in general and the Hack my House inquiry in particular. How can I scaffold my exploratory autobiographical hacks with accountability and deliberation? How can one approach autobiographical designerly hacking with self-care? In the next section, I shall describe a format for hacking my house in public which makes some suggestions.

Hacking with Friends: Hack my House Hackdays

To mitigate some of the challenges of my autobiographic inquiry that I have highlighted in describing the Kindle wallpaper hack, I conceived a lightweight workshop format inviting participants to *Hack My House*. These were loosely structured as a series of irregular hackdays with a small group of trusted friends, who were invited to come and make something playful with the products of my hacking. I would not have been willing to open my home and my network to strangers. Over the course of five events, nine friends (Dan Foster-Smith, Andy Garbett, Cally Gatehouse, Kyle Montague, Tom Schofield, Diego Trujillo Pisanty, Tim Sargent, Tim Shaw, Mike Vanis) came to hack my house, each with broadly designerly practices, working with software, electronics and networks, and with a mixture of academic and commercial experiences. Most returned on repeated occasions.

While these hackdays might seem to share some features of a participatory design workshop (Taylor and Clarke, 2018), they were explicitly designed not to operate as such. The focus was not on the generation of design concepts, but more obliquely on how a designerly public responded to and shaped the products of my private hacks. Outcomes were not intended as nuanced critical responses to the networked home per se, but instead to surface ways of engaging with these materials through the experience and expertise of others – allowing me to draw on a wealth of technical and creative insights. This shares some intention with Tim Shaw and John Bowers' concept of public making (Shaw and Bowers, 2016) – indeed Tim participated in Hack My House #5.

This is not the typical way in which a hackday might be expected to proceed, especially for those familiar with the hackathons described in Chapter Four – where there is likely to be a clear outcome, a competitive element, and maybe even a little hacking. Without a clearly stated objective, my concern was in keeping my friends engaged, fearful that they would otherwise think it a waste of their time. In this sense, I recognised early that a critical role for me on the day was as the host, responsible for curating materials to simulate their curiosities, as well as providing meals, snacks, cups of tea and coffee. Each day closed with a wide-ranging audio-recorded group discussion before we shared a take-away meal and some beers.

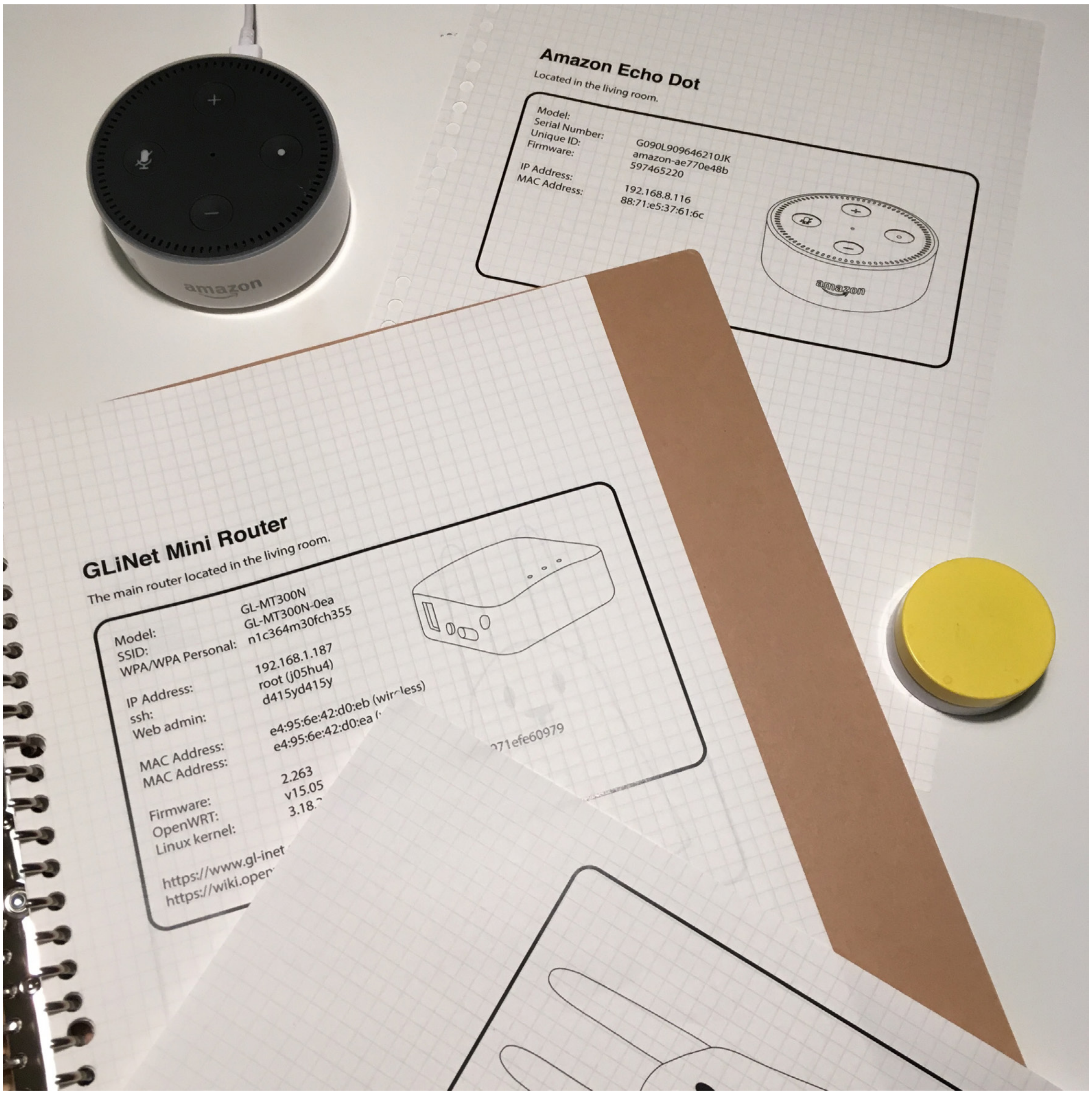
The durational format of these hackdays also marks them out from the typical participatory design and hackathons models. This allowed conversations to develop between us and engagements to change with the materials of the home and our interventions. Most importantly it built a degree of public expectation and critically some deadlines for my private hacking. This gave my work focus, as I found ways to make my network available to facilitate others to make rapid developments; in doing so I exposed, documented and curated the new technical potential that I was revealing through my ongoing hacking.

While it was refreshing to break from the hackathon model and return to an open-ended technology-led exploration of possibility, the Hack Day Manifesto (Knell, 2012) did prove a valuable reference in designing the Hack My House format. It contains some clear pragmatic advice on provisioning resources like power sockets and WiFi, making APIs and datasets easily available to participants, being explicit about potential issues like intellectual property (which remained with the participants), as well as a reminder to keep it fun!

From an ethical perspective the workshop presented few concerns. However, it was unusual in a number of respects that warrants some brief reflection. Firstly, being in a private space (a rented flat) I was mindful of the participants' safety ensuring that safety certificates, insurance policies and evacuation procedures were up to date. Secondly, being my own home, I considered my own safety and privacy; all the participants were already well-known to me professionally and socially, so a trusting relationship could be assumed. Thirdly, elements of hacking practice are illegal when exercised against a third-party's property, but here the focus is my private home network for which I can reasonably grant permission – external systems (like webservers) were not in the scope of the hackdays. Lastly, in catering for my participants I was careful of dietary requirements, allergies and intolerances. The application for ethical approval was granted by the Department of Design at Goldsmiths in October 2018; it is included in the appendix.

With some motivation established, the remainder of this section now describes how these *Hack My House* days unfolded and the design work they structured. I present a sequence of activities and hacks that are largely chronological with the intention of demonstrating the interplay between them. However, some activities were developed over long overlapping periods so there is some tension in a linear narrative. Activities previously described as designerly hacking are to be seen throughout this long-term exploratory material/immaterial engagement with the home. The final section of this chapter concludes by considering how these hacks then became more settled as they are put back together in public.

The House Handbook



Amazon Echo Dot

Located in the living room.

Model:
Serial Number: G090L909646210JK
Unique ID: amazon-ae770e48b
Firmware: 597465220

IP Address: 192.168.8.116
MAC Address: 88:71:e5:37:61:6c

GLiNet Mini Router

The main router located in the living room.

Model: GL-MT300N
SSID: GL-MT300N-0ea
WPA/WPA Personal: n1c364m30fch355

IP Address: 192.168.1.187
ssh: root (j05hu4)
Web admin: d415yd415y

MAC Address: e4:95:6e:42:d0:eb (wireless)
MAC Address: e4:95:6e:42:d0:ea

Firmware: 2.263
OpenWRT: v15.05
Linux kernel: 3.18.

https://www.gl-inet
https://wiki.open

71efe60979

Figure 21. The house handbook. © David Chatting.

In preparation for the first Hack My House workshop, I began to assemble a handbook for my house that would document the networked Stuff I had identified and the ways they might be hacked. My intention was to produce something close in spirit to a DIY manual for my home. For each device I created a single page detailing serial numbers, firmware versions, MAC addresses, account details, APIs, software tools, etc. In the workshop this was made available as an electronic PDF document and as a ring-bound paper copy. Individual pages made it easily shared and annotated during the workshop. Useful annotations made on paper were incorporated into the electronic document after the event and in this way the handbook evolved over the series of workshops.

While many of the devices had a network addressable interface, most were proprietary and while accessible not publicly documented by the manufacturer – so-called private APIs. However, a large online community reverse-engineer these devices, publishing the interfaces they find and the software control scripts they write under non-profit licences on the Internet. In preparation for the first workshop I installed and documented as many of these scripts as I could find (and make work) on the network. I limited my documentation to software hacks that ran on and altered the network, interoperating through the device's public and private APIs, rather than altering the device's firmware to change its behaviour.

To integrate these found scripts I hosted a webserver on a Raspberry Pi and wrote endpoints to call these functions. An endpoint is a URL that specifies an action the server will take when presented with data of a specified type and format, containing the parameters required for its operation. Figure 22 illustrates the JSON formatted data I defined to control my Ikea Trådfri lights via the JavaScript ikea-tradfri library (Stanford, 2017). In this way control of disparate technologies like the Chromecast and Trådfri lights were consolidated in a single web[55] API (a collection of endpoints) running on a single Raspberry Pi – such that the network appears to have but one node. Knowing that many of the workshop's participants had professional experience with web technologies and tools, in particular with JavaScript (Eich, 1995) and Node.js (Dahl, 2009), made the choice of these technologies for the web API straightforward – allowing easy integration of familiar software, workflows and practices. By documenting this single interface in the handbook, the intention was to bring together the ways these disparate devices are addressed and create some coherence – I was attempting to create some stability to these hacks by establishing a new black box. Through this API every device is primarily addressed by its MAC address in the same message format and the code translates this to meet its own requirements. I hoped that simplifying the orchestration of multiple devices might facilitate workshop participants in creating Rude Goldberg like machines – which, as previously discussed, seem to demonstrate an alternative orientation to the visibility of complexity. I wanted to facilitate participants to make interventions that operated on the home network without the cloud or even the Internet – without resorting to remote services like If This, Then That (IFTTT)[56].

[55] Web here implies an HTTP (Hypertext Transfer Protocol) server.

[56] https://ifttt.com/

```
{
    “mac”: “b0:72:bf:25:c3:41”,
    “values”: {
        “bulb”: {
            “name”: “Globe Lamp”,
            “isOn”: “true”,
            “brightness”: 20
        }
    }
}
```

Figure 22. JSON formatted data to control Ikea Trådfri lights

As I found in my explorations of the home’s *Hertzian Space*, several of my networked devices do not use WiFi. For devices like the Hi-Fi controlled by infrared, I installed an IR module on the Raspberry Pi so that the device could be controlled and triggered across the network. Similarly, the Wattson Energy Meter is not online but can be addressed as a serial device by a second networked Raspberry Pi. As described, the activation of the wireless doorbell and thermostat is controlled by radio frequencies, at 433 and 868 MHz respectively and these can be detected by SDR radio software using an inexpensive TV tuner module – again on a networked Raspberry Pi. In this way, bidirectional WiFi bridges can be formed for these devices and in turn, they can become incorporated into the single web API, which becomes the lingua franca for the wider networked home.

Over the series of hackdays, the handbook and API evolved. They became a focus of my efforts and how I made sense of new possibilities, integrated them with those already established and questioned what did not yet exist. Through this process of API design, common syntaxes are imposed and linguistic expectations emerge as more functions are incorporated. These designerly forms represented ways of creating a temporary settlement and imposed a meaning to the potential exposed through hacking the network. The Home API, as it became, is described at the end of this section.

Hack My House #1

The first Hack My House was a one-day workshop situated at my house (of course) with four participants (Andy, Cally, Tom and Kyle); all have academic practices working in software and electronics with a design or artist focus. This was my home and these were my friends, people I could trust and who I hoped would be comfortable going beyond the obvious. It was a Saturday and it needed to be relaxed and fun; no one was being paid. The day ran from 10 am to 6 pm, there was plenty of food; we shared a takeaway meal and some beers afterwards.

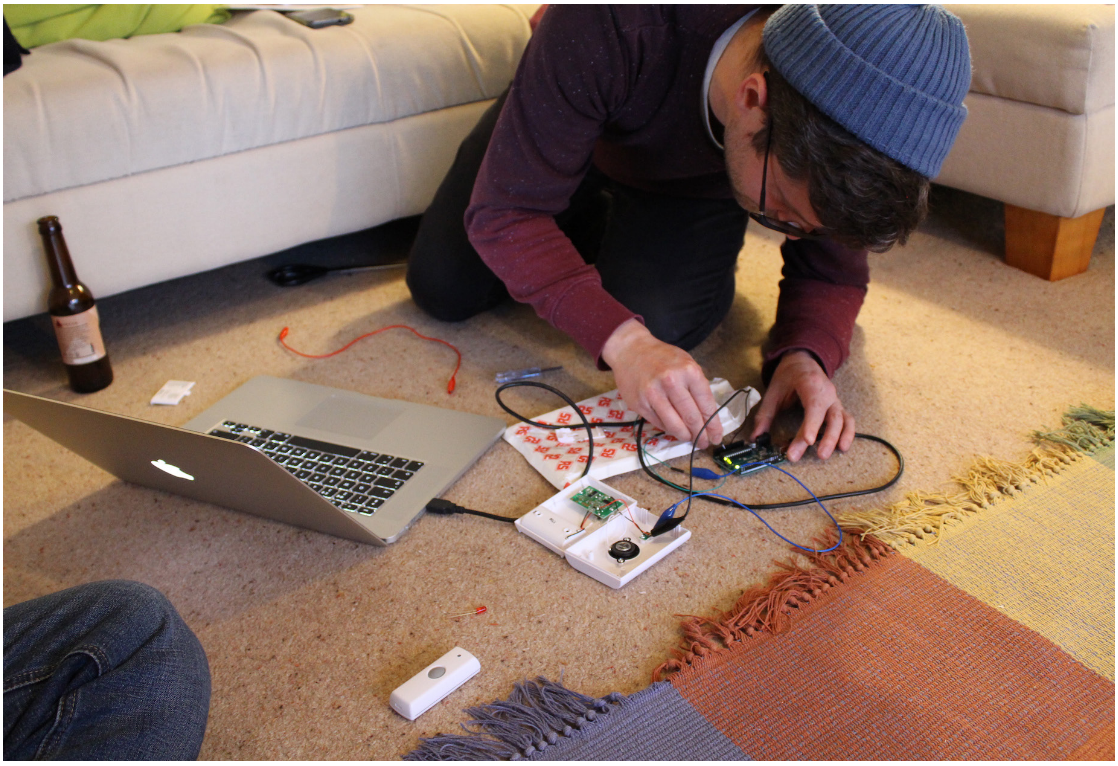


Figure 23. Hack My House #1. © David Chatting.

The day was lightly structured. I gave an introduction and suggested a loose design brief – to hack my house to demonstrate something, "*useful or useless, funny or shocking on the home network*". Beyond that, there was no direction to use specific things in the house or particular technologies to achieve the effect. I provided a printed copy of the handbook and gave a tour of each room of the house, pointing out what might be co-opted. I set up some basic collaboration tools: a private GitHub code repository, Dropbox for file sharing and a Slack channel for messaging. In addition to my home devices, there was an array of electronics and microcontrollers available (Arduino and Raspberry Pi) with a soldering station. Throughout the day we worked on a series of explorations, both individually and in pairs, using resources that I'd facilitated and others the group had made available. We also shared our ideas and tools; significantly Andy showed us Postman (Asthana, Sobti and Kane, 2014) a tool for testing and documenting web APIs. Not everything worked to plan, my Internet regularly buckled under the demand of five people, but we worked through it in good humour.

During the workshop, tinkering seemed to be an easy and satisfying activity for the group. Over the afternoon, as hoped, we created a Rube Goldberg like IoT machine. This proved a nice collaborative way to proceed, where each of us took an element of the machine and created a trigger for the next stage. In our final demonstration, the wireless doorbell triggered a picture to be taken and displayed on the television, whilst there is the sound of a barking dog. See Figure 24. This diagram (produced for this thesis) offers some rational context for this in situ, an IoT security trope, but in truth, the machine was quite absurd with its elements strung loosely together on my living room floor – it was this that we found so enjoyable.

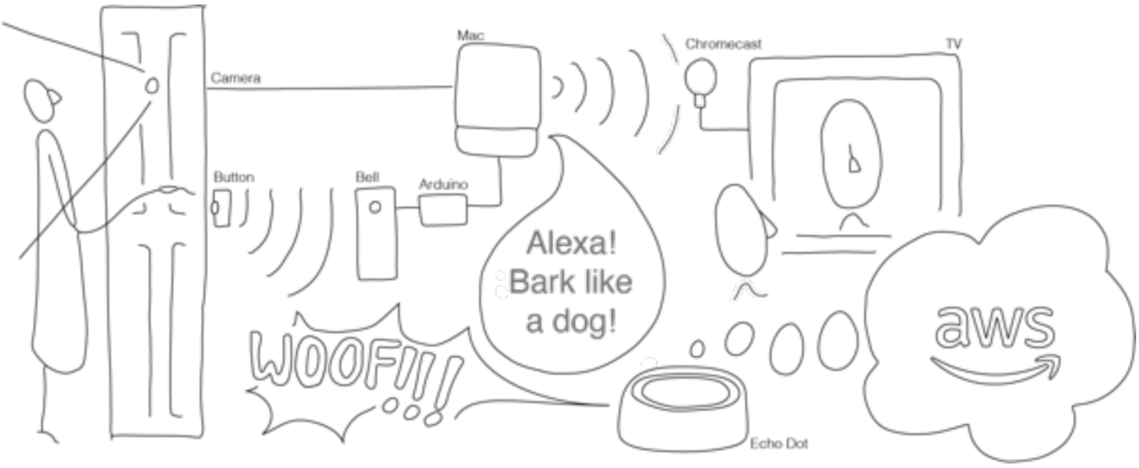


Figure 24. Rube Goldberg like doorbell machine. © David Chatting.

To briefly examine this machine in terms of DiSalvo's articulation one must consider how the elements are joined and form the chain or network (Figure 24). The doorbell button produces a radio frequency signal at 433 MHz, which is received by the Bell unit, wired to the Arduino and read over USB by the Mac laptop. This then: requests an image from the camera; uses my web API to send the image to the Chromecast, and speaks aloud a command for the Echo Dot – using the macOS say command – "*Alexa! Bark like a dog!*". The Echo Dot reaches into the cloud (the Amazon AWS) to interpret the command and makes the appropriate sound. There are two bridges to the network established here: how the Bell is integrated via an Arduino; and secondly, the ad hoc articulation between the Mac and the Echo Dot via a synthesised voice.

At the end of the day, we had successfully built something together and that seemed important. We had produced some code and some interesting experiments, but it was also clear that this was both unresolved and that we were enthusiastic to repeat it. Crucially I had also found a way to make my hacks less solitary and deliberate, whilst not making unreasonable or onerous demands of my participants, my friends.

Over the weeks that followed, I revisited critically the outputs of the first workshop and considered how to structure a second event. The experience gave me the impetus I had been seeking.

The Router of All Evil

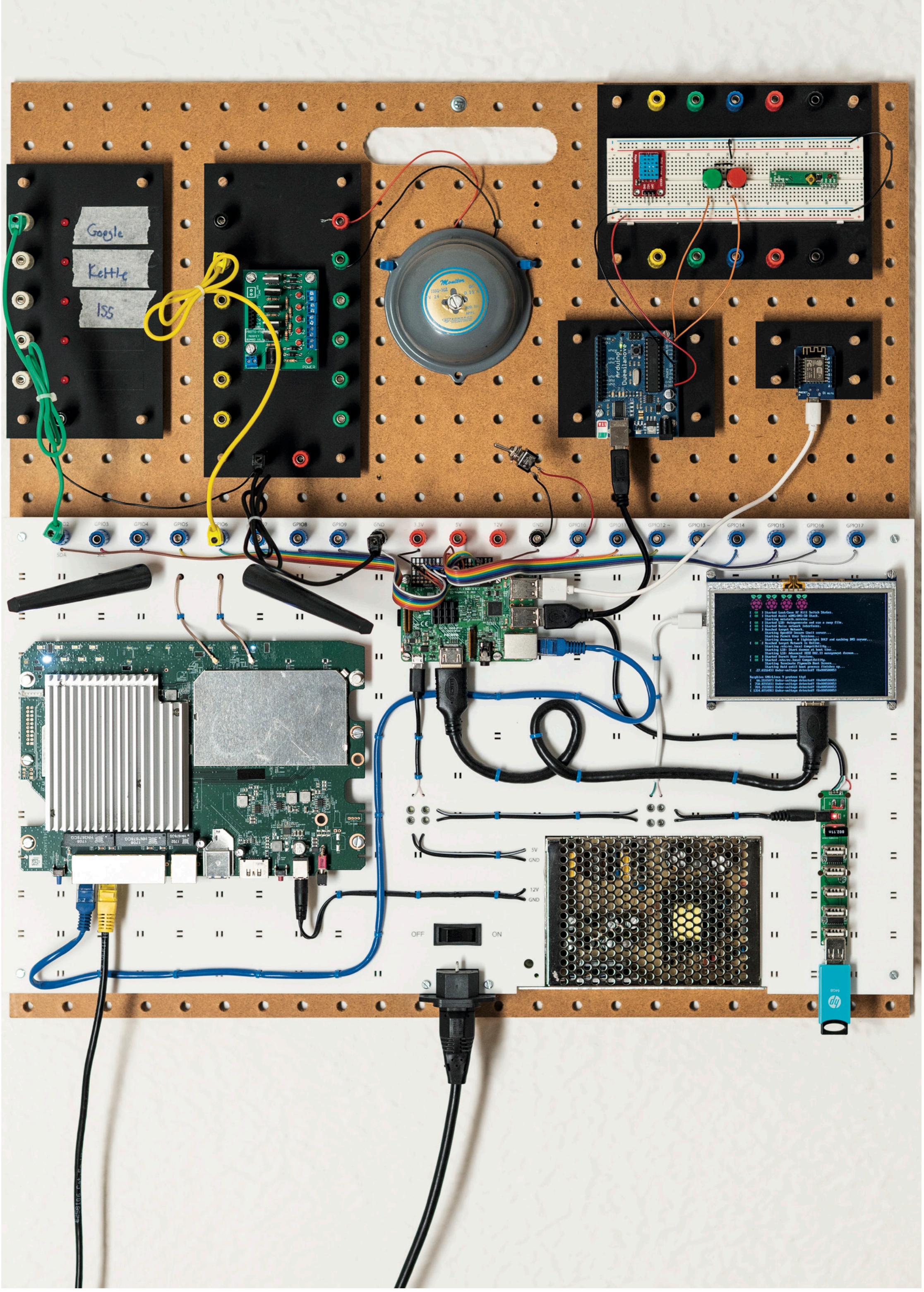


Figure 25. The Router of All Evil. © David Chatting.

For the first workshop I created a new WiFi network HackMyHouse using a mini wireless router (GL-MT300N) attached by Ethernet to my ADSL modem. Aware of the tensions in autobiographical work with homelife, I had separated this experimental space from my day-to-day network. The router was installed with the OpenWrt operating system, a popular Linux distribution allowing customisation of the routing software that might enable messages to be intercepted and modified. A similar approach was taken by Hill and Mattu (Hill and Mattu, 2018) in their Gizmodo article *The House That Spied on Me* – as described in Chapter One. However, the first workshop demonstrated that the mini wireless router was incapable of serving my home network with five resource-hungry hackers. While the use of OpenWrt would have been technically possible, nobody had explored ways of modifying the router preferring more self-contained hacks using scripts running on their own laptops.

To address the throughput of the router I purchased a Linksys 1200 AC router with a considerably higher technical specification than the GL-MT300N. The Linksys router was also able to run OpenWrt, but the installation required that the circuit board be removed from its enclosure to reveal a serial connector required to transfer the new firmware; this was a literal opening of the black box to reveal a new possibility. This process importantly suggested an alternative way that the router could exist, open not only to software configuration but also open to hardware modification.

The enhanced specification of the new router and its Linux-based operating system suggested that some of the functions previously served by the Raspberry Pi (namely the web API) might now be run on the new router. However, the Raspberry Pi creates many new possibilities with its abundance of hardware (HDMI screen, audio, Bluetooth BLE, WiFi and GPIO) and readily available software packages. So instead, the router and the Raspberry Pi became tightly coupled but separate and this combination became known as the Router of All Evil [57].

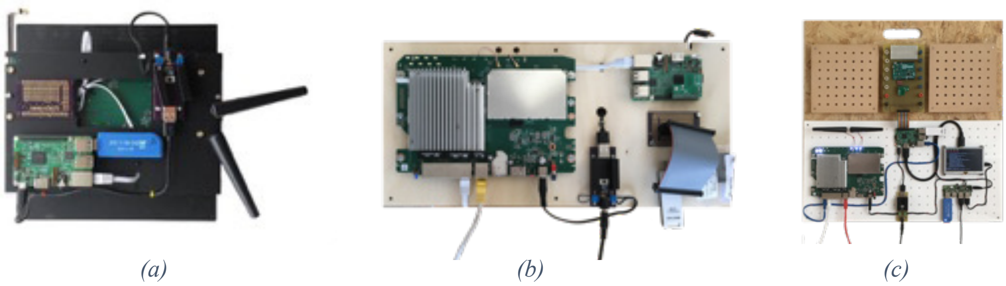

(a) (b) (c)

Figure 26. Hardware iterations of the Router of All Evil. © David Chatting.

[57] The Router of All Evil plays on the biblical proverb that, *"the love of money is the root of all evil*". The pun was suggested by Kyle and stuck, communicating perhaps a little of its counter-cultural spirit.

There were four major hardware iterations of the Router of All Evil (Figure 25, Figure 26) over the course of a year and through three Hack My House Workshops, that concluded with the final version see Figure 25. Its purpose was to support ways of experimenting with and reconfiguring the home network. In the first, the router and the Raspberry Pi were simply stacked with a 5" display into a compact semi-open unit (Figure 26a). Inside the Raspberry Pi GPIO was broken out on a bespoke PCB, there was a breadboard for electronic prototyping and a common power supply (on a second bespoke PCB) for the router and the Raspberry Pi. The router remained outside of its box and the circuit boards were attached to laser cut acrylic plates. This design reflected my then developing ideas of layers of mutability or pliability. The top layer, the display, could be changed rapidly and superficially by software; the middle layer accepted hardware changes; and the bottom layer was the bedrock of the router. I saw this as an expression of Brand's Shearing Layers (Brand, 1995), introduced in Chapter Two or more precisely his later Pace Layer model (Brand, 2018). However, at this early stage, this was an exploration of form and these potentials were not fully realised.

The second iteration of the router disassembled the stack of layers and laid out these same components on a single laser-cut plywood plate (Figure 26b). The cables between the components were neatly stowed behind. While this exposed all the elements the articulation between them was out of sight and the layout felt restrictive, rather than expansive and open to change. This led quickly to the third design.

The motivation of the third iteration of the router was to give each circuit board adequate space and allow the cabling between them to be visible (Figure 26c) and so improve legibility. I designed a laser-cut white acrylic cable board able to accept cable ties on a 1" pitch grid, which itself was mounted to an OSB (Oriented Strand Board) square plate (60 by 60 cm) – which was now large enough to warrant a handle. This version integrated an Arduino on a self-etched PCB where each of its input/output pins was broken out to a binding post. Sensors and actuators could then be assembled on the breadboard or pegboard panels. The PCB also allowed Raspberry Pi hats (expansion boards) to be plugged in. The Arduino was chosen for GPIO as it has more interfacing options than the Raspberry Pi, specifically it can read analogue sensors and operates at 5-volt logic, rather than the less common 3.3-volt. The power supply PCB was similarly reproduced on a self-etched PCB. Unfortunately, there was an unresolvable technical problem with the Arduino prototyping board and the power supply circuit ran too hot, the router was drawing too much current for the circuit. Furthermore, despite its large size the physical prototyping area again felt restrictive – the pegboard panels being quite small. These considerations motivated the fourth and final design.

The final iteration of the Router of All Evil (annotated in Figure 27) attempts to resolve the practical challenges of the previous versions and to embody more directly my notions of prototyping with layers of mutability which I shall later describe as Pace Layer Prototyping. Working from the bottom, the router transforms the infrastructurally delivered mains electricity via a new overly provisioned power unit into the 5-volt and 12-volt supplies that power both the router and the Raspberry Pi, with enough unprovisioned current for additional electronic circuity. The Raspberry Pi GPIO is now delivered directly to the edge of the cable board, via a row of labelled binding posts – with the power occupying the central posts. Binding posts were chosen as they allow both a connection by a plug and also by clamping a bared wire. The prototyping board was abandoned in favour of a more flexible arrangement of an Arduino mounted on an acrylic panel for the newly expansive pegboard (attached via USB) and a second panel for a larger breadboard.

The separation of the two areas demonstrates two ways of prototyping, one at the top in hardware and by software configuration below. While the hardware of the router has been opened up and unboxed, it has been laid out and made stable, a new logic is suggested for it. The pegboard area affords a range of responses – some by the ad hoc attachment to the board, others through the development of new panels that formalise the hacks (page 179). Similarly, the router's software layer offered new ways of enacting change, notably through the development of the Home API (page 180) and the later turn to the Node-RED environment (page 171).

The router was then a convenient site for hacks of the network, both for hardware and software, able to co-opt the existing devices of the network around the home in different ways – to create new logics between them. The House That Spied on Me (Hill and Mattu, 2018) and the privacy-friendly Candle Smart Home project (Schep, 2019) share this observation. However, I also wanted to be able to explore novel devices in different contexts in the home, with a view to designing new connected electronic Stuff

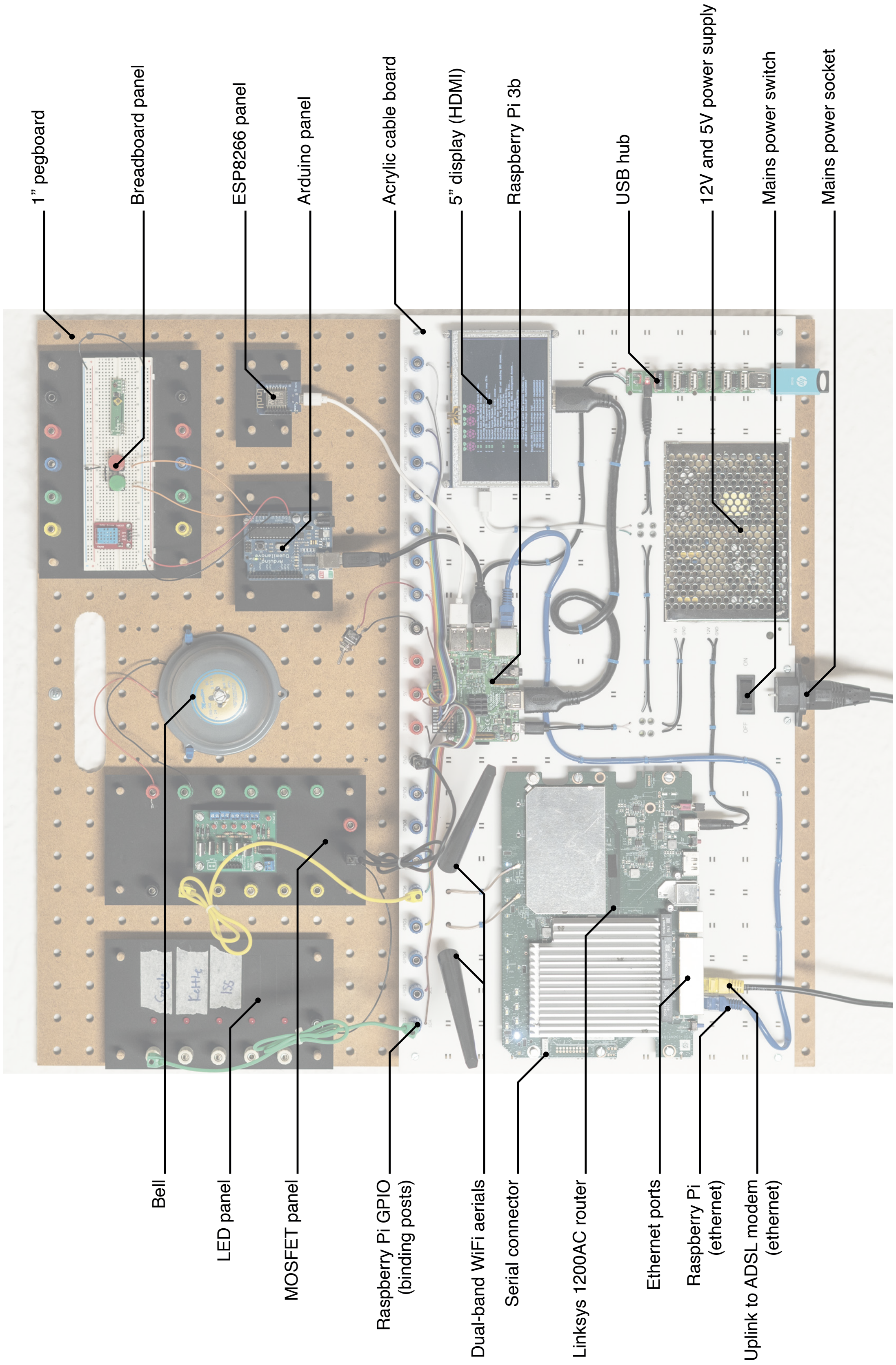


Figure 27. The Router of All Evil – annotated. © David Chatting.

Humidity Sensor (PCB version)

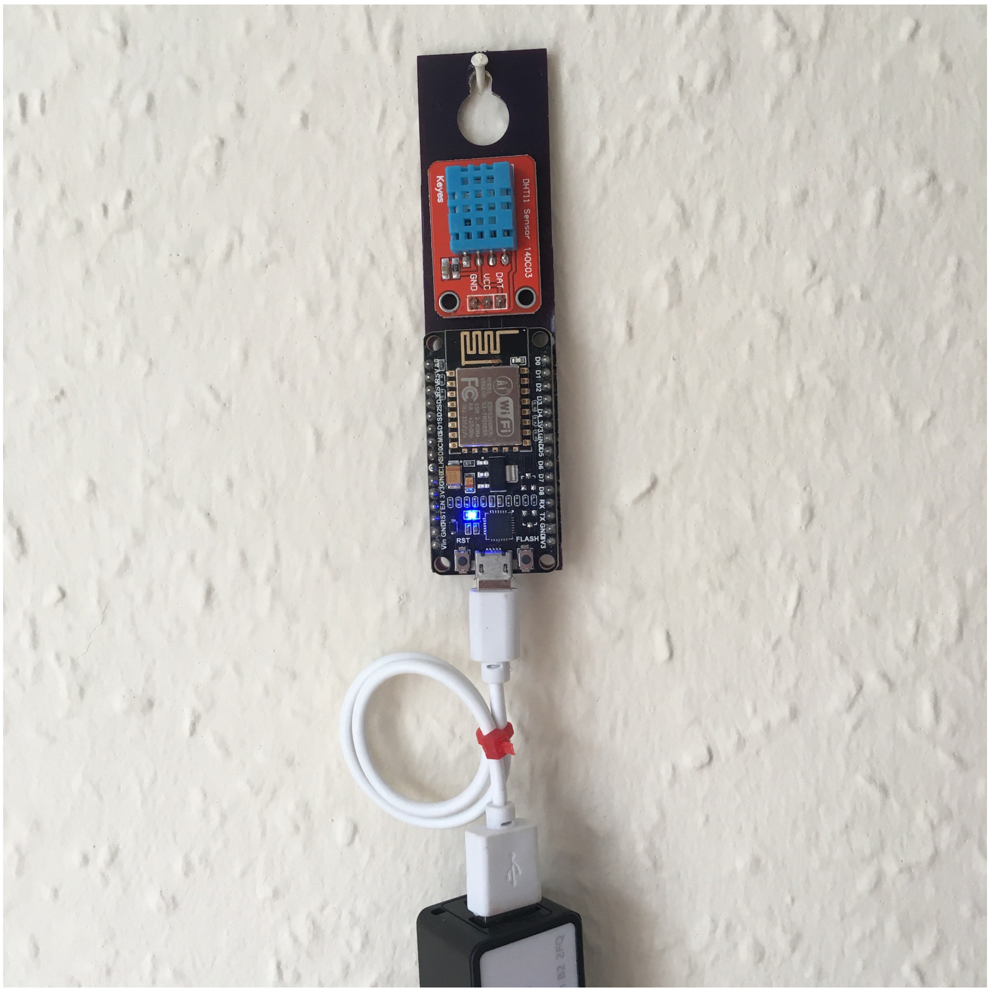


Figure 28. Humidity sensor (PCB version). © David Chatting.

In order to start an exploration of new connected electronic Stuff situated beyond the router in the context of the home, I built a simple humidity sensor – see Figure 28. The choice of humidity sensing was motivated by the discussion given in Chapter Two of the Internet of Things in rented homes. Sensing is seen by property management groups as a way to flag situations that are potentially harmful to dwellers or damaging to a landlord's property; not least the effects of humidity and dampness. I also saw potential here for integrations with the heating system.

The simple device I built is based on the low-cost DHT11 sensor and NodeMCU ESP8266 Arduino compatible WiFi microcontroller. The software I wrote reports the temperature and humidity once a minute over the network (Figure 28). The component cost was less than £10, but the bespoke PCB I design was relatively expensive. So that the sensor might be fixed in place anywhere in the home, the PCB integrates a hole to co-opt a nail and can be powered by USB from a socket or a dangling battery pack – to allow use far from a mains electricity socket.

Message Queuing - MQTT

To allow the simple sharing of messages between devices such as the humidity sensor, I installed the popular mosquitto package (Eclipse, 2009) MQTT (Message Queuing Telemetry Transport) broker on the Router of All Evil (on the Raspberry Pi). MQTT is a lightweight protocol designed for IoT devices to publish small amounts of arbitrary data on a specified topic to a broker, in this case on humidity, other clients may then subscribe to this topic via the broker and will be pushed relevant messages as they occur (Stanford-Clark, 1999). Software architects know this as a pub/sub or publish and subscribe or observer design pattern (Gamma et al., 1994). MQTT is widely supported by software libraries, including those for JavaScript and Arduino, which further simplifies implementation. For Hack My House, this enables a lightweight way to make chains of loosely connected components and Rube Goldberg like machines – our doorbell machine had previously depended on relatively inflexible articulations.

The humidity sensor publishes an MQTT message containing a value for the current temperature (in degrees centigrade) and for humidity (as a percentage), every minute – in addition to a unique identifier for the sensor, its MAC address. The message is formatted as JSON (JavaScript Object Notation), a notation of data/value pairs arranged hierarchically, but expressed as a single text string. As previously discussed, JavaScript and its associated technologies, including JSON were chosen as the common language for these endeavours – the Ikea Trådfri light API works in the same way (see Figure 22).

Energy Monitoring

To explore my home's use of mains electricity I installed the DIY Kyoto Wattson Energy Meter (Figure 29). The meter has two components: the electromagnetic induction clamp (left) which needs to be positioned on the main cable coming into the fuse box and the digital display (right) which is designed to be in the living space. The clamp communicates with the display via a radio signal at a frequency of 433 MHz, reporting a reading in Watts every five seconds.

First marketed in 2006 the Wattson has no connectivity beyond the display, but it was possible to access the current reading over the display's USB serial connection. In 2010, Främling and Nyman published their Openwattson code to demonstrate its simple serial protocol (Främling and Nyman, 2010), today this code is maintained on GitHub[58]. In a contribution to the project made in 2011, Mikko Pikarinen described the

[58] https://github.com/sapg/openwattson

Wattson's serial protocol, the set of possible commands and the format of the results[59]. Working from this document I was able to attach a Raspberry Pi with a WiFi dongle to the Wattson display and publish results to the network using MQTT (Figure 29, right). In this way, these two domains of the networked home are bridged

The Wattson MQTT message contains two values, the current power consumption in Watts and the change (delta) this represents since the previous reading five seconds before; and again, the MAC address of the device as a unique identifier. It was intended that the delta reading would capture instances of individual electrical devices being turned on or off.

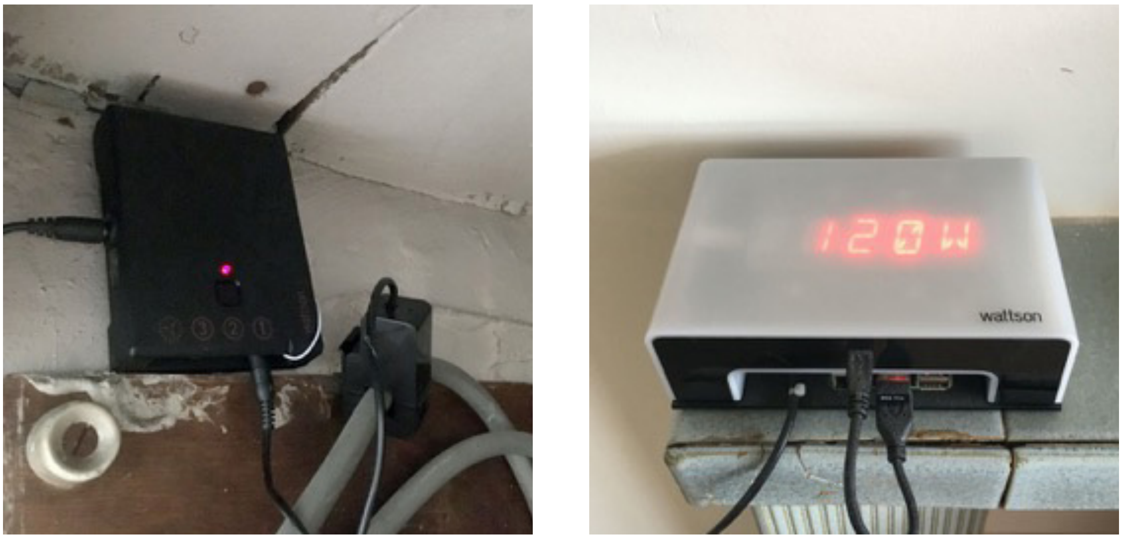


Figure 29. Wattson energy monitor. © David Chatting.

Hack My House #2

Several months after the first workshop on a Wednesday afternoon we reconvened at mine for the second Hack My House this time with five participants (Dan, Andy, Cally, Kyle and Diego). I had some new offers for the group: the Router of All Evil (version 3) and the MQTT feeds for humidity and electricity consumption. I had also extended the router so that it published any DNS request made on the network in real-time to an MQTT topic – as described in the Kindle wallpaper hack, a DNS request will start any device's interaction with a remote server and so this became a powerful mechanism to watch any device's real-time behaviour. The MQTT messages produced contained the queried hostname (e.g. google.com) and the device making that query (identified by IP and MAC addresses).

[59] https://github.com/sapg/openwattson/blob/master/protocol.txt

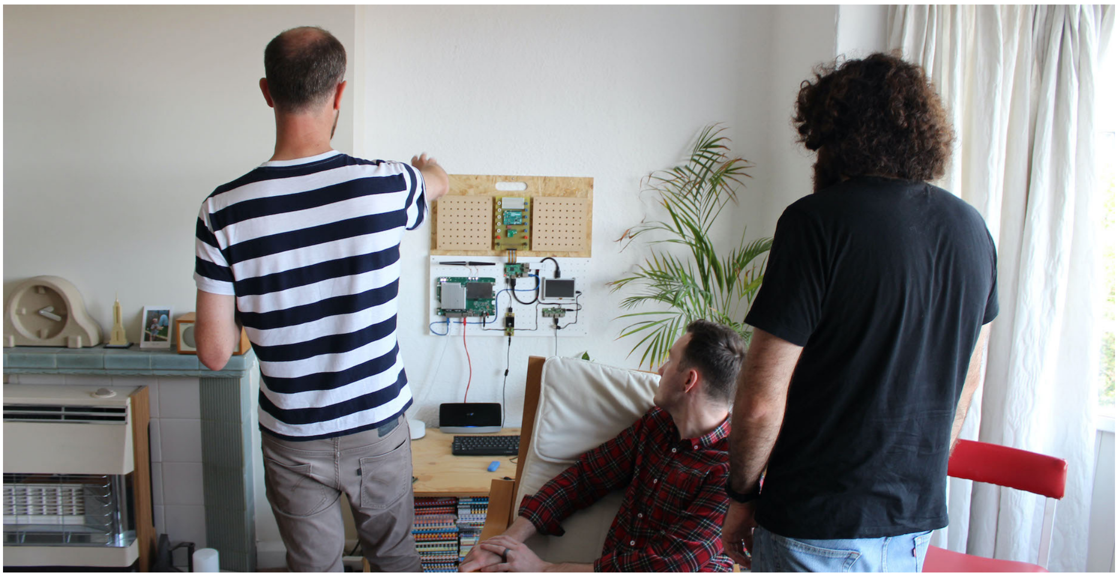


Figure 30. Hack My House #2. © David Chatting.

My offer for this workshop was to explore some new ways of building the Goldberg-like chains of action that had previously been successful. I considered that MQTT would be a way to make this more straightforward, that elements might react to some subscribed topics and publish results to others, forming a chain reaction. To encourage this, I prepared code examples for JavaScript, Processing and Arduino to create and manipulate MQTT messages. Since building the humidity sensor, I had found an even less expensive WiFi module, the WEMOS D1 mini (£3 each); this was also an ESP8266 based device with Arduino IDE compatibility. I ordered a set of these for the workshop and provided some rudimentary electronic components.

In just a few hours, we created two interesting demonstrations. Firstly, an electrical consumption game attempted to identify appliances as they were turned on by watching the change in the power consumption from the Wattson's MQTT messages; as the cooker and the toaster have different demands, for instance. The game dynamic was less resolved but might motivate raising or lowering the house's overall power. Over the weeks that followed, this hack inspired the Power Trigger Breadstick (see page 168). The second demonstration was a service that would read aloud on the Chromecast (audio) any text that had been sent to an MQTT topic – this used the Google cloud text-to-speech service. This had an appealing and playful flexibility, but perhaps more interestingly the use of cloud services sparked a debate about what services the home need and need not provide for itself.

In conversation afterwards, we reflected that these demonstrations were suggestive of a local distributed architecture for managing rules of action and reaction – in contrast to the centralised cloud model of services like If This Then That (IFTTT).

Instead, we showed that MQTT messages could be read by processes on any device on the network, which could then send on an interpretation of these messages via MQTT or cause some other action – a chain reaction. The electrical consumption game showed that these events could also bridge the domains of the networked home – offline electrical devices could have consequences on the network.

Yet again there seemed to be more to do and we talked enthusiastically about attempting something over a longer period. I started to think about how I could encourage deeper interactions with the fabric of the house and how these interventions might be made in ways that I could live with them for a while, rather than the fleeting experience of the demo.

Breadsticks

Following the hackday, I wanted to explore a deeper interaction with the fabric of the house, installing inventions in situ, perhaps for days or weeks at a time. The humidity sensor had had some of this intention and while the PCB design allowed the device to be placed around the home, it was relatively expensive and created a fixity that hampered further explorations with the electronics. Through my own hacking and at the hackdays there had been some unwillingness to create hacks in the sense of a quick physical fix – generally, the hacks had been in software and run on a laptop, with the notable exception of the doorbell machine. If subsequent hacks were to introduce some new semi-permanent devices into the home, as the chain reaction proposal seemed to demand, then there would need some way of rapidly prototyping in hardware. To address this, over the subsequent months, I developed a series of prototyping boards that became known as breadsticks (Figure 31).

The breadstick is an evolving design for a low cost, rapidly produced and easily configured prototyping board; designed to endure short deployments in the home. The stick is laser cut from birch plywood (with a thickness of 2mm) and offers a variety of holes and attachments that anticipate a range of uses and fixings in the environments. Some elements can be broken free by snapping them out – reminiscent of an Airfix model and the Interaction Research Studio's ProbeTools camera circuit board (Boucher *et al.*, 2019). The material can easily be further configured with a drill or sharp knife. Figure 32 shows a later iteration of the design. In order that it might temporarily occupy space, the breadstick design allows it to be hung from a nail (in the same way as the original humidity sensor) and to be attached around a mains electricity adapter (as later described in Figure 35) from which to resource power. In Research Product terms these are manipulations of finish and independence (Odom et al., 2016), as I described in Chapter Four.

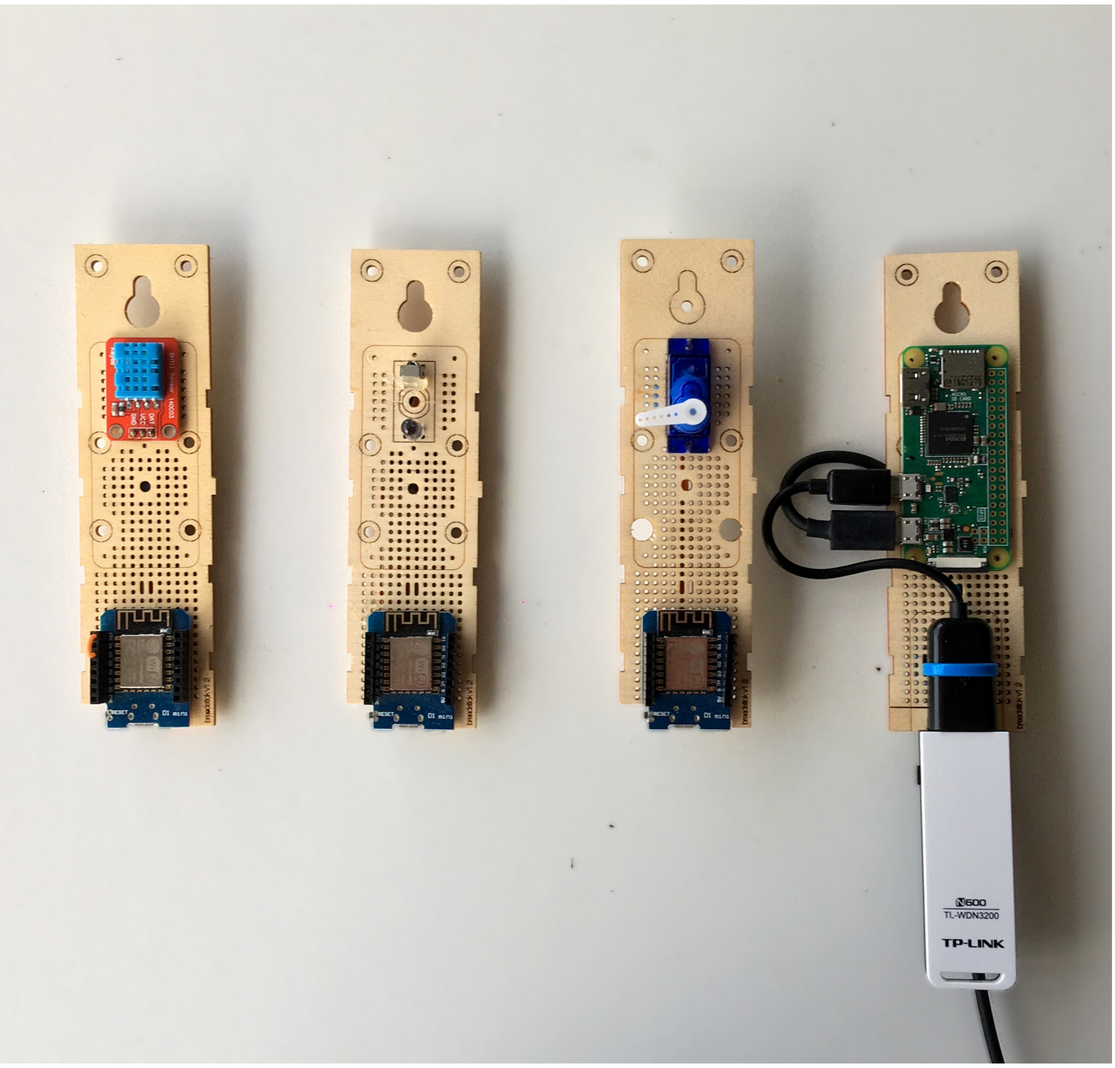


Figure 31. Four breadsticks. © David Chatting.

Figure 31 illustrates four early prototypes built around the breadstick design. Left to right: a second design of the humidity sensor; an infrared remote transceiver; a servo motor; and a Raspberry Pi Zero. The humidity sensor, now based around the cheaper WEMOS D1 mini, operates as before.

The Infrared Transceiver Breadstick can both send and receive the remote-control protocols from a large set of manufacturers[60]. When it decodes a command, it forwards it to the MQTT ir topic. It can also be addressed by another device on the network, via MQTT, to produce a specific command. In this way, it forms another bridge of the technologies that constitute the networked home – pressing a button on a remote control can now have enumerable actions on the network and vice versa.

[60] Including JVC, NEC, Philips, Samsung and Sony.

The Servo Motor Breadstick demonstrates a mechanical actuation in the home, it was not built to interact in any specific way, but rather to suggest a possibility. In its original configuration the servo motors position was determined by the orientation of the Ikea Trådfri lightbulb dimmer control; reading its value from an MQTT topic. In later versions of the breadstick design additional fixing hole for Lego and Meccano were included to support mechanical extensions to actuate some element of the home – see Figure 32.

The Raspberry Pi Zero Breadstick can support any application of the popular Linux based computer.USB dongles can be used to extend this breadstick's capabilities and it is shown with a second WiFi card in Figure 31, used for the location experiments described later.

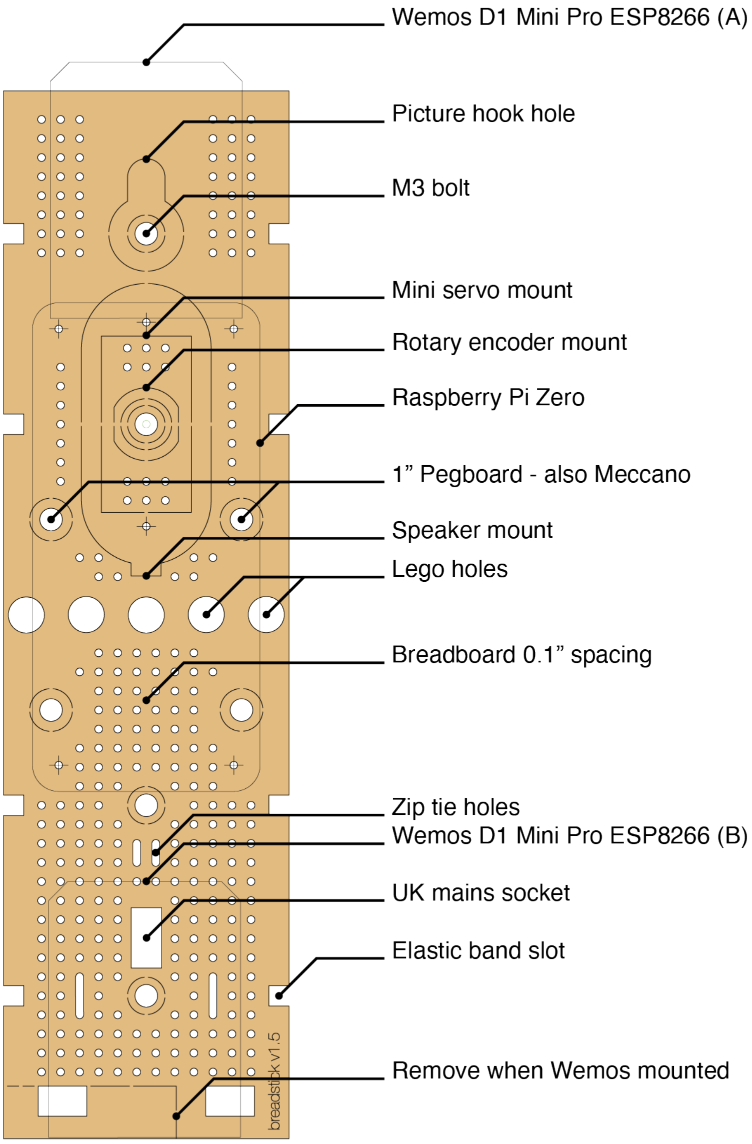


Figure 32. Breadstick design (v1.5). © David Chatting.

The breadstick is named in reference to the *breadboard*, a common electronic circuit prototyping tool where the legs of components are pressed through holes onto a sprung clip that makes an electrical connection, without the need for soldering. The board contains rows and columns of these holes, which typically have a pitch of 0.1 inches (2.54 mm), able to accept the common dual in-line packages of Integrated Circuits (ICs). The breadboard then allows some semi-permanent circuits to be constructed for prototyping; originally breadboards were literally kitchen chopping boards on which circuits were assembled with nails and wound wire.

Hack My House #3

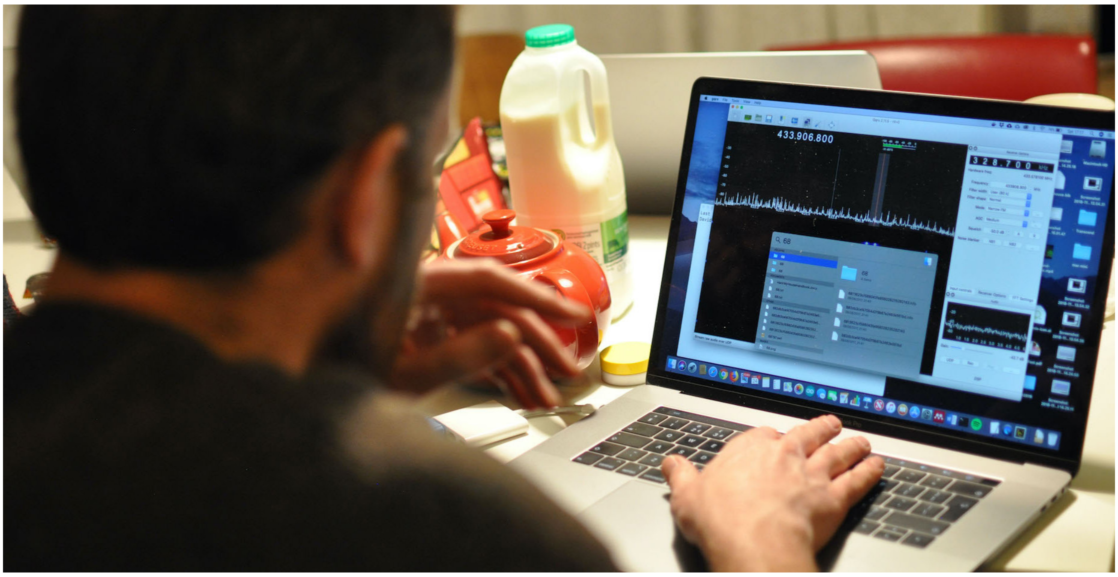


Figure 33. Hack My House #3. © David Chatting.

Two months after the second workshop we convened Hack My House #3, a two-day weekend workshop at my house with four participants (Dan, Andy, Cally and Diego). In preparation I had revised the Router of All Evil to further open it to hacking through its web API and developed the breadstick prototyping boards, previously discussed. The intention over the course of the weekend was to create some semi-permanent interventions in the space. Following my earlier attempts to map my Hertzian space, I renewed attempts to decode the doorbell and thermostat’s wireless control using the TV tuner module and SDR radio software.

Early in the weekend Diego introduced us to and installed the Node-RED software on the Router of All Evil. Node-RED (O’Leary and Conway-Jones, 2013) is a visual flow-based programming platform that runs in the browser and allows multiple sources of data to trigger events, including MQTT messages. It is based on Node.js and many packages exist for common IoT devices , for example, to control the Google Chromecast or to use the GPIO on a Raspberry Pi or an attached Arduino. By installing the package node-red-node-pi-gpio electronics could be developed on the router to provide novel inputs or outputs. Node-RED seemed like the missing piece of the puzzle, allowing us to rapidly experiment with rules and integrate new hardware rapidly prototyped on the router.

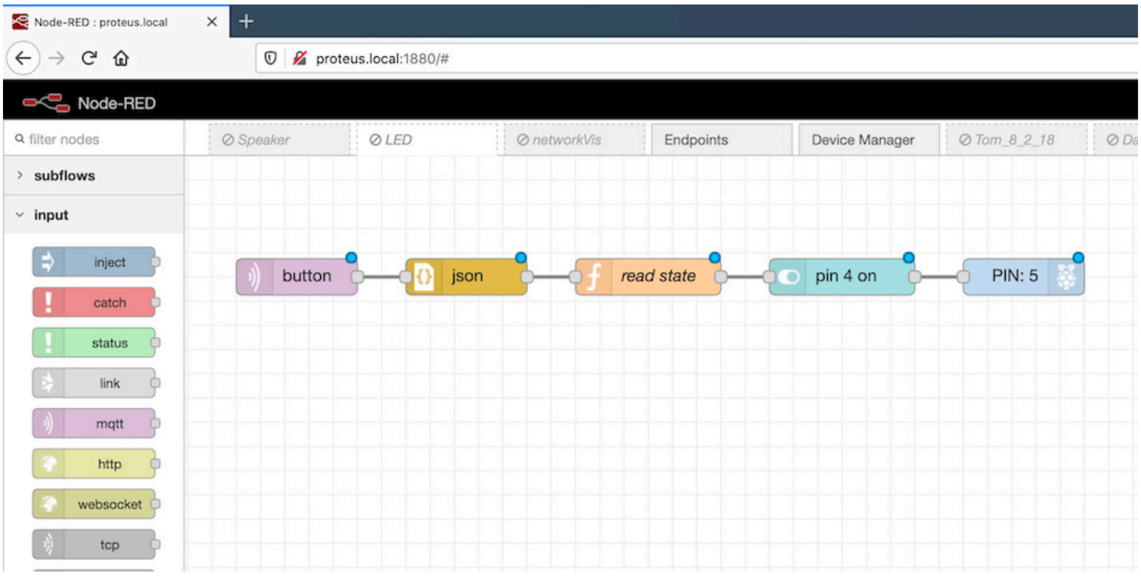


Figure 34. An MQTT flow in Node-RED. Used under license, Apache License 2.0.

The rest of our weekend was spent exploring the potential of Node-RED. Andy and Diego collaborated to make an MQTT button with a WEMOS module and a breadboard to remotely control an LED attached to the GPIO on the router (see Figure 34). We started to rewrite the Home API so that it also ran in Node-RED and wrote flows to send audio to the three Chromecast speakers around the house. Text-to-speech messages could now be read over a particular speaker. Cally also explored how the Line-us robot arm could produce data-driven drawings, realising that it accepts the common G-Code over a network interface. Yet again, by the end of the weekend we could see yet more potential than we had begun with and wanted to do it again; the longer format had been altogether more relaxed and social. In contrast to previous workshops there was more focus on creating potentials than demonstrations, despite my intervention focused design brief.

Power Trigger Breadstick

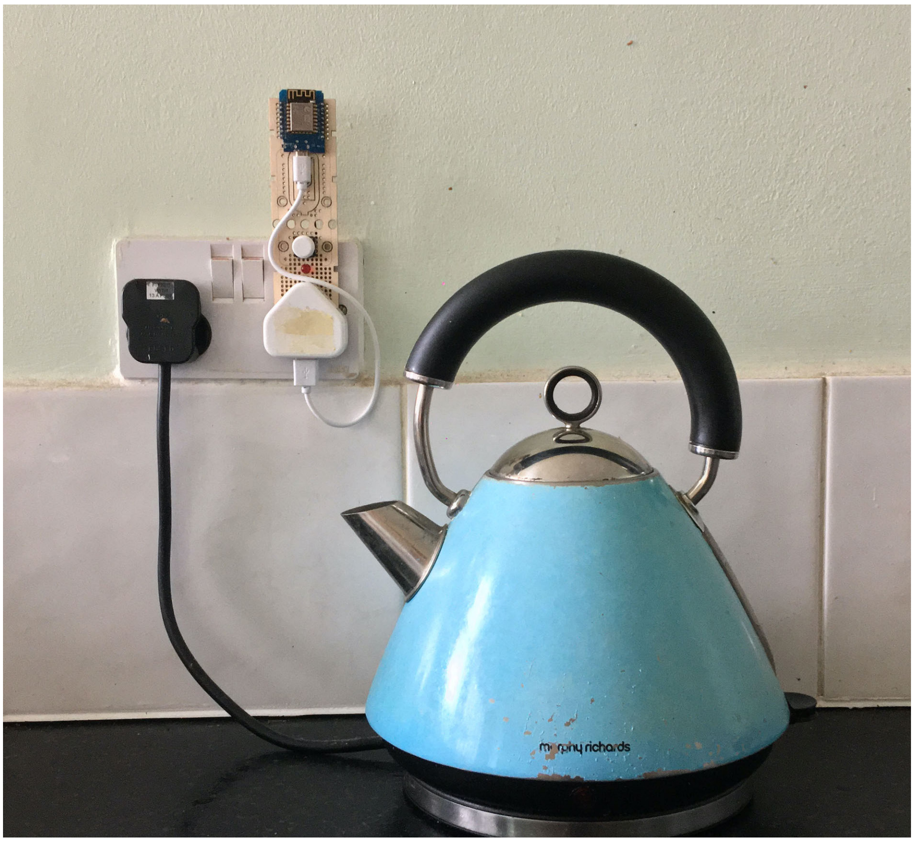


Figure 35. Power Trigger Breadstick. © David Chatting.

At the second Hack My House workshop, we had begun to explore the ways in which different electrical appliances could be identified by the change in power consumption of the home. Following a revision to the breadstick design to incorporate the three holes for a UK mains socket (see Figure 32), it could be attached to and permanently powered by a USB phone charger; this then allowed some in situ interventions.
The Power Trigger Breadstick (Figure 35) attempts to learn the power (in Watts) of any electrical appliance. First the appliance is operated, then the white button is pressed, the Arduino code then attempts to identify the change in power that was associated with that event, by looking at the home's energy consumption over the last few seconds from the MQTT messages. This value is then stored and the next time the power changes by this amount (within a tolerance) the LED lights and a new MQTT message is generated. If the power instantaneously drops by this amount the LED is turned off and another MQTT message is sent. In this way arbitrary electrical appliances can trigger network events; another example of a network bridge . In practice, this works well for appliances that draw the same high power on each operation – like kettles, toasters, electric cookers, vacuum cleaners, etc., but lower power appliances like light bulbs, radios, etc. are less easily discriminated.

Naming Breadstick

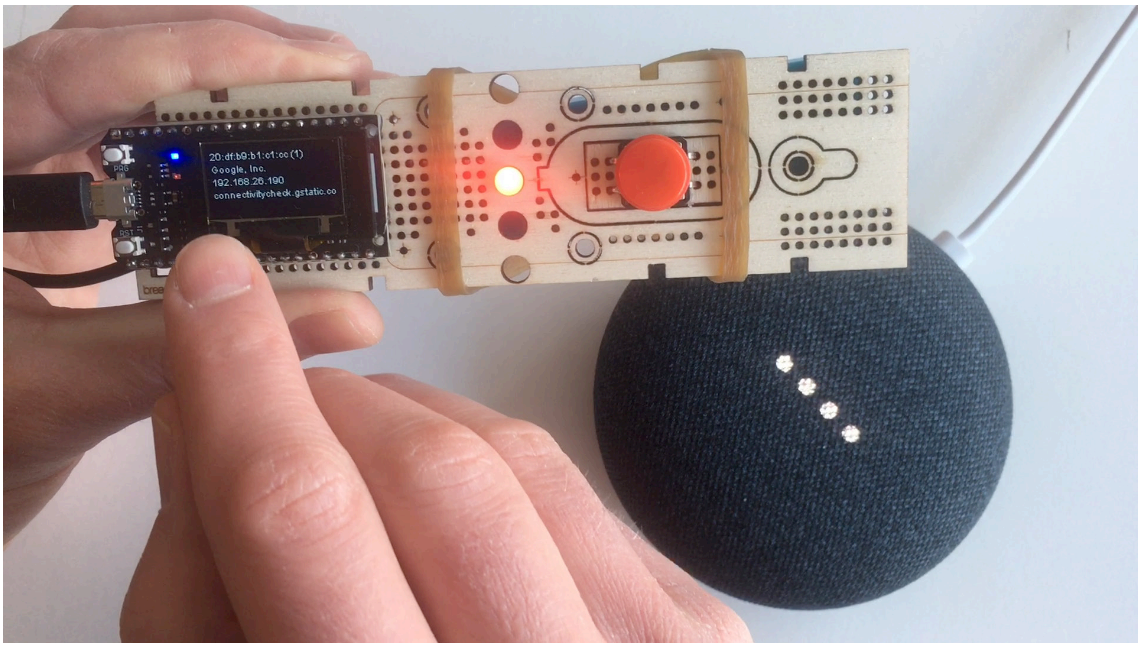


Figure 36. Naming Breadstick. © David Chatting.

Through these explorations of WiFi and the home network a common problem is how one finds the identity of a device on the network; knowing this might then allow rules to be attached to its operation or its capabilities to be inspected. Typically, this might involve command-line network tools like nmap, as previously described in reference to the Home Network Map (page 143). Yet I was wanting to find a more direct physical, tangible way to interact with my network. The Naming Breadstick reveals the identity of a WiFi device by physically bringing it in proximity. This displays the MAC address, manufacturer and IP address of the device; then as it accesses servers the names of these are displayed in real-time and the LED flashes . The Naming Breadstick will remain paired with this device until by the same operation it is paired with another. Pressing the red button will remove the paired device from the network, by subjecting it to a deauth (deauthentication) attack – the hack used by the *dropkick.sh* Airbnb camera script (Oliver, 2015).

Technically there are several elements to the Naming Breadstick's operation. Pairing is achieved through packet sniffing, as discussed in the Home Network Map. These packets can be filtered by their signal strength (RSSI - Received Signal Strength Indicator), such that only ones from proximate devices remain. While the contents of these packets can generally not be decoded, the MAC address of the device is inspectable. Supplied with the MAC address, the Home API will return the manufacturer and IP address of the device. Further, all DNS requests made by this device for Internet servers are also available from the MQTT feed in real-time. The ability to deauth a device from the network, by supplying its MAC address, is provided by the Home API controlling a WEMOS D1 mini mounted on the Router of All Evil's pegboard as a panel and attached by USB. More nuanced contextual interactions would also be possible; perhaps to increase the volume for a speaker or to turn on a light bulb. It might then become a universal control able to interact appropriately over a range of devices.

This breadstick employs a powerful ESP32 WiFi module with an integrated OLED screen, on which a wide range of interactions can be explored. The ESP32 is also programmed through the Arduino IDE and shares a codebase with the other ESP8266 breadsticks. The design of this breadstick significantly informed the later design of the Approximate Library (see page 185) and the Device Wheel meter for the Home Network Study (Chapter Six), which uses the same mechanism and code to pair with a target device and examine its network traffic.

Spatial Reasoning

This period of time represented a high degree of productivity in my own private hacking; after three hackdays there was an abundance of technical possibilities that could be relatively easily configured and combined. Through my examinations of the struggles of the home in Chapter Two, a recurring theme is that of spaces and the ways in which these are socially differentiated, whether by being public or private, gendered or otherwise. The technology of WiFi has no such concerns and IoT manufacturers typically consider the home as a uniform and homogenous space. I began to wonder if I could recast the domestic Internet with a spatial understanding of the home using the technologies I had assembled. Could some of the vision of Weiser's Ubiquitous Computing be realised without requiring a surveillant infrastructure? It might be possible to ascribe a position to a device either absolutely in the home, or relatively by range to some other device – without disclosing that position to the system, much like a GPS module's on-device calculation of longitude and latitude. With spatial reasoning a device may change its function in the office or living room or one could address all the devices in the kitchen or locate a particular device in the home.

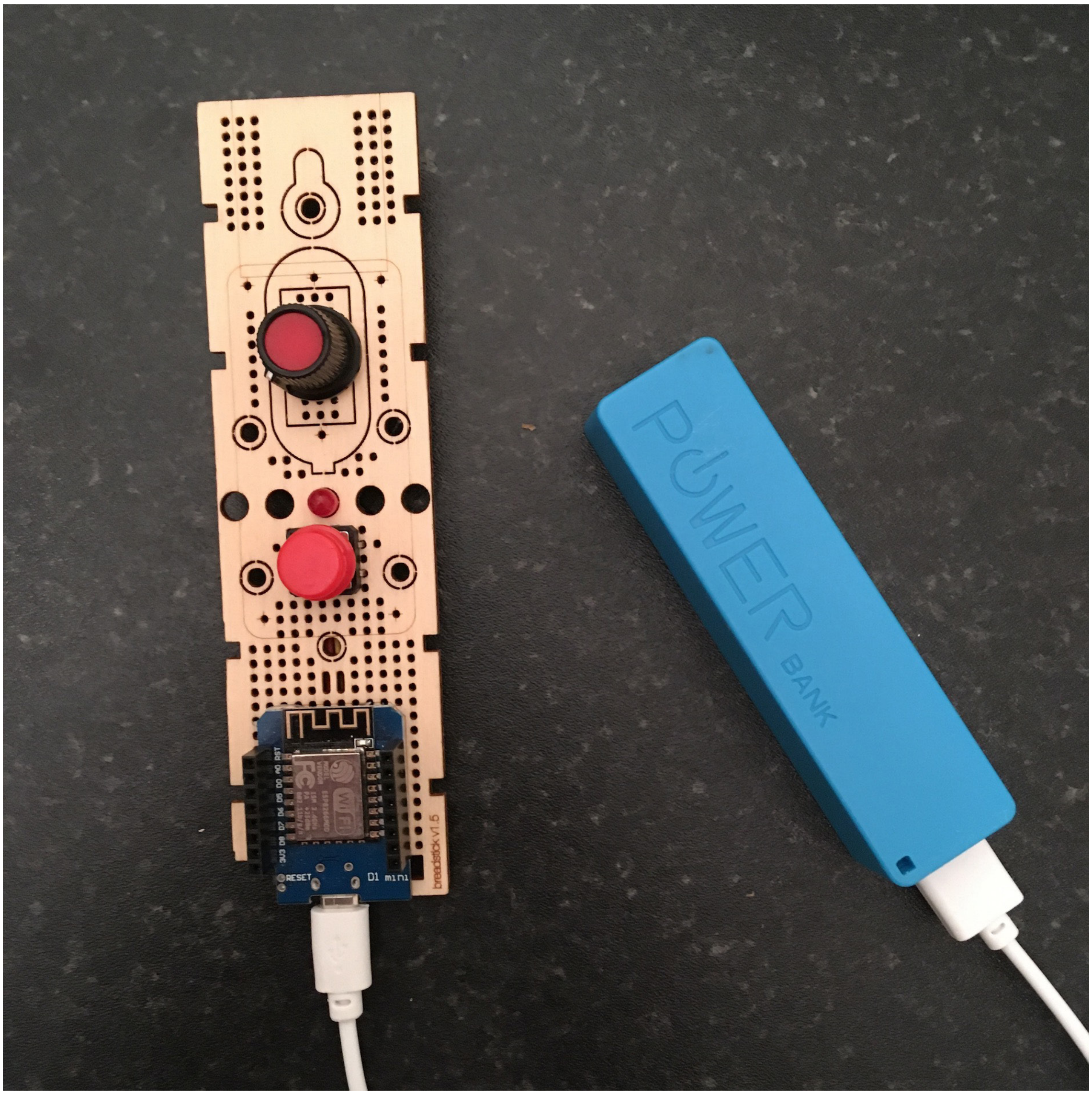


Figure 37. Spatial Volume Breadstick. © David Chatting.

In a series of exploratory hacks, I attempted to add some spatial reasoning to the network. In the first, an ad hoc placement of Raspberry Pi beacons packet sniffed the signal strength (RSSI values) of devices in the vicinity, which in combination might allow some location by triangulation. This worked very badly, the RSSI values were noisy and difficult to interpret. In the second, an ESP8266 breadstick (Figure 37) packet sniffs, but only for neighbouring routers – which are assumed to be static and in an apartment building, plentiful. By pressing the red button, a survey is made of this location, noting the routers visible and their signal strengths – the LED lights to mark this place. When the breadstick is moved to a different location this fingerprint of signal strengths changes and the LED turns off, when it is moved back the LED is lit again. Using the volume knob, the accuracy of the match is increased or decreased and so the volume of space within which the LED will lit is increased or decreased. This worked rather better but was still somewhat unpredictable in different locations – nonetheless I was generally able to recognise when the breadstick was on (or near) my dining table and when it was not.

The most promising avenue for developing precise spatial reasoning for the home network is the most technically involved. As it turns out the RSSI value is itself a derivation of a more complex measure of signal power known as called CSI (Channel State Information). CSI measures the signal over multiple frequency bands with the intention of shaping the transmission to avoid local perturbations. These perturbations will be walls, furniture and people. The CSI information can be interpreted to reconstruct some of these features, through a technique known as WiFi Sensing (Ma, Zhou and Wang, 2019). It is claimed that WiFi Sensing can be applied to a set of activity recognition problems, often where the data feeds a machine learning component. Furthermore, it seems that these same techniques might also be applied to location recognition for a moving device. The Nexmon opensource project makes these tools available for exploration with a Raspberry Pi (Schulz, Wegemer and Hollick, 2017; Gringoli *et al.*, 2019). The fingerprints created by measuring the router's CSI from a device are multidimensional and defy simple strategies for rule making. However, my experiments suggested that location might be plausibly determined from the fingerprint by an on-device computation that applies a machine learnt classification using tinyML[61] or similar.

While I wasn't able build a reliable spatial reasoning system, these first-hand experiences gave me an intuition on what would and crucially would not be possible with measures of RSSI and CSI. Specifically, the noisy characteristic of RSSI significantly informed the later design of the Approximate Library (see page 185), which in later versions also supported the measurement of CSI.

Hack My House #4

Three months after the third workshop we convened for *Hack My House #4 - Haunt My House*, a one-day workshop on a Friday at my house with five participants (Dan, Andy, Cally, Kyle and Tom). My framing was a little more explicit on this occasion, encouraging longer-term interventions, to "*build something for me to live with for the following week - something to surprise me, that will perhaps haunt the space!*". I suggested that the weekend afterwards could be used as an open house, if there was more to do. After three workshops the group had some established expectations of the day and the notion of haunting my network served both to refresh the format a little and speak directly to issues of one's agency at home; this was met with enthusiasm.

[61] TinyML is a popular software library for implementing machine learning on low-cost microprocessors.

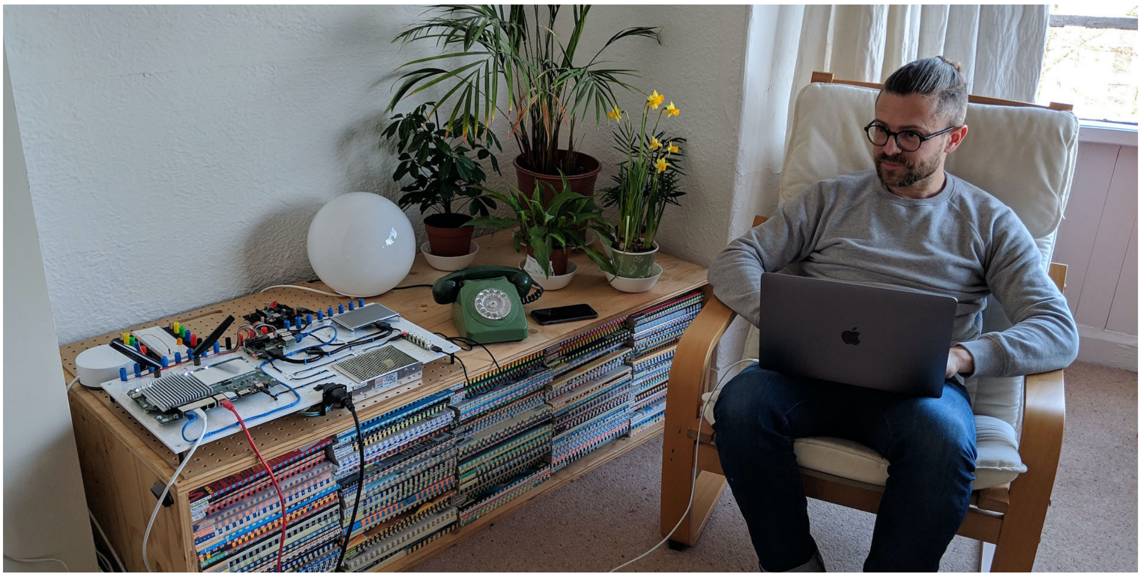


Figure 38. Hack My House #4. © David Chatting.

This workshop was the public debut of the final version of the Router of All Evil, with the new pegboard and Arduino and breadboard panels. The Home API had been considerably revised and I introduced three ways it could be used: as a trigger when something new joins the network, to *deauth* (throw off) any device from the network for a period of time, and to track any device around the house with respect to the Raspberry Pi beacons previously described. I was imagining that my phone joining the network, as I came home, might trigger some creepy sound effects in the home. I was curious whether over the period of a week I might be caught out by these events, even if I knew they were installed. Cally responded to the mystical dimension of the brief by building a crystal radio kit to interact with the home's Hertzian space. Kyle started to prototype a ghostly experience on the Kindle that would trigger events in the home. Tom created a visualisation of the location data – which proved rather definitely that the beacons approach did not work very well!

While the offer of an open house for the weekend was made, nobody was able to participate. However, Tom asked whether I would open up the network so that he could access it remotely and hack from afar. This caused me to hesitate, both in reaction to my exposure outside the situation of the hackday and a concern that the resulting hacks might become too abstracted. However, I reasoned that for a limited period, with Tom continuing what he had started in situ this would be interesting to try – and consistent with experimenting with my agency at home. I used the *ngrok* service to expose the Router of All Evil to the Internet, secured with a password. While this was again met with enthusiasm, without the structure of the workshop, nobody made immediate use of it. In the end, despite our best intentions, nothing got haunted that hackday.

Pegboard Panels

With the inclusion of the pegboard in the final version of the Router of All Evil, panels mounting an Arduino and breadboard on acrylic were produced, held in place with wooden pegs. Shortly afterwards a panel for the WEMOS D1 mini was similarly included. These first panels were primarily about making these components available and offering them a stable position allowing electronic prototypes to be rapidly explored. Subsequentially an LED panel for indication and a MOSFET panel for operating high power outputs were introduced, these were designed to directly interface with the Raspberry Pi's exposed GPIO binding posts – such that a patch wire could easily make a connection. Internally the binding posts on the panel are wired through to an LED via a series resistor such that they can be driven directly by the logic levels from the Raspberry Pi. In combination with Node-RED these panels allow complex events to trigger simple outputs – for instance, an LED that lights every time the network makes a request of Google. The LED panel allows an ad hoc annotation of these relationships using a simple handwritten label – reminiscent of the practice of writing a Scribble Strip on a mixing desk console, where a piece of tape is stuck by a control to temporarily associate it with a particular track or effect. This has a similar intention to the marker-based annotation on the surface of the Home Network Map (Chatting, 2017).

The MOSFET panel can control five high power outputs from the Raspberry Pi's GPIO, each switching up to 60 volts. The panel mounts a commercially available MOSFET board whose inputs and outputs are again wired to binding posts for easy connection. Panels of switches, buttons and a mechanical stepper motor were planned but not realised.

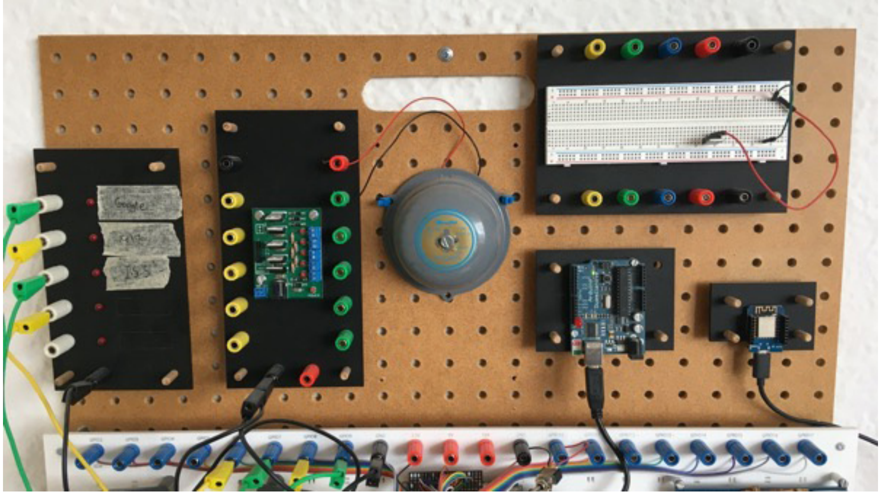


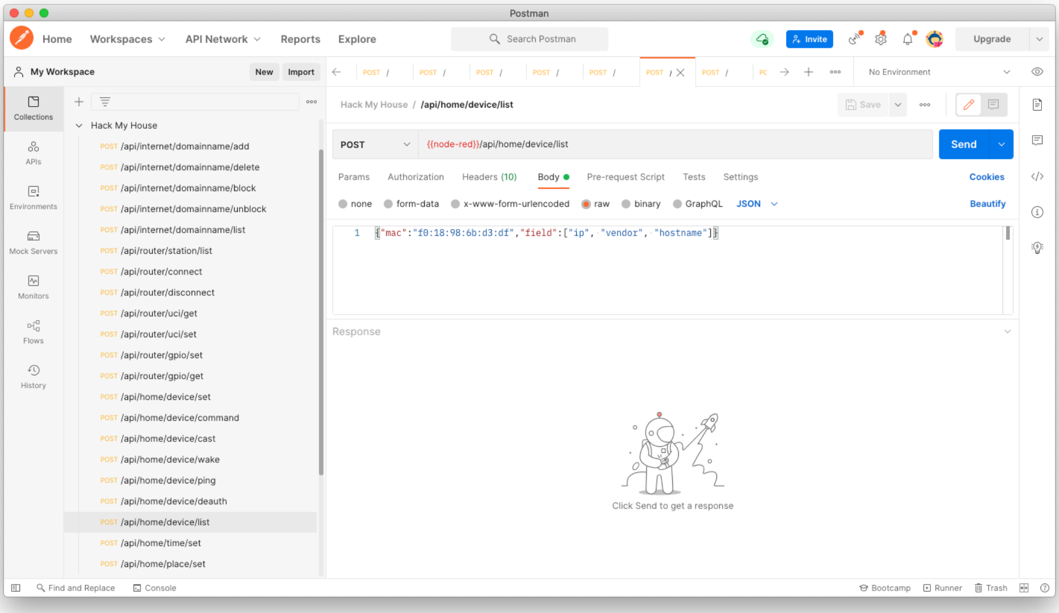
Figure 39. Router of All Evil - pegboard panels. © David Chatting.

Home API

The task of designing a Home API began in preparation for the first workshop, to bring the first found hacks together in a common location. It evolved over the period of the workshops to accommodate the new technical possibilities being disclosed through hacking, as I attempted to impose an order on these disparate technologies. This process was suggestive of logical, but absent, new functions to develop and include. Likewise, through this process common syntaxes and linguistic expectations emerged, as more functions were incorporated. The resulting Home API interface is itself a designerly form that attempts to create a temporary settlement of the found and developed hacks, offering new desirable technical affordances, whilst obfuscating less desirable ones. As Chapter Three discussed at length, the API is a black boxing exercise in which complexity (and work) is rendered invisible.

The Home API, as it was finally settled, supports both web request-response (HTTP) and publish-subscribe (MQTT) methods by which clients can straightforwardly acquire data from the router and the network; these methods are often used (as with the Naming Breadstick) in combination. For HTTP the API is defined by a set of endpoints; for MQTT by a set of topics. The HTTP API was designed with a further commitment to the popular architectural pattern known as REST (Representational State Transfer) or RESTful, which requires each request to specify in absolute terms the parameters of its operation on each occasion – such that the server need not surveil the activity or state of individual clients, as no operational context is required (Fielding, 2000). The MQTT broker allows clients to define their own topics on which to publish and subscribe, allowing ad hoc events and sensor readings to be readily shared between clients. In these ways the server architecture, while defining a central API, also promotes autonomy in its clients.

Both the HTTP server and MQTT publishers were ultimately implemented in the popular Node-RED visual coding environment, built on Node.js and JavaScript. This came about at Hack My House #3 through Diego's intervention and was an important turning point as Node-RED then provided an environment for everyone (not least me) to easily make their own experiments and contribute to the API in one common public place. From Hack My House #1 Andy showed us the Postman tool for documenting and testing APIs; I added each new Home API endpoint to the Postman collection with a simple demonstration of its use, see Figure 40. For each workshop I then updated both the House Handbook with details of Home API and shared the latest Postman collection. This process of public documentation necessitated a period of reflection and invariably led to edits of the API.



Hack My House

- POST /api/internet/domainname/add
- POST /api/internet/domainname/delete
- POST /api/internet/domainname/block
- POST /api/internet/domainname/unblock
- POST /api/internet/domainname/list
- POST /api/router/station/list
- POST /api/router/connect
- POST /api/router/disconnect
- POST /api/router/uci/get
- POST /api/router/uci/set
- POST /api/router/gpio/set
- POST /api/router/gpio/get
- POST /api/home/device/set
- POST /api/home/device/command
- POST /api/home/device/cast
- POST /api/home/device/wake
- POST /api/home/device/ping
- POST /api/home/device/deauth
- POST /api/home/device/list
- POST /api/home/time/set
- POST /api/home/place/set

Hack My House / /api/home/device/list

POST {{node-red}}/api/home/device/list

○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL JSON

```
{"mac":"f0:18:98:6b:d3:df","field":["ip", "vendor", "hostname"]}
```

Figure 40. Final Postman endpoint collection. © Postman Inc, 2022. Author asserts fair use.

The opportunity to bring order to the Home API is primarily defined by the structure and pattern of endpoint URLs. The design of these endpoints creates a simple and consistent taxonomic structure that arranges the existing functions and suggests those that are missing. The endpoints are hierarchical forward-slash separated phrases, with the form: */api/domain/noun/verb*. The */api* prefix simply partitions every endpoint from other resources the server may manage. The domain is then either: *internet*, *router* or *network*; the noun then refers to something in that domain and the verb describes the specific operation. An example endpoint is */api/home/device/deauth*, which removes a device from the network – as previously described. Each endpoint in the Home API uses the HTTP POST method and requires that a JSON request is sent refining the operation and a JSON response is received for each transaction with details of the outcome[62]. The MQTT topics follow the same naming structure, but without a verb and carried a JSON message payload. An example topic is */api/home/power*, reporting the real-time electricity consumption of the home. As far as possible the format of all JSON messages is consistent across the API.

[62] HTTP defines a set of request methods (POST, GET, PUT, PATCH, and DELETE) such that when an endpoint is addressed by different methods this verb is used to alter its behaviour accordingly – for instance, POST to write a value and GET to read a value. However, I prefer the more explicit style of endpoint naming that includes a specific verb and simply uses the POST method for all operations.

In my hacks, for instance the Naming Breadstick, perhaps the most useful endpoint was */api/device/list*. This returns a list of all the devices known on the network, details about their MAC address, IP address (both IPv4 and IPv6), hostname, vendor, any open ports it presents, any state information and the last time it was seen on the network. The Node-RED flow responsible for maintaining this list consumes information from a number of sources but its foundation is an nmap scan (previously discussed). This endpoint can also be used to perform queries matching partial information; Figure 40 illustrates a request for the IP address, vendor and hostname of a device specified by its MAC address.

Hack My House #5

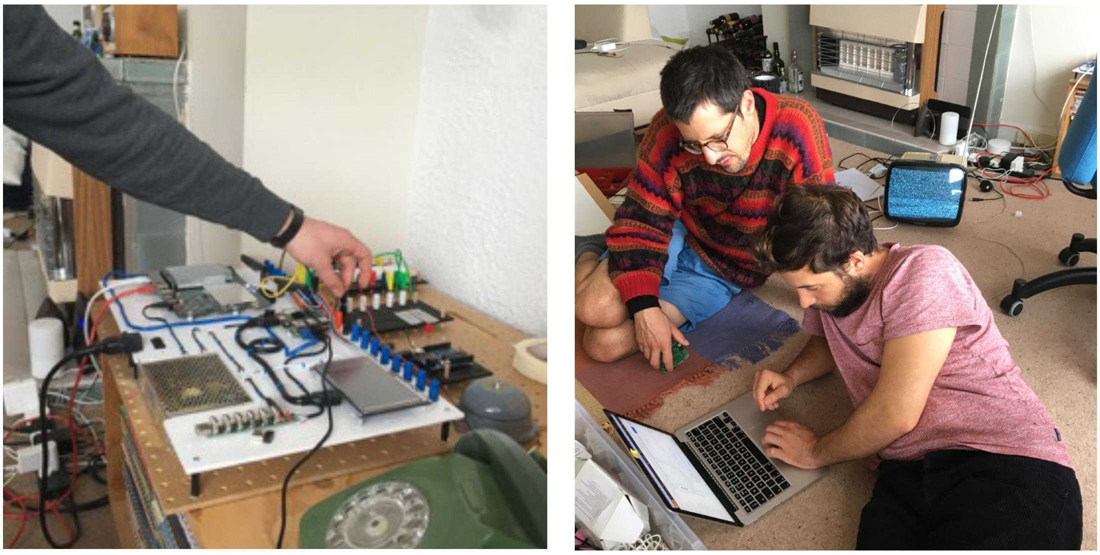


Figure 41. Hack My House #5. © David Chatting.

Four months after the fourth workshop it was the final *Hack My House #5*, a one-day workshop on a Friday at my house with six participants (Mike, Tim Shaw, Tim Sargent, Andy, Cally, and Diego). Diego was able to participate remotely from Mexico using the remote access I had previously configured via ngrok. With the new pegboard panels and the refinement of the Home API I wanted to offer some conclusion to the workshops, I wondered if we might work together to build something bigger and likely electronic. Mike and Tim Sargent were to be staying for the whole weekend and were both experienced at building large-scale installations.

Mike and Tim Sargent started to prototype in Node-RED a system that would disconnect the router when my apartment was notionally shadowed by the ISS (International Space Station). For any given location the NASA website provides the time the ISS will next flyover in the XML format – the Node-RED flow downloads this data, calculates the interval, and then waits before triggering the disconnection. They considered this would happen infrequently and unpredictably enough, typically once or twice a week, to cause me a moment of reflection on each occasion. Their first conception of this powered off the router with a Sonoff Wireless WiFi Switch, but without the network it would then be impossible to automatically power it back on. So instead, they used the Home API to acquire a list of all devices on the network and started to extend the deauth endpoint to allow multiple targets. Prior to this the flow would turn on the television and display an image of the ISS on screen, by way of some explanation. This was interesting to me because it would create an almost celestial rhythm for the network in my home, much as perhaps Shabbat does in Jewish homes (see Chapter Two). By the end of the weekend it was not quite working properly, but it had pushed the Home API on and given us cause for thought.

Tim Shaw has a sound-based artist practice and was drawn to the old Brionvega television. In the static on the screen, in the absence of an analogue broadcast, he could see the interference produced in and around the home by electrical devices. An electromechanical bell wired to the router via a relay was clearly visible and we discussed ways we could sonify or visualise aspects of the home's Hertzian space – we talked about microwaves and sparks. The bell was later attached to the router via the new MOSFET panel and rung on each request to a Google server. Tim showed that we could use a high voltage spark generator to light a candle with the clear proposition that the router could produce fire!

Once again, we had an interesting and lively time – my friends had enthusiastically engaged with the five workshops over a period of six months and returned on multiple occasions. Each time there was a push and pull between what seemed possible and interesting, and what could be achieved within the boundaries that the format had established. I had feared that without a clear objective, people would think this to be a waste of their time and that it would be difficult for me to report intangible outcomes. And yet on each occasion there was some resistance to a formalised brief and the occurrence of a workshop structured a fleury of private productive hacking in-between. The workshop products were ultimately somewhat fragile and incomplete, with none being installed for long periods of time. Our hacking was more of a continuous expedition, rather than series of investigations punctuated with demonstrations of what we had found. Some semi-permanent installations built by my friends would likely have yielded some interesting insights, but this was just beyond what the circumstances of this workshop format allowed and demanded. Their fast hacks allowed a lot of ground to be covered and it was then my role to slowly consolidate what had been found between the workshops.

Our hackdays had become very different to the Silicon Valley inspired hackathons, described in Chapter Four. Importantly, we had proceeded with a respect for each other's time and comfort. Personally, I had found the emotional support and scaffold

I needed for my isolated autobiographical hacking. Over the period of the workshops this small designerly public had responded to and shaped the products of my hacks in all the many ways I have shown. Some of our hacks demanded to be put back together for a wider public audience – I shall discuss the development of the Approximate Library in the next section.

Putting Back Together in Public

The hacking of my house had proceeded first in private and then within the participatory gaze of a small invited public, my friends. Designerly hacking suggests that this process should then conclude with the production of some public designerly forms which put some of the possibility found back together it such as way as to construct the broadest possible audience, with the broadest range of skills and interests. This necessarily requires that something revealed through hacking is identified and made useful. An obvious candidate for this were the spatial reasoning hacks that seemed to offer an alternative pattern for realising some of the vision of Weiser's Ubiquitous Computing without requiring a surveillant infrastructure and which relate to Chapter Two's concerned with boundaries and the control of space. These hacks used the signal strength (RSSI) of WiFi data packets, observed by packet sniffing, as an estimate for distance to a device. This can be accomplished without any modification of the tracked device – so long as it regularly accesses the network. In adversarial terms, this packet sniffing observes a shared medium, creating an unseen parasitic relationship with a client that does not directly destabilise its normal operation – essentially a tactic of TAZ (Chapter Four).

This section briefly describes my attempts to create such a public designerly form of packet sniffing – to put this hack back together in a new black box of my making. This is accomplished through the development and publication of the Arduino Approximate library – *for building proximate interactions between your Internet of Things and the ESP8266 or ESP32*. While other hacks explored in this chapter are not subjected to this degree of resolution, their influence is to be found in the design patterns developed in Chapter Eight for a network of one's own.

The Approximate Library

The Approximate Library was developed incrementally, first as a simple reusable Arduino code library to initiate packet sniffing on the ESP8266 or ESP32 with the intention of hiding some of the complexity of this operation inside a C++ class, aptly called *PacketSniffer.cpp*. Most usefully it allowed the MAC address and RSSI values to be parsed from the raw packet data and a measure of the packet size in bytes. This used the codebase developed through my previous hacking that integrated my own understandings of WiFi packets with those I had found described by others. *PacketSniffer.cpp* uses many low-level functions defined by Espressif (the manufacturer of the ESP8266 and ESP32) that allows finer control over the module's behaviour than those functions made available by the standard Arduino WiFi library.

This first version of the library was called *Snifter*, a playful name that suggested packet sniffing and an alcoholic drink. However, this surfaced a fundamental question: was this a library to facilitate (potentially nefarious) packet sniffing or was this an attempt to create some alternative settlement for a more specific (legitimate and serious) purpose? The name of the library alone would start to set expectations of its intended function.

The decision to rename the library from Snifter to Approximate was a pivotal moment. Approximate was intended both to suggest an imprecision and the notion of proxemics (Edward T. Hall, 1963). Proxemics provides a rich language to describe the relative distances between individuals, rather than a surveillant absolute positioning of everything. While proxemics relates to bodies; *intimate*, *personal*, *social,* and *public* spaces make an intuitive sense for interrelations that include people and Stuff. At this point, then, a new C++ class called *Approximate.cpp* was created which makes use *PacketSniffer.cpp*, but offers a new interface to the outside world that codifies some of the logics of proxemics – forming the Approximate Library's public API. The use of the C++ language with Arduino is significant in that it is an object-orientated language that defines public and private APIs, encouraging code/object reuse (Stroustrup, 1985).

The most deliberate way in which the API imposes a new logic on the hack is its requirement to be authenticated with the network. *PacketSniffer.cpp* needs only the WiFi channel on which to operate – which is simply mapped to the frequency on which to listen. However, it is likely in a domestic setting that multiple neighbouring networks will occupy the same channel (1, 6 and 11 being the most popular) and as such simply packet sniffing on a channel will observe many data packets from other homes. The Approximate Library is intended only for authorised use on a home network – it is not a hacker's tool. To this end, observed packets can be straightforwardly filtered by the MAC address of the home router, but this still does not require authentication. Instead, the API defined by *Approximate.cpp* imposes a new condition requiring that the target network can be legitimately joined. For initialisation it demands both the network name (SSID) and password; if it can successfully join the network, it determines the channel and MAC address of the router such that the packet sniffer can filter only those packets of interest. In this sense, it simplifies the operation of the packet sniffer requiring less esoteric parameters and it also allows the library to manage any subsequent WiFi data connections that may be required by the developer.

The Approximate Library defines two types of interaction with devices; producing events when a device becomes in proximity (using a Proximate Device Handler) or when a specified device is actively using the network (using an Active Device Handler) regardless of distance. The Proximate Device Handler requires a threshold distance, that can be set as RSSI value or using pre-set values for *intimate*, *personal*, *social,* and *public* distances. This handler maintains a list of the devices currently in proximity and issues events only when a new device is seen (an arrival event) or when an existing device is deemed to have timed out (a departure event). These events report the MAC address, RSSI and size of the data packet – the data also has a direction, either up or downloading, to or from the router. Optionally, the library can also report the IP address of these devices, which is made possible by the authenticated WiFi connection and the technique of *ARP scanning*. In this way Approximate Library enables the essential features of the Naming Breadstick (page 168), identifying proximate devices and monitoring their traffic, such that a developer can easily include these functions in their code.

At the time of writing the Approximate Library has been publicly available on the GitHub website[63] and via the Arduino Library Manager[64] (integrated into the Arduino development environment) for over one year. These platforms construct a technical (but not necessarily expert) potential audience that tends to be open to experimentation with found examples. However, with the intention to address this technical audience comes some specific ways that this hack needs to be put back together and the ways it can then operate in public.

GitHub is a popular website for sharing and collaborating on coding projects that integrates with the Git version control tool. Git is the industry's de facto tool for software version control, allowing changes to be committed (and reverted if needed) by collaborative teams of developers. GitHub itself was founded in 2008 by Tom Preston-Werner, Chris Wanstrath, P. J. Hyett and Scott Chacon, but since 2018 has

[63] https://github.com/davidchatting/Approximate

[64] https://www.arduino.cc/reference/en/libraries/approximate/

been a subsidiary of Microsoft. Git was created by Linus Torvalds in 2005 for the development of the Linux kernel (Torvalds, 2005). GitHub and Git bring with them a vocabulary of collaborative terms. To *clone* is to copy a Git *repository* or *repo* for one's own use in such a way as to maintain the possibility of receiving subsequent published incremental *commits* or named version *releases*. *Forking* a project is similar to cloning but specific to GitHub, such that the forked project is published on one's own account and so enables it to gather a new independent public that can develop new features independently on this fork. A GitHub fork may make a *pull request* of its parent (or *upstream*) repository to contribute new features back to the main project or simply exist in parallel. GitHub users can star and follow repositories they favour. As a software author, GitHub's community standards encourage the inclusion of an explanatory *README.md* file and *License.txt* that specifies the licence under which others can reuse the repository – here, the short and permissive MIT License[65]. Between October 2020 and August 2021, I made 219 commits and 12 version releases of the repository.

The Approximate Library has also been available from the Arduino Library Manager since December 2020, such that it can be simply searched for and installed from within the Arduino development environment. The Arduino Library Manager makes several demands of prospective contributed libraries – requiring compliance with the Arduino Library Specification[66]. This is relatively lightweight specifying that the library must include a *library.properties* file, must follow some straightforward naming conventions, must exclude some file types and must be a Git repository, and be available from a Git-hosting website like GitHub. More descriptively there is an API Style Guide[67] that codifies some expectations the library's users will have – specifically relating to the naming of functions and their likely operation. The style guide also describes how example uses of the library, that prioritise readability, might be written. The Arduino's *Examples* menu has been long integrated into the development environment and serves an essential pedagogic function whereby students are encouraged to find, modify, and combine existing example sketches, rather than starting from scratch. Contributed libraries are encouraged to publish examples to this menu illustrating its basic and advanced functions. The requirements and expectations of the Arduino Library Manager shaped the library's development from early in the process – not least through the production of coherent examples.

[65] https://opensource.org/licenses/MIT

[66] https://arduino.github.io/arduino-cli/0.19/library-specification/

[67] https://www.arduino.cc/en/Reference/APIStyleGuide

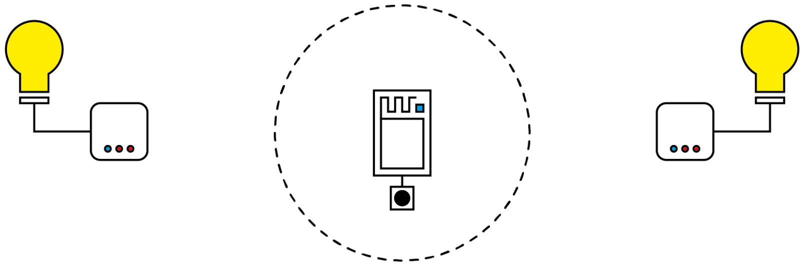
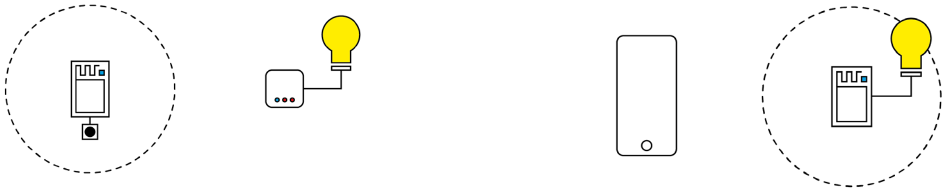


Figure 42. Approximate Library - CloseBySonoff example. © David Chatting.

Three basic examples using the Approximate Library were created: *CloseBy* (a demonstration of the Proximate Device Handler), *FindMy* (a demonstration of the Active Device Handler) and *WatchDevice* (combining both the Proximate Device Handler and Active Device Handler). *CloseBy* simple reports the arrival of any device on the network brought into proximity and its departure after it is no longer seen. *FindMy* uses signal strength to locate a specified device by monitoring the traffic it produces. *WatchDevice* uses proximity to make a pair and then watch the traffic from that paired device. There are two additional variations of CloseBy: *CloseByMQTT* which reports the arrival and departure of devices via MQTT and *CloseBySonoff* which enables one to turn on and off a proximate Sonoff WiFi switch. In a sense, these examples describe combinations of two *design patterns* (Gamma *et al*., 1994), unfinished software templates, for spatial reasoning. Design patterns are expressed with a formality that makes them easily understood – a well-chosen name, a clear diagram, and a legible code sample.[68] With this same intention, each of the examples was documented in detail in the *README.md* file, which being in the markdown format allowed hypertext links, images, and code samples. To communicate the dynamic properties, I constructed an animated diagram in the GIF format for each example – see Figure 42. In later releases of the library, a simple CSSI example for location fingerprinting was included for the ESP32, but this is to date undocumented.

As my development of the WiFi meters for the Network Home Study (Chapter Six) unfolded, they also demanded legitimate simple ways to use packet sniffing to monitor how devices were using the network. It became clear that I should develop the Approximate Library with these more resolved scenarios in mind. The use the meters made of the library disclosed some oversights which led to improvements in the parsing of packets, but also highlighted some errors with the found hack which meant large data packets were frequently corrupted. I attempted to recover data in this case, but unsuccessfully – the library was only then a partial settlement of the hack. Nevertheless, as I shall describe in Chapter Six, the Approximately Library worked sufficiently well for the meters.

[68] The Approximately Library will later be expressed as a design pattern for a network of one's own in Chapter Eight (and included in the appendix).



Smart controller (CloseBySonoff)

Smart sensor (Spiess)

Figure 43. Approximate Library - two design patterns for controlling a light – the dotted line indicates the threshold distance. © David Chatting.

In order that the Approximately Library might construct its own public, I publicised it through my Twitter account (1400+ followers), by documenting it on the hackaday.io website[69] and by making comments that referred to it on related YouTube videos. One such comment engaged the well-known electronics YouTuber Andreas Spiess (with 342,000 subscribers) through his video *Wi-Fi Sniffer as Sensor for Humans*[70]. Spiess created a new video featuring the Approximate Library, *Secure and cool Remote Controls*[71] in which he attempts to use the library to turn on a WiFi controlled light when his phone is close by – much like my Sonoff example. This video currently has 3,100 views. Spiess engaged with the project via the GitHub issues[72] to report that the departure event was not as responsive as he would like; his video raised security concerns about MAC address spoofing for a garage door opening scenario. Through our discussion it became clear that he was using the library in a way I had not anticipated. In my example the ESP module identifies a proximate light so that on the operation of the button it can address a network message to turn the light on and off – a smart controller. Spiess uses the proximity of a known smartphone to automatically trigger the light. Internally the Sonoff WiFi switch contains an ESP8266 which he reprogrammed using the Approximate Library. Spiess' phone then is simply a token, broadcasting its unique MAC address – the light is a smart sensor watching for the proximity of specific tokens, hence the concern about spoofed MAC addresses with a high-stakes security application. Figure 43 illustrates these two design patterns. On reflection, Spiess' smart sensor is the same design pattern as Want's Active Badge (Want *et al.*, 1992) which was foundational in Weiser's articulation of UbiComp (Weiser, Gold and Brown, 1999) – the mobile stuff is not smart, the smartness exists in the surveillant infrastructure. My smart controller pattern offers an alternative.

[69] https://hackaday.io/project/178369-the-approximate-library-identify-close-by-iot

[70] https://www.youtube.com/watch?v=fmhjtzmLrg8

[71] https://www.youtube.com/watch?v=cXh0T1CWtyg

[72] https://github.com/davidchatting/Approximate/issues/18

Ultimately Spiess' use of the Approximate Library is as a strawman that motivates an alternative non-WiFi system that opens garage doors automatically, with a degree of security. The YouTube comments almost exclusively respond to this proposition – however, is it clear from the GitHub statistics that many people did engage with the Approximate Library in the days after Spiess published his video on 9th May – see Figure 44. As I shall describe in Chapter Six, there was a later second wave of publicity for the library through its association with the WiFi meters and their coverage on the Hackaday website.

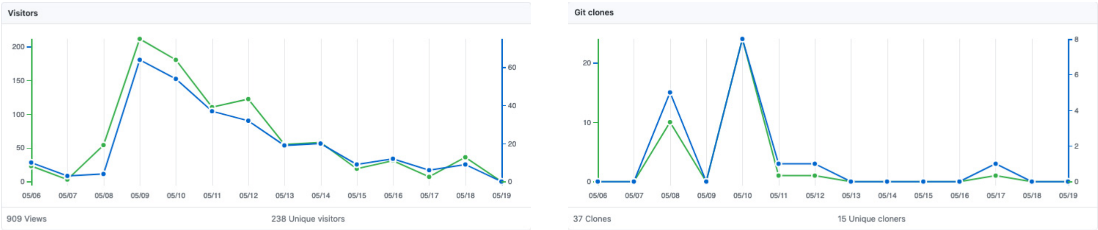


Figure 44. GitHub statistics in the days after Andreas Spiess' YouTube video on 9th May (05/09)

While it is impossible to know how many projects the Approximate Library has been used in, the GitHub statistics suggest that it has successfully engaged a considerable public audience.

As of October 2021, the library has been starred 87 times by users and it has been forked 12 times, although there have been no pull requests to date. At present the page is seen by approximately four unique visitors per day and an average of four unique users clone the repository every week. There are no download statistics available for the Arduino Library Manager. However, few in this combined audience would likely identify as designers, rather than perhaps as tinkerers, makers or coders; in this respect while these forms created a technical public for the Approximate Library, they did not perhaps reach their designerly potential. Chapter Eight will suggest that designerly hacking can bridge this technical gap for a design audience by revisiting the concept of design patterns (Gamma *et al.*, 1994).

Discussion

This chapter has described my attempts to disclose new technical alternatives in the networked home and how this process of designerly hacking has enrolled a broader public; private hackerly forms have been transformed into public designerly forms, first through the hackdays and then via public websites. Through this I have faced personal, practical, and professional challenges. The resulting products create kinds of settlements and order, be that a physical prototype and a code repository and photography; and yet when these settlements engage with new audiences and environments, they become changed. The research products I have made through this process of hacking my house are designed to accept and learn from this change. In retrospect, I have come to think of this as Pace Layer Prototyping.

Pace Layer Prototyping – how prototypes learn

Pace Layer Prototyping, by my definition, is a prototype where its form and function are not static and immutable, but instead respond to the environment in which it finds itself and the designer's emerging intentions; desirable qualities in a Research Through Design inquiry[73]. It is named to clearly reference Stewart Brand's Pace Layers model (Brand, 2018), which is a somewhat generalised form of the Shearing Layers (Brand, 1995). In Brand's sense, these are prototypes that learn by being changed by the world, in ways a human designer can interpret and manipulate – this is not learning in an artificial intelligence sense.

Pace Layer Prototyping acknowledges that once engaged with the world, prototypes and research products participate in change at different paces and that by virtue of their designed material (and immaterial) affordances can adapt and so learn. For electronic Stuff, these affordances are created by material enclosures (or substrates) and surfaces, the electronic hardware, the embedded software, data, and any subsequent interactional behaviour – with each layer participating at a different rate of change. The precise configuration of layers will be dependent on the prototype. Pace Layer Prototyping is then the design of prototypes, especially of electronic Stuff, that affords layers of change and makes it legible in a Research Through Design inquiry.

Others have previously discussed software in terms of the Shearing Layers and pace of change. In their article *Big Ball of Mud* Foote and Yoder (Foote and Yoder, 1997) consider the architecture of haphazardly developed software that rapidly evolve from

[73] For a discussion of emergence in design see Emergence as a Feature of Practice-based Design Research (W. W. Gaver *et al.*, 2022), a paper to which I contributed.

quick-and-dirty code to deployed systems. They apply Brand's model to understand how code is maintained and adapted by multiple authors over time. This analysis highlights how some modules of code become established, whilst others are subject to continual modification. This discussion is limited to software and does not consider interactions with hardware. In Dan Hill's 2003 blog post *iPod and adaptive design* (Hill, 2003), he describes how after a firmware update, he had "*a whole new iPod*"; yet the integrated battery (that typically failed after 18 months of use) was not user replaceable and the physical aspects (control wheel, buttons and screen) were unchanging. Hill briefly explains how the Shearing Layers might inform a better adaptive design for connected electronic products. These ideas seem to naturally apply to prototyping and suggest a more deliberate approach to design for change and learning.

Pace Layer Prototyping is intended then to be a useful way to describe many of the prototypes and activities of designerly hacking in this chapter, specifically the Breadstick design and the Router of All Evil. The Breadsticks offer just enough stability for the electronics to endure in the home, fixing the components together and temporarily occupying space by making attachments to the home, whilst easily (and cheaply) allowing physical reconfiguration. The Router of All Evil is perhaps the clearest illustration of Pace Layer Prototyping, where the layers are even most explicit. The commercial router has been unsettled in the hack by removing it from its case, exposing the circuit boards and allowing the original firmware update, but given a new stability through the backplate and new power supply. The addition of the Raspberry Pi and electronics prototyping area (including the pegboard panels) straightforwardly accepts hardware changes that can be recontextualised with a simple handwritten label. Immaterially the router is reconfigured in software, a process made easier through the design of the Home API (via HTTP and MQTT) and the use of Node-RED environment. Finally, the screen creates a surface on the router that can be changed 60 times a second.

This long process of *hacking my house*, has produced multiple private hacks and some public designerly forms. The notion of Pace Layer Prototyping is also intended to be a useful public outcome, applicable to many types of prototype development, where there is something to be learnt or something to emerge. It is probably most suited to designerly hacking activity in a Research Through Design inquiry as it describes how hacks are put back together – what becomes settled and what remains unsettled. This pace layer analysis of electronic products is also carried forward to the Stuff of Home model in Chapter Seven.

Conclusion

This chapter has described at length the autobiographical study of my own home and network, seeking to find technical alternatives through designerly hacking – in doing so revealing some of its invisible work. The chapter has documented many of the hacks of my network that were made privately and with workshop participants at the Hack my House hackdays; these include the Kindle, Router of All Evil and breadstick prototypes. It has become clear that while technically demanding there are a variety of practical ways to assert a network of one's own.

The development of the Approximate Library demonstrated how hacks can be transformed into public designerly forms with some success. Importantly these forms demand less technical understanding from their audience, while presenting them with new technical possibilities. In the next chapter, the Approximate Library will be used in a set of WiFi meters that help explore contemporary networked homes through ethnographically inspired methods.

Through this process I have addressed some of the practical challenges of doing autobiographical work which is self-resourced and self-directed; I hope others can apply these learnings in their work. I also proposed Pace Layer Prototyping to consider the design of prototypes using material (and immaterial) affordances to adapt and so in some senses learn at different paces of change – I hope that can inform a broad range of future Research Through Design inquiries.

Chapter Six: The Home Network Study

This chapter describes the Home Network Study which is intended to offer accounts of the domesticated Internet as it is currently configured in some British homes. Domestication here is understood through the lens of Brand's Shearing Layers (Brand, 1995), which pulls into focus rates of change and the liberties of individuals to make change in their homes – which speaks directly to the aspiration of this thesis: *a network of one's own*. To explore this, the participants of the Home Network Study are renters and so to some degree struggle with precarity, in that they do not own the spaces in which they live. The study of renters is both personally relevant, giving an intrinsic motivation to my work and widely experienced, making it easy to communicate to a public. By working with renters, the study can then disclose ways that participants make change in their homes, in general, and with their home networks, in particular. This is broadly intended to deliver a defamiliarisation of the networked home through the ethnographically inspired methods described in Chapter Three, that is subsequently used to inform theory and can inspire alternative designs.

The Home Network Study takes the familiar Design Research form of a cultural probes package (Gaver, Dunne and Pacenti, 1999) which constructs moments designed to glimpse everyday life and give participants some cause for reflection; the response materials generated inform and inspire the design process and subsequent theoretical work. Studies of this kind tend to include a collection of both paper-based and technically mediated probes, for instance maps, listening glasses, dream recorders (digital memo-takers) and disposable cameras (Boehner, Gaver and Boucher, 2012). The Home Network Study continues in this tradition using a set of provocation cards that suggest written and drawn responses or captions for photographic responses. A disposable camera no longer needs to be provided as the availability of a smartphone can be reasonably assumed. However, to allow participants to witness and make accounts of their networks does require some uncommon instruments.

The Home Network Study includes three bespoke WiFi meters that measure invisible qualities of the network: the signal strength of the home router, the dynamics of an individual device's use of the data and an overview of the constituents of the network. These Research Through Design instruments allow participants to experience and make directed explorations of their networks, while reinforcing fundamental concepts – for instance the invisible qualities of WiFi as a radio broadcast. Participants are not expected to have a detailed understanding of networking technologies but might gain some insight through their use of the meters. The meter designs are not in themselves prototypical of some speculated product or service, they instead serve to shape an experience, that pragmatically makes the network visible, in the present moment.

The Home Network Study was challenged by the COVID-19 pandemic during 2020 and 2021. Cultural probes studies can facilitate face to face and in situ meetings, between researchers and participants, at which both parties have an opportunity to nuance their understandings of the other. However, here contact was necessarily remote and mediated by technologies. As such the probes package had to be designed to be delivered as a single parcel received in the post, with sufficient self-explanation to allow participants to proceed with minimal distanced support. For this purpose, a printed booklet was produced stepping participants through the study's objectives, expectations and suggested exercises with the meters and provocation cards.

This chapter has seven sections. First, I review the related work, framing the scholarly contribution of the Home Network Study. The second section describes the constituent parts of the probes package – before the third reflects on the Research Through Design process that brought them into being. Fourthly, I give details of the deployment of the cultural probes with the recruited homes. The fifth section examines the returns materials collected and suggests some emergent themes that make a contemporary account of the domestication of the Internet and the home network. The sixth section discusses these themes concerning the related work; in particular to the Shearing Layers, which subsequently informs the Stuff of Home model proposed in Chapter Seven. I identify some common patterns of network configuration and use, which informs the articulation of a network of one's own developed in Chapter Eight. Finally, I offer some words of conclusion.

Related Work

The previous chapters have done a good deal of the necessary work to situate and motivate this study. Chapter Two made some early commitments to struggle and agonism, offering Stewart Brand's Shearing Layers as a model of domestication, over Roger Silverstone's more narrowly construed Domestication Theory (Silverstone, 1992). Chapter Three (Part One) offered a historical context to the domestic technologies and interaction paradigms that are likely to be found in the homes in this study – especially with respect to their implication of invisible labour. Chapter Three (Part Two) describes a process of defamiliarisation through ethnography and the practice of material/immaterial engaged Research Through Design as a way to produce domestic design alternatives that make the struggles with the networked home visible and challenge uncomplicated narratives of homelife.

From the perspective of HCI or Design Research, few others have applied the Shearing Layers to questions of domestication – Tom Rodden and Steve Benford (Rodden and Benford, 2003), and Marshini Chetty, Ja-Young Sung and Rebecca Grinter (Chetty, Sung and Grinter, 2007) are the exceptions. Rodden and Benford (Rodden and Benford, 2003) consider, *the evolution of buildings and implications for the design of ubiquitous domestic environments*, through their application of Brand's layers and make three useful insights: firstly (as previously noted), that the *home is never static*; secondly, to suggest HCI has a preoccupation with Stuff; and thirdly, to identify the range of stakeholders who coordinate their activities to support a home, making a specific distinction between rented and owned homes. However, while they focus on contextualising ubiquitous digital services, they do not consider the home network explicitly.

Chetty and colleagues (Chetty, Sung and Grinter, 2007) built on Rodden and Benford's work (Rodden and Benford, 2003) to question the evolution of the networked home. Through interviews with eleven participating households, they develop an account of how home networks are built, evolve and are managed. While wireless networking was part of this picture in 2007, many of the interviews relate to the challenge of Ethernet cabling and much of the discussion of WiFi is about its then insecurity. However, this paper does not engage with Rodden and Benford's ownership model and it is implied that all these households own their own homes – a necessity for wiring through the fabric of the building. Nevertheless, several interesting themes emerge from this study: the control of this complex network and means by which representations and metaphors may assist; how some see the home network as a Do-It-Yourself project; and the politics within the home of who and what is allowed to connect and when. While this work clearly demonstrates the utility of the Shearing Layers, it does not productively extend the framework.

There are several other notable ethnographic HCI home network studies, specifically: Grinter, Edwards, Newman and Ducheneaut's *The Work to Make a Home Network Work* (Grinter *et al.*, 2005) and Tolmie, Crabtree, Rodden, Greenhalgh and Benford's *Making the Home Network at Home: Digital Housekeeping* (Tolmie *et al.*, 2007). While they do share authorship with the previous work, they do not explicitly reengage directly with Brand's Shearing Layers, but rather reveal tasks of digital housekeeping – which one might read in terms of Brand's concept and practice of maintenance; neither do they deal explicitly with questions of domestication.

The studies described thus far slightly predates the mass adoption of secure wireless networking in the home. In the UK at least, by the end of 2006 half of all adults were living in households with broadband (Ofcom, 2007) but it took until around 2008 for the growing number of previously insecure domestic WiFi networks to require a password, using the relatively secure WPA2 protocol. It is my contention that this adoption of fast secure wireless, over wired networking, was transformational for the domestication of the Internet – especially for people who did not own their homes. However, this transition seems relatively neglected by the ethnographic HCI literature. By 2012, Andy Crabtree and colleagues (including Richard Mortier and Tom Rodden) were concluding that networking had become unremarkable, that, "*for most people the home network has ceased to be a technological object and has become a sociological object*" (Crabtree *et al.*, 2012, p. 563); and yet by this point wireless networking was assumed, almost without mention. Instead, the attention of these researchers had shifted to matters of contention and ownership. In 2010, Marshini Chetty in collaboration with Microsoft Research at Cambridge (including Richard Harper), evaluated an instrument to monitor network bandwidth called Home Watcher with six households, intended to reveal *who's hogging the bandwidth?* (Chetty *et al.*, 2010). In 2012, Richard Mortier and colleagues (including Tom Rodden) were proposing redesigns of the home router to own your home network by allowing monitoring and control of network traffic (Mortier *et al.*, 2012).

The WiFi meters in this study were designed to disclose otherwise invisible qualities of the network in specific experiential ways, but unlike (for instance) the Home Watcher (Chetty et al., 2010), these are not intended as prototypical tools, but instead are technically mediated probes designed to elicit moments of reflection, in a Research Through Design inquiry. While such probes are common in studies that employ cultural probes, their design and motivation are perhaps underexamined. My designation of these meters as instruments attempts to redress this, deliberately reflecting Dewey's language of pragmatism (or indeed instrumentalism) and bringing a focus on specific situated experiences (see Chapter Four). Peter Dalsgaard helpfully offers a conceptual framework for such instruments of inquiry in design, comprised of five qualities: perception, conception, externalisation, knowing through action and mediation (Dalsgaard, 2017). Perception: what the instrument reveals and what it hides. Conception: how the instrument poses questions and hypotheses. Externalisation: how the instrument operates to enable distributed cognition (Hutchins, 1995) and creates external representations. Knowing through action: how knowledge is generated through embodied acts with the instrument. Mediation: how the instrument mediates between the constituent actors and artefacts – indeed the network. I shall later use this language in describing my meters.

With regard then to the related work, the Home Network Study seeks to productively extend the Shearing Layers framework, contributing a contemporary account of the (predominantly wireless) networked home and a consideration of the design of technically mediated probes.

The Probes Package

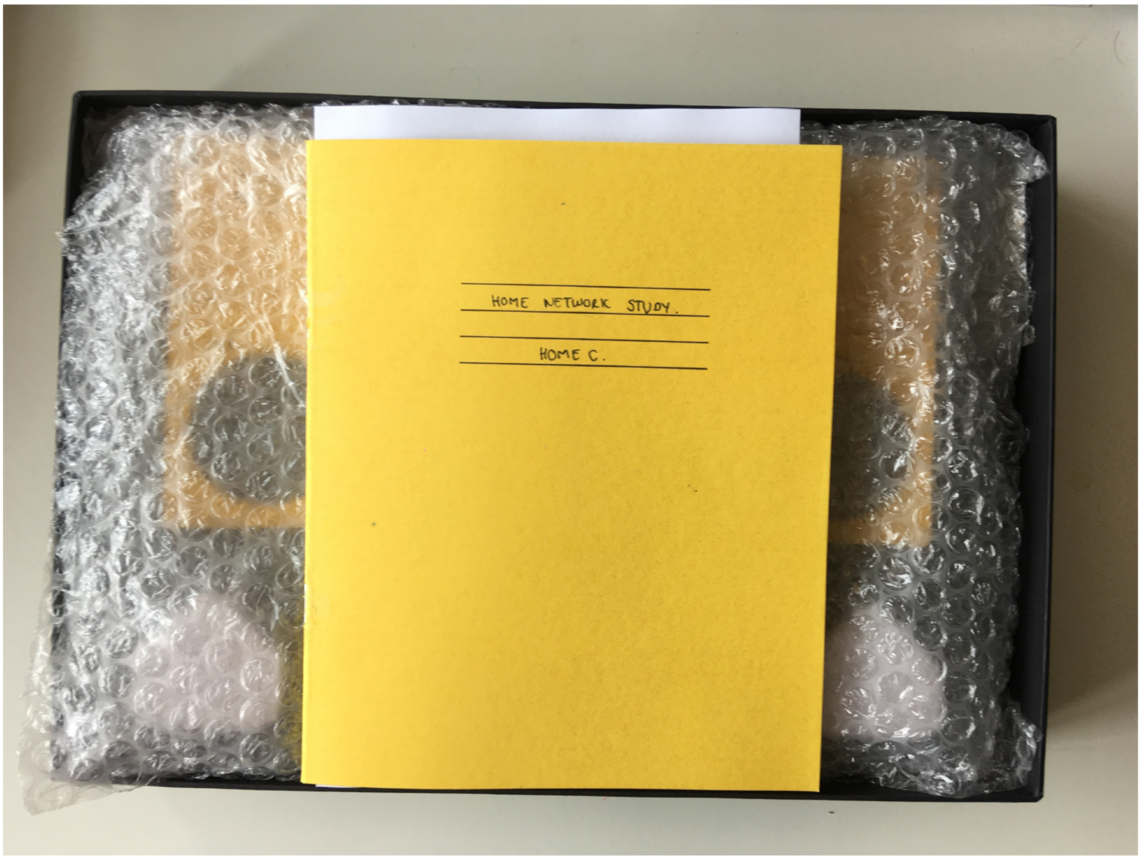
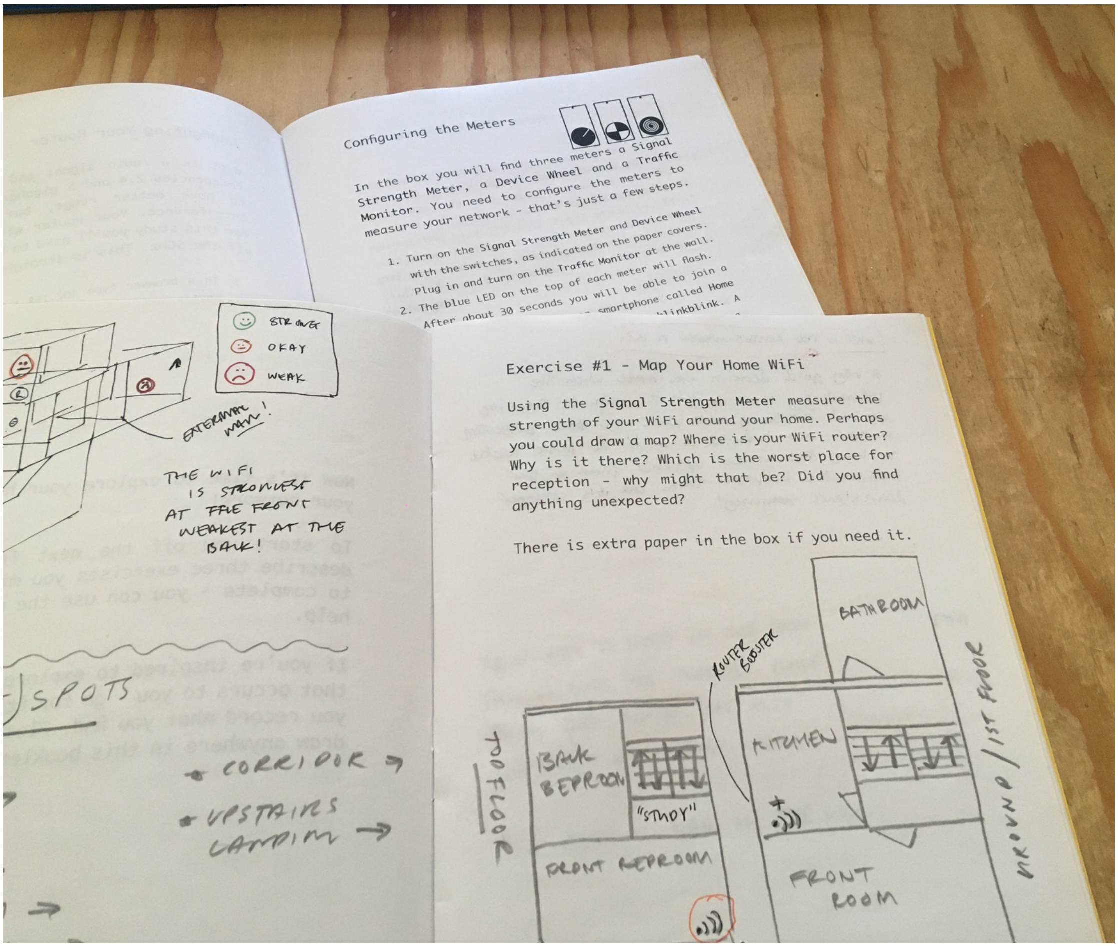


Figure 45. Probes package. © David Chatting.

Once delivered, the participant opened the package to find first the printed booklet, then three WiFi meters (including cables and USB power adapters) and 52 provocation cards. This section describes each of these elements as they were encountered using the descriptive text from the booklet – the section that follows offers some rationale for the many decisions these designs embody and the Research Through Design process of which they were part. When enacted the probe package is designed to generate a wealth of rich visual and written return materials, to reveal perspectives of contemporary cultural and technological practices.

The Booklet



Configuring the Meters

In the box you will find three meters a Signal Strength Meter, a Device Wheel and a Traffic Monitor. You need to configure the meters to measure your network - that's just a few steps.

1. Turn on the Signal Strength Meter and Device Wheel with the switches, as indicated on the paper covers. Plug in and turn on the Traffic Monitor at the wall.
2. The blue LED on the top of each meter will flash. After about 30 seconds you will be able to join a smartphone called Home linkblink. A

Exercise #1 - Map Your Home WiFi

Using the Signal Strength Meter measure the strength of your WiFi around your home. Perhaps you could draw a map? Where is your WiFi router? Why is it there? Which is the worst place for reception - why might that be? Did you find anything unexpected?

There is extra paper in the box if you need it.

Figure 46. Booklet pages. © David Chatting.

In this booklet you can record your findings as you explore your home and your network. At this point please complete the enclosed consent form.

You will find three WiFi meters and a set of 52 cards in the box. First you will need to configure your router and the meters to measure your network. The next few pages will show you how – it won't take long. Then there some exercises to get you started and an explanation of how to use the cards.

Happy Exploring!

With a remote deployment the printed booklet was required to speak with my voice to quickly reiterate the study's objectives, expectations and to suggest exercises with the meters and cards – while allowing responses to be made on its blank pages. This required a careful treatment with clear direct written language and formatting – each page succinctly covered a new topic. There were 15 single-sided printed pages, followed by 8 double blank pages – on which participants were encouraged to write or draw. For this British audience, the booklet is recognisably a school exercise book to further encourage this form of engagement.

Two configuration steps are required for the network and the meters. Firstly, the 5GHz network needs to be temporarily disabled on the router. Having previously requested details of the router, the booklet contains bespoke instructions to clearly enumerate the required actions. Secondly, the booklet instructs the participant on how each meter is configured with the details of their WiFi network. These steps were carefully designed for those with little or no experience of network administration.

The remaining pages of the booklet described each meter and suggest three exercises that promote the use of the meters: Map Your Home WiFi, What's on your WiFi? and Traffic Conditions. Finally, the provocation cards are introduced, and it is suggested that they might be used as captions for photographic responses.

The Signal Strength Meter

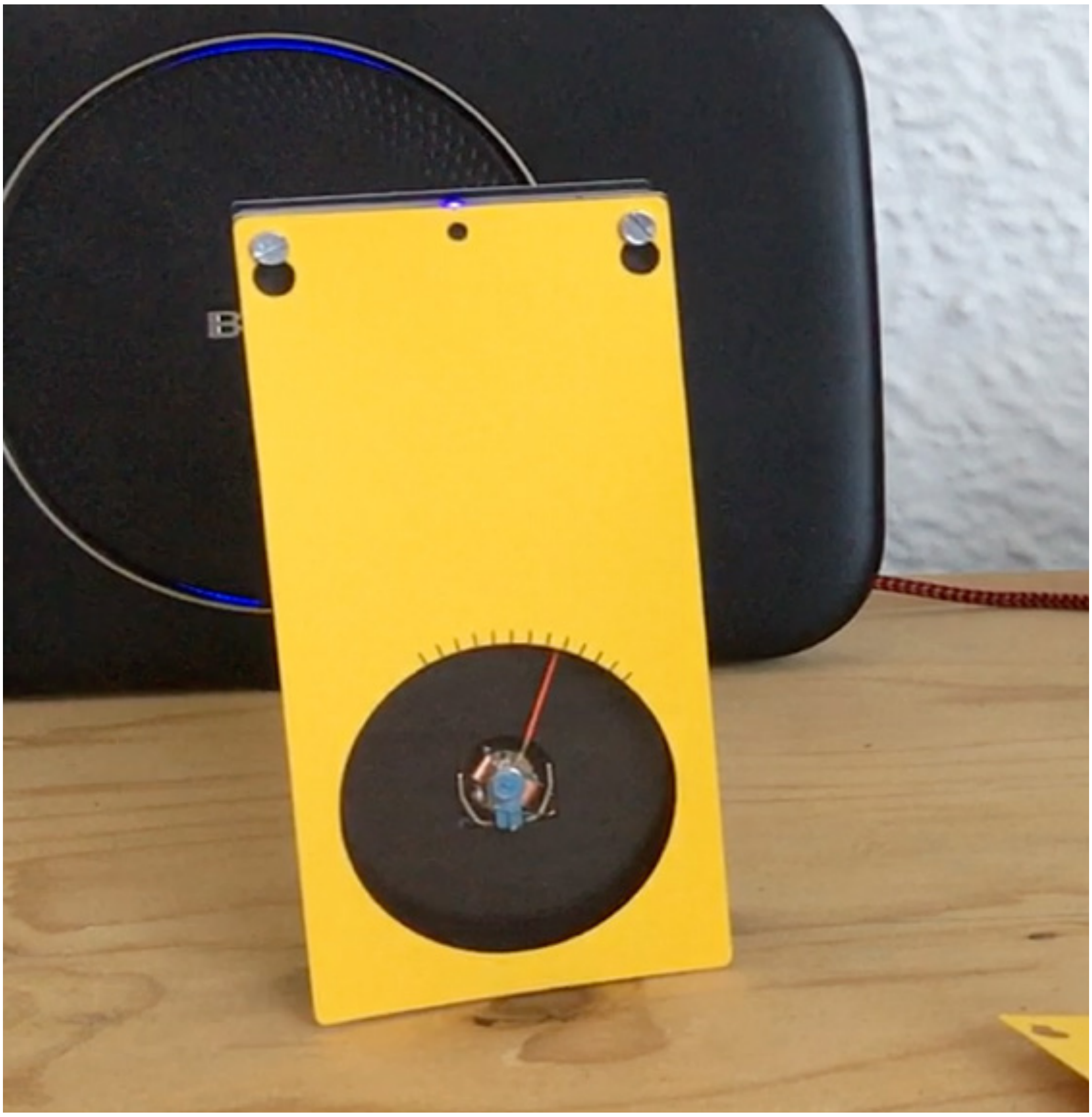


Figure 47. Signal Strength Meter. © David Chatting.

The Signal Strength Meter measures the signal strength of your router in different parts of your home. Use the switch on the side to turn it on–- if it is properly configured after a moment the blue LED will light steadily. If it continues flashing, it can not see your network and may need to be reconfigured. If it does not light the battery is flat and will need to be recharged.

This meter charges via a USB socket–- a lead and power adapter are to be found in the box.

The Device Wheel

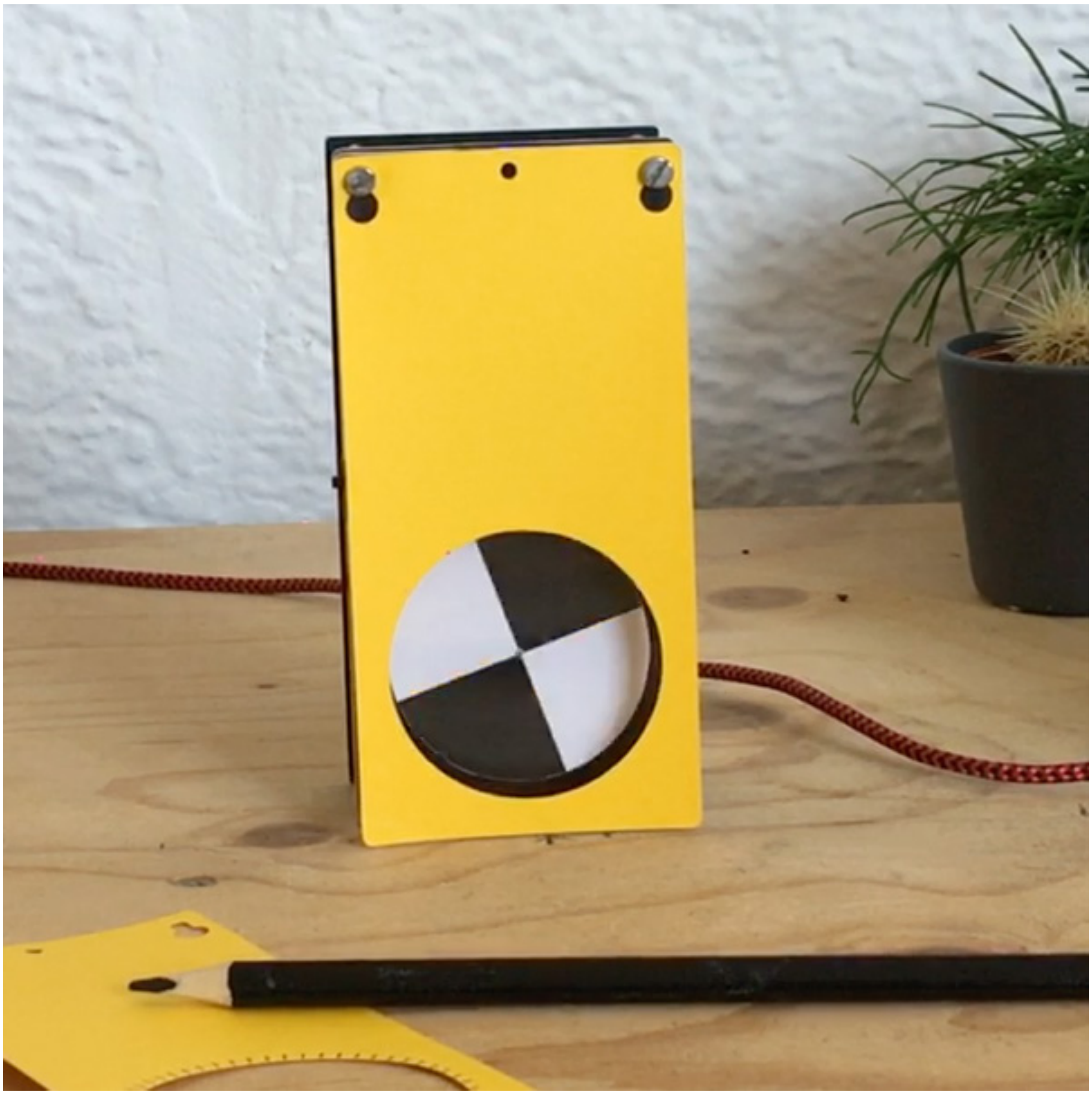


Figure 48. The Device Wheel. © David Chatting.

The Device Wheel is a meter that watches an individual device's use of the network. Use the switch on the side to turn it on–- if it is properly configured after a moment the blue LED will light steadily. If it continues flashing, it can not see your network and may need to be reconfigured. If it does not light the battery is flat and will need to be recharged.

Bring the meter close to a device – the blue LED will blink. Now whenever this device uses the network the wheel will spin–- clockwise for downloads, anti-clockwise for uploads. Repeat the process to make a new pair.

On the back of the meter you will find some ways of putting it up in different places. Be careful with the magnet – it's very strong and would damage a computer's hard disk, etc.

This meter charges via a USB socket–- a lead and power adapter are to be found in the box.

Traffic Monitor

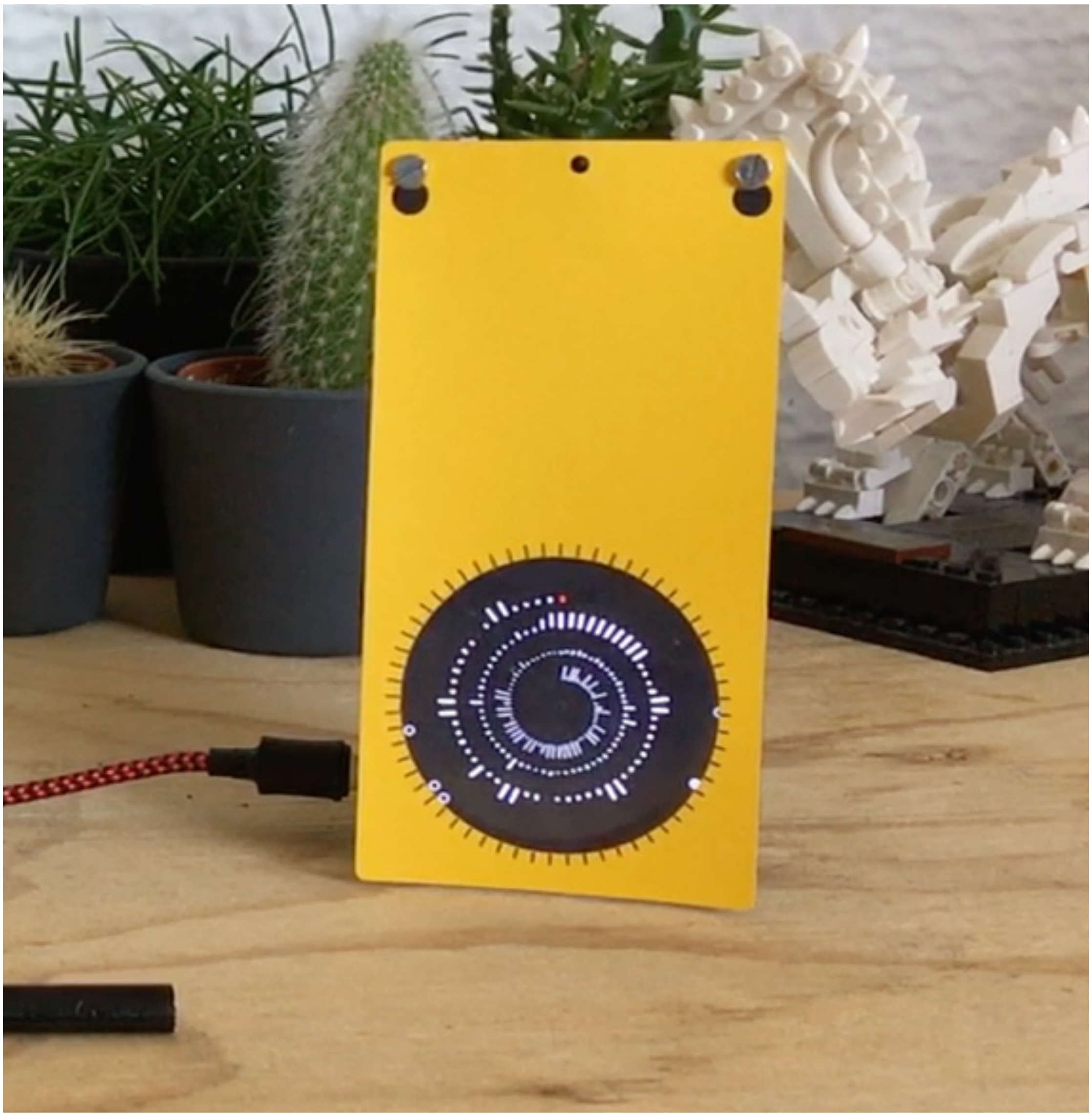


Figure 49. The Traffic Monitor. © David Chatting.

The Traffic Monitor is a meter that displays the last three minutes of your WiFi network traffic.

Plug it in with the USB socket on the side – the lead and power adapter are to be found in the box. You will see the computer boot on the screen, after a minute or so the black and white dial will be seen.

If it is properly configured after a moment the blue LED will light steadily. If it continues flashing, it can not see your network and may need to be reconfigured. This meter has no battery and can stay plugged in. It will get warm, but not hot. It can be switched off at the wall.

Once operational, the meter will show devices on the network as circles on the periphery of the dial, which flash when they are active – always in the same position. Lift the paper cover for more details.

Provocation Cards

1. The smartness non-human
2. A technology free zone
3. The oldest working electrical appliance
4. Switched off at the wall
5. The Internet starts here
6. The Internet stops here
7. The smallest thing that’s part of the furniture
8. Immovable
9. A new thing looking for a place to live
10. An intruder
11. A poltergeist
12. The walls have ears
13. Something Google doesn’t know about
14. Mind of its own
15. Something that’s been painted over
16. Something the landlord doesn’t want you to touch
17. Something the previous tenants should collect
18. Can’t touch this!
19. The landlord needs to fix this
20. A bodge, a fix and a hack
21. Where things go to charge
22. What does your network look like?
23. All the things on your network
24. A hiding place
25. From a different planet
26. Frequently lost
27. A portal
28. Something to hide from the landlord
29. Something I’d change if I owned this place
30. A thing that’s not on the Internet anymore
31. A utility
32. If this was on the Internet, it’d…
33. Where does this lead?
34. Precarious
35. On its last legs
36. You rang, m’lord?
37. A keeper
38. In case of emergency
39. Work, rest and play
40. Useless
41. My best D.I.Y.
42. Homemade
43. Purgatory
44. Remote control
45. Where the heart is
46. Useless without the network
47. Now lives in the cloud
48. Something that comes and goes
49. I have never… refused a visitor my WiFi password
50. I wish I knew who named this network…
51. Alreet pet?
52. Canny

You’ll find 52 cards in the box, each asks a question or makes a suggestion for something you could explore at home. Try some out–- the instruments are there to help you. Some cards are a little poetic, others a little scientific.

Many of the cards might be answered with a photograph – hold up the card in view so I know what it is. For other cards you might want to write or draw something here in this booklet – make sure you include the title of the card with your response.

At the end of the week we will arrange for the meters and booklet to be returned to me. The photographs you choose to share with me could be sent via Whatsapp or similar.

Probe Design

This section offers some rationale for the many design decisions embodied in the probe package expressions of my Research Through Design process.

A Family of WiFi Meters

With the ambition to make simple instruments with well-defined and easily communicated functions, a small set of meters was preferred over a single multi-meter design – which would necessarily have had to accommodate different modes and views. Such collections are reminiscent of the Interaction Research Studio's design of the Indoor Weather Stations (Gaver et al., 2013) and imply a consistent design language is found. As the Research Through Design process played out, a set of strong family resemblances came to be imposed between the meters through their physical design, hardware, software, and consequent behavioural qualities. Each facet of the design accommodated change and experimentation at different rates, consistently with my account of Pace Layer prototyping, described in Chapter Five. Once settled, family resemblances simplified both the interactional experience of using the meters and their construction.

Function

With respect to the function of what should be designed, the possibility of the WiFi meters was exposed through a process of designerly hacking and an interest in scale. My immaterial explorations of a home network (Chapter Five) suggested an early candidate was a signal strength meter for the router, to measure the availability of WiFi around the home (using RSSI). This surfaces some of the radio nature of WiFi and demonstrates how radio reception is shaped by the physical/slower layers of the building – giving an infrastructural perspective on the network. With the signal strength meter as the starting point, the other two meters were then developed to examine two further scales of inquiry. The Traffic Monitor asks what devices constitute this network and how they use this shared resource. The Device Wheel scrutinises but one device, spinning a wheel in response to its network traffic.

The design of the meters responds to a range of existent designs, not least Natalie Jeremijenko's Live Wire (also known as Dangling String) (Weiser and Brown, 1995) and the Tangible Media Group's Pinwheels (Dahley, Wisneski and Ishii, 1998; Ishii, Ren and Frei, 2001); originally described in the context of Ubiquitous Computing (Chapter Three). Both have an appealing tangible analogue quality that allows the network to be experienced in some sense; yet they are both installed for exhibition in a space, rather than at the personal scale implied by a meter. In seeking to expose people's *network anxieties*, James Pierce's handheld ghost/listening bug/radio wave detectors offer some reference points for meter design (Pierce and DiSalvo, 2018). Pierce manipulated the surface design of electromagnetic field meters, originally meant for scientific and engineering purposes, by replacing their printed elements, like product labels and scales, achieving a superficial recontextualisation of devices. The resulting careful ambiguity of quantitative readings is consistent with the intention of technically mediated cultural probes.

An instrumentational, yet ambiguous, functionality is mirrored in all three WiFi meters. The Signal Strength Meter transforms signal strength into movements of a needle on an unlabelled analogue gauge; there resonances here with Timo Arnall and colleagues' light painting with WiFi (Arnall, Knutsen and Martinussen, 2013) and Erik Grönvall's FeltRadio (Grönvall, Fritsch and Vallgårda, 2016) and WiredRadio (Grönvall, 2018). The Device Wheel shows the size and direction of data flowing by driving a disc clockwise and anti-clockwise, most clearly inspired by Live Wire and Pinwheels, but also sharing some purposes with Nicole He and Eran Hilleli's Invisible Roommates concept made for Ikea (He and Hilleli, 2021). The Traffic Monitor creates a visualisation of activity on the whole network over the past minutes; revisiting some of the intentions of my Home Network Map (Chatting, 2017) and also of BERG's Network Murmurations (Formo, 2012), Abigail Durrant's OnLines (Durrant *et al.*, 2017) and Mike Shorter's Scout (Shorter, 2019).

Physical Design

The meters have a strong physical family resemblance intended to communicate an equality between the designs; each fascia has the same height and width (63mm x 126mm, a 1:2 ratio) and is built of the same laser-cut stacked materials (3mm mat black and clear acrylic) – each display inscribes a circle with the same centre point and is framed by an identical paper window. The paper cover is intended for participants to mark with their recordings, and it allows the meters to be directly annotated with instructions. It can be easily removed and replaced – with the blank sheets provided. The meters have a simple colour palette of yellow and black, with details in white and red. The dominant yellow is commonly associated with scientific test equipment and this paper colour offers good contrast with dark pen inks. In general bright colours can usefully make a design strange, highlighting an intervention or speculation against the environment – consider Superflux's Uninvited Guests (Superflux, 2015). However, as inquiry-driven Research Products, rather than a superficial film prop, the meters' design requires a sufficient finish and independence to allow them to be operated confidently by non-experts over a period of days or even weeks (Odom *et al.*, 2016).

There are specific ways in which the physical affordances of the meters differ too in relation to their function. The Signal Strength Meter is designed to be held in the hand as measurements are taken around the home. While the Device Wheel is a kind of sentinel that makes sense if temporarily positioned in proximity to the device it is watching. To enable this the back surface supports various ways of making temporary attachments in the home – informed by the Breadsticks in the Hack My House study. It can be hung on an available nail with the provided keyhole slot, stuck to a surface with the suction cup or with the strong magnet. With this intended mobility both the Signal Strength Meter and Device Wheel contain batteries that are rechargeable via USB. The Traffic Monitor is imagined on the mantlepiece like a clock, and as such it stands at a slight upwards facing angle. The Traffic Monitor is then intended to be statically positioned and always-on, powered via a micro-USB socket made accessible at the edge of the device.

The physical stacked design of the meters makes the Pace Layer Prototyping of Chapter Five explicit; where the paper layer and attachment affordances are the most explicit demonstration of this, accommodating in situ reconfigurations of the meters in deployment.

Hardware

Much of the hardware design is also common between the meters. Each uses the inexpensive ESP8266 WiFi module (as previously used in Hack My House); with the WiFi aerial being exposed through the enclosure in the same position under the paper layer. At the top of each meter a blue LED indicates the state of the WiFi connectivity. The Signal Strength Meter’s display is a modified analogue gauge (a voltmeter) driven directly by PWM. The Device Wheel operates a Walkman motor, via a motor control module. The Traffic Monitor employs a Raspberry Pi Zero to drive a 4-inch colour screen[74] and read data from the attached ESP8266. For the battery-powered Signal Strength Meter and Device Wheel a convenient choice for power management was the Adafruit Feather HUZZAH which incorporates an ESP8266 and a charging circuit, that also supports a simple power switch.

While the choice of the inexpensive ESP8266 simplified the development of the meters, it constrained their operation in a significant way. The ESP8266 (and related ESP32) interoperates with 2.4GHz WiFi bands, but not the higher 5GHz frequency. At the time of development there were no similar low-cost WiFi capable microcontrollers

[74] Being the largest component, the display informed the width of all three meters.

available, operating at 5GHz.[75] Almost every modern home router supports both frequency bands, but devices tend to default to 5GHz – which means their use of WiFi will be invisible to the meters using the ESP8266. This can be resolved by turning off the 5GHz network, forcing devices to switch to 2.4GHz. However, giving participants this immediate technical challenge gave me a good deal of deliberation. The performance of 5GHz tends to be better as it operates in regulated frequencies and has better strategies to reduce interference, but 2.4GHz by virtue of its longer wavelength has better penetration of walls and so is likely to have superior coverage. I had turned off my home 5GHz network in developing the meters and had noticed no significant difference. Asking participants to temporarily turn off the 5GHz then seemed to be a reasonable request. The challenge then was to communicate this procedure clearly to participants and ensure it could be easily reversed. This was accomplished through a page in the booklet which detailed each step, tailored to the model of the participant's router. I synthesised the steps through my understanding of the routers gleaned from online manuals and videos, sensitive in my use of language that participants may have little or no experience of network administration. Rather than an inconvenience, I came to see this moment of technical challenge for the participants as part of the probe inquiry, when some of the functions of the router would be revealed to them.

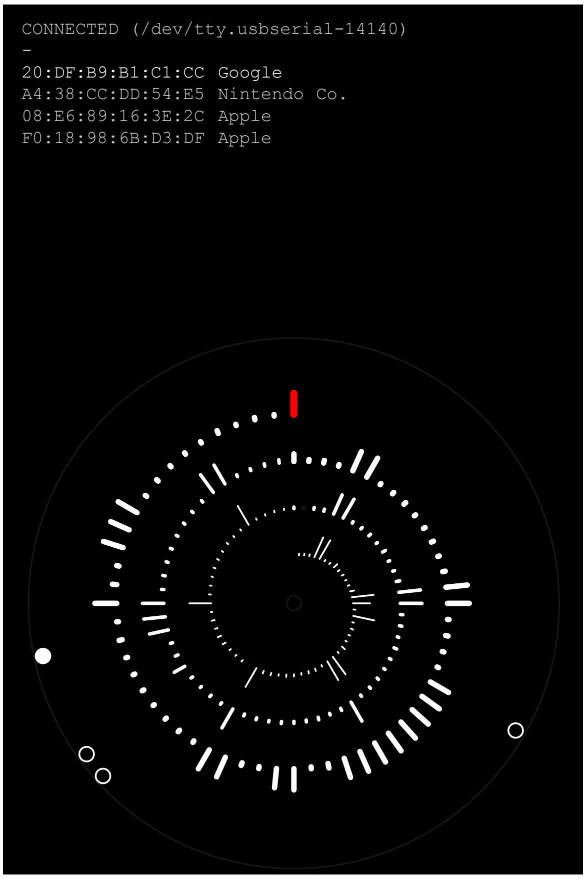
Software

With a common hardware platform, the meters could share much of the software code, allowing consistent behavioural qualities and interactions. The ESP8266 WiFi modules were programmed using the Arduino IDE in C++ and the Raspberry Pi Zero ran a Processing sketch written in Java.

As my account of Pace Layer Prototyping suggests, the software for the meters underwent frequent change in this Research Through Design process. In early prototypes of the Device Wheel, the device under examination needed to be manually reconfigured to join a new WiFi network created by the meter, which seemed arduous. However, the Naming Breadstick (Chapter Five) had suggested an alternative: that

[75] The unavailability of 5GHz devices should not go without comment. Unlike the 2.4GHz band, the use of 5GHz is regulated by bodies such Ofcom (Office of Communications) in the UK and the FCC (Federal Communications Commission) in the USA and requires product certification. As such there are associated costs in the development of 5GHz device. Interestingly the 2.4GHz band is unregulated precisely to allow the operation of microwave ovens at this frequency; one domestic technology shapes the opportunities for the next (Herman, 2010).

devices could be identified simply by bringing them in proximity of the meter and their network usage could be monitored using this same packet sniffing technique. Over time these hacks became formalised as functions in my Approximate Library (Chapter Five), which ultimately was used in some way by every meter. In use the meters disclosed some initial oversights in the library, which in turn led to improvements in how packets were parsed internally. However, some errors were also highlighted which have to date not been resolved, where large data packets are frequently misread. The library is then only then a partial settlement of the hack.



```
CONNECTED (/dev/tty.usbserial-14140)
-
20:DF:B9:B1:C1:CC Google
A4:38:CC:DD:54:E5 Nintendo Co.
08:E6:89:16:3E:2C Apple
F0:18:98:6B:D3:DF Apple
```

Figure 50. Traffic Monitor Visualisation. © David Chatting.

With its display and computation, the Traffic Monitor offered the most abundant and open-ended possibility that could be configured flexibly in software. The visualisation of the traffic went through multiple iterations over an extended period in search of a satisfying balance of detail and ambiguity. In early prototypes, the meter presented information about the connection to the Internet (for instance, upload and download speeds) as well as the state of the home network. While interesting this seemed to somewhat unhelpfully shifted attention outside the home. I sketched more artful visualisations that cast network activity as the movements of cellular creatures or particles in a cloud chamber, but I ultimately preferred the sparser instrumentational form that seemed it be more consistent with the other meters.

In the final version of the Traffic Monitor, the spiralling graph juxtaposes the past three minutes of network traffic volume. A somewhat familiar watch face is suggested with a one-minute circumference and with time proceeding in a clockwise direction in one second units. The function mapping the volume of observed network traffic (in bytes) to graph height (in pixels), was calibrated so that some common network events would likely be visible. I tuned it for voice assistant commands, audio streaming and video conferencing, magnifying smaller differences in midrange values using a logistic Sigmoid function. A consequence of this high sensitivity was that with relatively little traffic, in comparison to the network's total capacity, the meter will display the maximum value. I considered ways of adjusting sensitivity and timescales using physical controls but instead preferred to keep the interaction simple. A sparse representation of devices on the network is shown on the periphery of the circle, with a more detailed device list, showing the MAC addresses and manufacturers, to be seen by lifting the paper layer[76]. Both network device representations blink when active. Figure 50 shows the design.

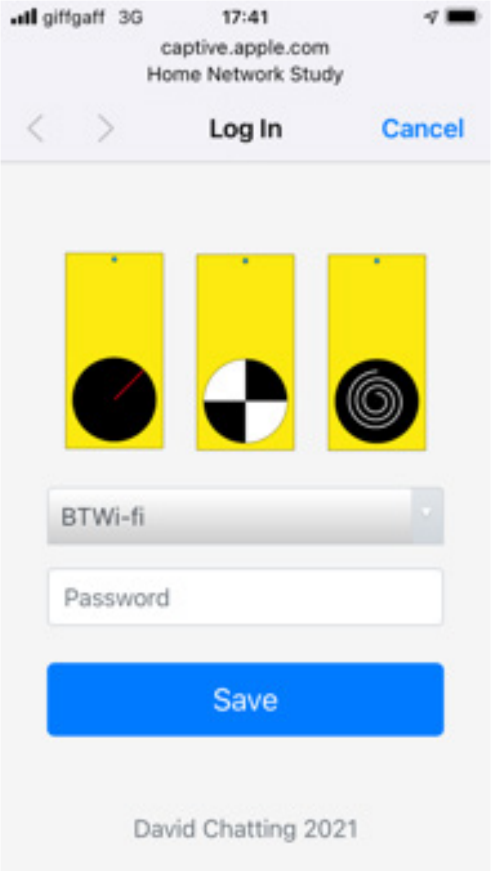


Figure 51. WiFi configuration as viewed on an iPhone. © David Chatting.

[76] Such a paper window is reminiscent of Luckbites' BirdBox Alarm Clock (Bishop and Hulbert, 2009) that co-opts an iPhone display.

In combination with the hardware and physical design, the software contributes to the behavioural qualities of the meters, with each intended to have a mechanical/analogue quality. While their physical design references scientific instruments, each attempt to render a quality of the network with a degree of ambiguity, rather than an absolute numeric quantity. In each an available level of precision that is obscured and other qualities that are deemed uninteresting are discarded – this speaks directly to Dalsgaard's perception. There is then a necessary degree of sensemaking required to interpret these ambiguous measures that is intended to encourage an experimental knowing through action as hypotheses are conceived and tested. Each instrument's paper layer supports in situ annotation, an aide for externalised distributed cognition. It is the explicit purpose of these meters to disclose the mediation between elements in the network, they are not directly interactive (e.g. through button pressing) but instead react to how they are placed with respect to elements of the network and its activity.

Finally, WiFi configuration was a considerable software challenge for the meters. Beyond their physical finish and build, their *independence* was dependent on the participants' ability to configure them correctly for their network, without my intervention (Odom *et al.*, 2016). With three individual meters it was clear that configuring each in turn could become tiresome. A popular pattern for WiFi configuration is called a *captive portal*, which will be familiar to users of WiFi in public spaces – a temporary network is created by the device itself, which once joined by a third-party device, like a phone, pops up a simple page allowing an SSID and password to be set and saved. With the credentials set the device will automatically join the configured network and the captive portal network will no longer be visible. Ultimately, the meters used the YoYoWiFiManager Arduino library, developed for the Yo-Yo Machines project at the Interaction Research Studio, to which I contributed (Gaver and Boucher, 2021). The YoYoWiFiManager, unlike the popular WiFiManager (Tzapu, 2015), creates a peer network of the meters that allows all to be configured in a single simple interaction – see Figure 51. It also allows full customisation of the configuration webpage and the use of modern responsive JavaScript frameworks like Vue and Bootstrap. Like the Approximate Library, the development of the YoYoWiFiManager library and the meters were contemporary, with each influencing the development of the other. Successful independent configuration of the meters was crucial and consumed much of the technical development time – indeed it failed in the initial pilot study.

As a further way of engaging a public in the outcomes of my designerly hacking, I maintained a software repository for the project on github.com[77], published under an

[77] https://github.com/davidchatting/ThreeWiFiMeters

MIT License. This continues to serve as a record of the incremental evolution of the software and a site for documenting my meter designs. For this purpose, I created an image of the three meters in operation (a short animated GIF) and circuit diagrams for each. These enabled me to create graphical posts for my Twitter[78] and Instagram[79] accounts, then to approach the hackaday.com website to cover the project on their popular blog. The resulting story, *ESP8266 Network Meters Show Off Unique Software* (Nardi, 2021), describes the meters and the software libraries (Approximate and YoYoWiFiManager), curiously likening the meters to the enigmatic *three seashells* in the film Demolition Man (Brambilla, 1993)[80].

Provocation Cards

The provocation cards were designed primarily as photo caption cards to be used in combination with a phone camera. I initially considered making a fourth device, a dedicated camera, using the TaskCam designs from the ProbeTools project (Boucher et al., 2019), but a camera is not revealing of the network in the same way as the meters were and it seemed to complicate the set. Instead, I took inspiration from TaskCam's short question format and designed a set of playing cards that would primarily be used as in situ captions for photographs; but being made of card they could also be marked on in response to the question. To suggest a playful approach, I decided on a deck of 52 cards, a number also large enough as to be clear they should not be completed exhaustively, but instead selected if they resonated. The 52 questions and statements evolved over time; some were intended to be used with the meters (6. The Internet stops here), while others suggested specific compositions (15. Something that's been painted over) and some were more ambiguous (45. Where the heart is). In combination the questions were designed to surface accounts of the domesticated Internet and the liberties of individuals to make change in their homes – especially as they might relate to Brand's Shearing Layers. The card format came to resemble Peter Schmidt and Brian Eno Oblique Strategies card (Schmidt and Eno, 1975) and this also suggested a style of language to adopt.

[78] https://twitter.com/davidchatting/status/1419339763165941762/

[79] https://www.instagram.com/p/CRs_6b1IL-O/

[80] Sylvester Stallone's character in Demolition Man is woken after 36 years of being held in a cryogenic prison to find unfamiliar future. The unseen *three seashells* are a comic example of the confusion that meets him, to be used in some way as a functional replacement for toilet paper. Yet the viewer's imagined affordances of these shells creates a comic confusion of how exactly this should accomplished.

Deployment

The deployment of the Home Network Study was challenged and shaped by the COVID-19 pandemic during 2020 and 2021 in significant ways. The participants were necessarily remotely recruited, receiving the probes package in the post and after (typically) one week returning the package with completed returns materials, ahead of an online interview over Zoom or Teams that lasted for at most one hour. The interviews were semi-structured around the returns and some demographic questions; they were all consensually audio recorded.

A single set of meters were reused in each household, with the printed materials being reproduced on each occasion. The deployment was trailed with a pilot study, which demonstrated that the provocation cards worked well as photo captions but exposed a serious problem with the meters' WiFi configuration and Andriod phones. This was resolved for the first full deployment.

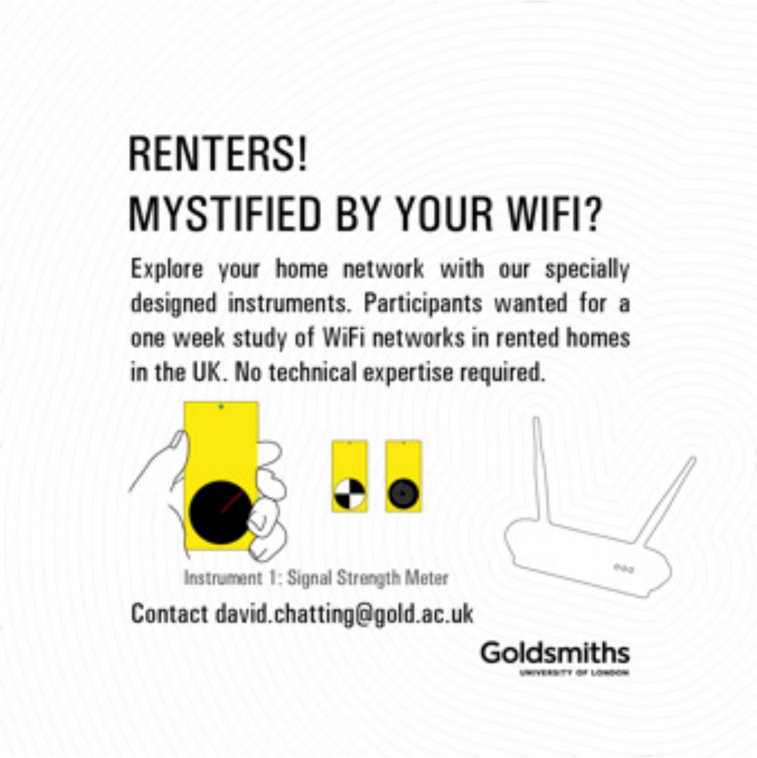
Ethical Considerations

While the ethical protocols for cultural probe studies are well established, by its nature this study produces a set of responses that reveal some of the private life and dynamics of the home on and off the network. As such this study needed to be approached with sensitivity. The WiFi meters were deliberately designed so that they do not retain any of the data they collected from the network, instead presenting it in ways for the participants to mediate what was disclosed. The application made for ethical approval considers the participants' security and anonymity carefully; it is included in full in the appendix and was granted by the Department of Design at Goldsmiths in October 2018. The COVID-19 necessity to conduct the interviews online, rather than in person, mitigated issues related to my own safety in participants' homes.

Recruitment

I produced a recruitment flyer communicating the essential details of the study, which I distributed through my social media accounts on Facebook, Twitter and Instagram – as well as by word of mouth – see Figure 52. I incrementally recruited six households and while I was by no means overwhelmed by applicants, as the roster grew, I was able to select participants with a diversity of situations, geography, and outlooks.

Initially I had limited participation to households in Newcastle and London, to allow face-to-face meetings and in-person deployments; once the study became fully remote the probes package had to operate more independently, but the scope of locations became wider, with the only constraint being courier fees. Nevertheless, to give the study a degree of specificity, I required participants to be renting homes in the UK; indeed, ultimately all six households were in England.



RENTERS!
MYSTIFIED BY YOUR WIFI?

Explore your home network with our specially designed instruments. Participants wanted for a one week study of WiFi networks in rented homes in the UK. No technical expertise required.

Contact david.chatting@gold.ac.uk

Goldsmiths
UNIVERSITY OF LONDON

Figure 52. Recruitment flyer. © David Chatting.

Participants

Following the pilot study, seven homes (A to G) were recruited; however, personal circumstances prevented the participation of Home F. The six remaining households consisted of 12 adults (aged 26 to 45 years old) and one child (aged 2 years old); eight males and five females. By the UK government's Index of Multiple Deprivation (IMD) on a scale from 1 (most deprived) to 10 (least deprived), participants' homes (by postcode) have IMD scores of between 2 and 10 (according to the latest 2019 statistics). The six households were then:

Home A

Steve (male, 27 years old) and Helen (female, 28 years old) are partners and live in a two-bedroom top-floor flat in Longbenton, Newcastle upon Tyne (IMD of 2). Both are in full-time employment with permanent accountancy jobs. They have rented this flat together for the past two years, having previously lived in a larger shared flat. Steve was the primary respondent.

Home B

Chris (male, 31 years old) and Claire (female, 31 years old) are partners and live with their flatmate Ella (female, 30 years old) in a split-level two-bedroom apartment above a shop in Dulwich Village in South West London (IMD of 8); the shop is owned by their landlord. Chris is a full-time PhD student, Claire works part-time in retail with a permanent contract and Ella is a full-time teacher. Chris and Clare have lived there for the past seven years, originally with Chris' coursemate; Ella is the fourth person they have shared with, they previously shared with John and his partner. People typically stay for two years at a time. When Ella moves out shortly, Chris and Claire will live there by themselves. Both Chris and Claire were joint respondents.

Home C

Matthew (male, 33 years old) lives in a ground-floor two-bedroom flat in South Coventry (IMD of 8), in moved in during the pandemic a year ago and in recent weeks has started a new full-time permanent contract in the computer games industry. Previous, to this Matthew had a fixed-term job in the cultural sector and lived with his parents for a year during that time.

Home D

Robert (male, 28 years old) and Owen (male, 26 years) are housemates and live in a top-floor two-bedroom flat in an apartment block in Benton Park, Newcastle upon Tyne (IMD of 10). They have lived together in the flat for the past four years. Both Robert and Owen have permanent full-time jobs in the software industry. Robert was the primary respondent.

Home E

Anika (female, 29 years old) and Daniel (male, 36 years old) are partners and live in a semidetached house small village eight miles north of Bristol (IMD of 5). They relocated here a year ago, moving from the north of England during the pandemic in 2020. Previously they lived in a house that Daniel owned. Anika is a contractor for a small design agency four days a week, working at home, and Daniel has a permanent full-time contract working in an office in Bristol. Anika was the primary respondent.

Home G

Peter (male, 45 years old) and Rachel (female, 29 years old) are partners and live with their son Oliver (male, 2 years old) in a two-floor garden flat in St Johns Wood, North West London (IMD of 6). They have lived here for the past six months, having moved during the pandemic. Peter heads account management for a city-based business software company – with a full-time permanent contract. Rachel did not give details of her employment. Peter was the primary respondent.

While these households represent a range of experiences, particularly in the relationships between occupants and some geographic diversity, a small study with a few people like this will inevitably be able to speak only to a limited set of the domestic struggles that I identified in Chapter Two. Notably absent are those experiencing unemployment, disability, larger households (especially those including young adults), elderly and older adults, and those engaging in religious practice.

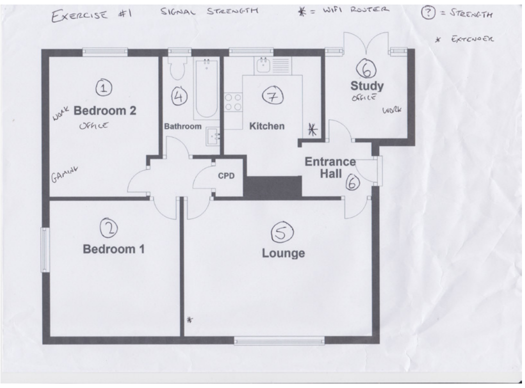
Thematic Findings

After typically one week participants returned the probe package to me in the post, having completed the exercises in the booklet to their satisfaction and having experienced the meters. Shortly afterwards each household participated in an online Zoom interview, which typically lasted for 50 minutes (none were longer than an hour) and was structured around the returns. All participants agreed to be audio recorded and I transcribed each interview (with the aid of speech recognition software). By considering the totality of material, over a period of weeks, I found one theme for each home which I considered seemed to be particularly resonant or dissonant with the other homes . This allowed me to ask, *so why is this home interesting?* This ensured that each unique home contributed to my findings, rather than a few enthusiastic respondents dominating my thinking. As I incrementally added themes, I reconsidered existing ones and modified my choices in response to my interest in domestic struggles and the materiality/immateriality of the home network. The six resulting themes are introduced here taking each home in turn and then drawing on material from across all the homes. Through this analysis, this section offers a thematically structured account of the domestication of the Internet and the home networks in six rented homes in 2021. Stood alone these thick descriptions are intended to offer a reader with designerly intentions some inspiration, beyond that they directly inform the theory developed over the subsequent chapters: the Stuff of Home model proposed in Chapter Seven and the articulation of a pattern language for a network of one's own in Chapter Eight.

Struggling with WiFi (Home A)

The meters and the exercises directed participants to explore their home networks, specifically how their WiFi was immaterially shaped by their material home; and this is to be seen in all the returns and the interviews, not least in Home A. Like many participants Steve and Helen had worked from home during the UK pandemic lockdowns of 2020 and

2021, and their home and the network had been necessarily recast as working spaces in which they evidently *struggled to be productive*. Their “sunroom” (a study with doors onto a small balcony) was made into an office for Helen and their second bedroom into an office for Steve. While Helen’s office was close to the router and was well served by WiFi, Steve’s room was not. He produced a map and annotated it using the Signal Strength Meter to show this arrangement – see Figure 53. The WiFi router is positioned in the kitchen (marked by a star), and attached to the only telephone socket in the flat (see Figure 54). With the map as a reference, Steve could speculate in material terms about the poor signal in the office (Bedroom 2), “*I suppose it does go through more walls to get to the bedroom. And it goes through like tiled walls, maybe. There’s like a big fridge here, which probably messing with it a bit. I don’t know. But if you look, it’s still has to go through the boiler though to get over there.*”



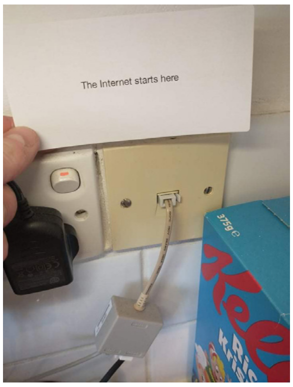
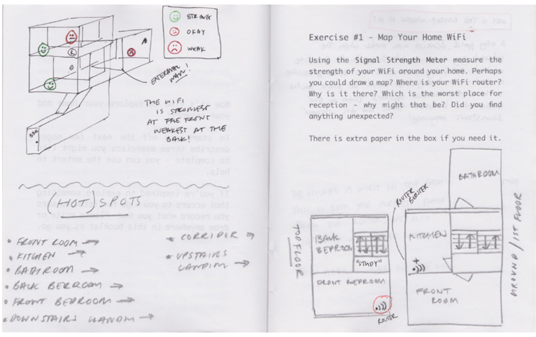


Figure 53. Layout in Home A.

© Anonymous. Used with permission.

Figure 54. Kitchen phone socket in Home A.

© Anonymous. Used with permission.


Exercise #1 - Map Your Home WiFi

Using the Signal Strength Meter measure the strength of your WiFi around your home. Perhaps you could draw a map? Where is your WiFi router? Why is it there? Which is the worst place for reception - why might that be? Did you find anything unexpected?

There is extra paper in the box if you need it.

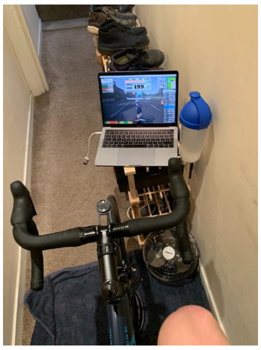


Figure 55. Layout in Home B.

© Anonymous. Used with permission.

Figure 56. Zwift racing in Home B.

© Anonymous. Used with permission.

Similarly in Home B, Chris, Claire and their housemates had to accommodate new working practices at home during the pandemic. Claire worked from a desk in their bedroom, their housemate John and his partner worked from their bedroom; while Chris occupied a space on the landing (marked as “study” in Figure 55). This reuse of space was accomplished by installing a desk and running an electrical extension lead down the stairs. Beyond workspaces, from Chris and Claire's perspective, the network had not presented many difficulties during the lockdowns. Yet the placement of the router in their bedroom had been a decision they had taken at the time of its installation some years previously and does create some disparity between the front and the back of the house; their housemates' Ella's room being at the back. Chris wrote in the booklet, "*A very quick decision was made when the Internet guy came to fit the WiFi. At the time we had our living room where the back bedroom is now – we thought it would be more useful to have the router upstairs than [keep it] in our housemate's bedroom.*"

In Home A it was clear that Steve's use of the network for work was not his priority, "*I care more about if my internet's any good when I play games than when I worked, to be honest. Because at work, like it's good enough. It's not so bad that I can't do my job.*" Although he later clarified that he would regularly use 4G for work Zoom video calls when he had troubles with the WiFi. He continued, *"Whereas sometimes when I'm playing games, I have to stop because I just can't even run."* Steve has a PlayStation 4 (PS4) on which he plays Call of Duty (CoD), the popular online first-person shooter video game. The PS4 is also sited in the second bedroom/office and uses the WiFi network, which not only creates challenges for gameplay, but also for the regular game updates. These updates are often of many gigabytes in size and can "*take like 14 hours*" for Steve to download – during which time the game cannot be played.

The demands of online gaming on the network were echoed by other households. Owen in Home D also played the CoD game and his housemate Robert commented, "*Everybody wants the cutting edge – you don't want to be lagging out and then die because of your network. You want it to be because you're not good at the game!*" Similarly, Chris in Home B competes in online Zwift cycling races where his performance on an indoor bike controls the game[81]. He commented, "*I've done races where [the network's] glitched and basically, then you're lost, you're completely out of the race.*" These real-time online games engage players intimately with the performance of their networks. The physical exertion required by Zwift necessitates a space that will accommodate the use of a fan and a towel on the floor, as well as a laptop and network connectivity – see Figure 56. By way of a network extender Chris had previously used the bathroom, but now uses the hall space at the bottom of the stairs (see Figure 55). Chris was adept at finding uses for unusual spaces.

[81] Zwift is a curious example of hard visible work being put into the Cloud.

Home B engaged easily with the signal strength meter, but as Chris said, "*[It] was kind of interesting, but confirmed a kind of like inner feeling of knowing where the hotspots were anyway.*" A sentiment shared by many of the respondents. Many spoke of where they knew they could and could not stream YouTube videos on their phones. However, Claire's perception was changed by her experience with the meter, having previously *"had some hope that I might get signal [in the bathroom]*".

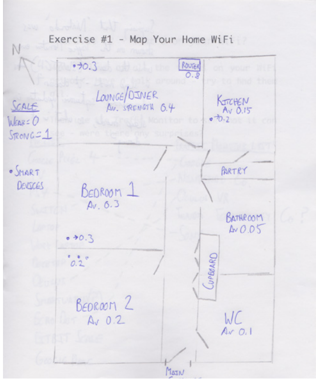


Figure 57. Layout in Home C.

© Anonymous.

Used with permission.

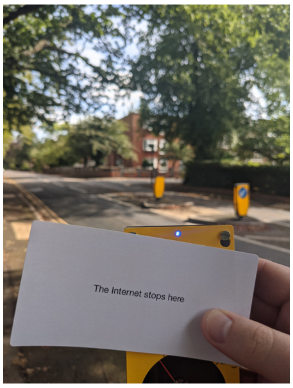


Figure 58. The Internet stops here. Home C is in the distance.

© Anonymous. Used with permission.

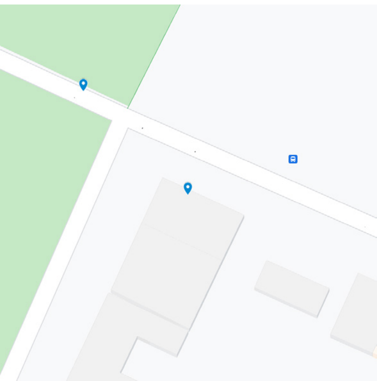


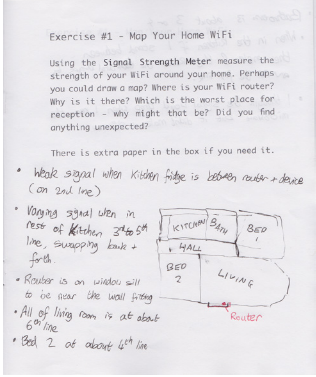
Figure 59. Google Map of Home C [details removed for anonymity].

© Anonymous. Used with permission.

Similarly, in Home C Matthew produced a map using the signal strength meter (see Figure 57) that confirmed his bathroom had the weakest signal. However, he also knew that when waiting for the bus across the street he would be able to connect to his home WiFi; this prompted an outdoor exploration for the provocation *The Internet Stops Here* (see Figure 58). Matthew created a Google Map to visualise these locations (see Figure 59), showing the position of his router in the centre, with the location of Figure 58 to the left and the bus stop to the right. This prompted the realisation that "*I get WiFi whilst I'm waiting for my bus, which also means when buses go past, that's also kind of picking up my router as well.*" Matthew was aware of how his home and its network were ill-fitting and somewhat public.

In Home A, despite Steve's problems with gaming he had not been motivated to reconfigure the network. He said, "*I didn't realise how much I hate my internet until I did this [study], but I haven't gone so far to do anything about it. I do have like a 30 or 35 foot Ethernet cable in the garage that dad made for me in the first year [of university]. But I don't want a big ugly grey cable drooped across my house like and as I said I don't really feel comfortable drilling holes and running it neatly somewhere like through the walls or whatever.*" The couple had installed a WiFi extender but this could only be conveniently sited in the corner of the lounge, where electricity sockets were available (see Figure 53 – marked by a star). Steve said, "*I don't use the extender. I don't think I don't think it does anything, Helen is convinced it does, but we don't know. I don't think it's any faster, it's just a range thing. So even though that signal is weak here, I'm still in range. And if I connect to that, it doesn't make it any better. And if I connect to that, and try and play games, it's really bad. Which I think might because that's talking to that.*" While Steve had a plausible hypothesis, he had a good deal of uncertainty and struggled to articulate how his experience of the Internet might be improved and at what cost.

Both Home A and B had tried "cheap" WiFi extender sockets, with Home B seemly having more success. Matthew in Home C used powerline networking sockets that extend the network over the home's mains electrical wiring. He commented, "*I don't even know how home plugs work, I know it's about wiring. I've also been told the wiring in this building is very bad. And I noticed that because the actual difference between upload, there's quite a big difference, but for download speed, that's very minimal difference between being on a home plug or just on WiFi.*" Home D experienced few network problems having recently invested in "*a pretty good router [in] not a huge flat*". While Robert's response to the *Immovable* provocation was a photograph of the BT Openreach socket, this was conveniently situated in the living room (see Figure 60) with the router on the windowsill, adjacent to Robert's desk, the television and PlayStation. The PlayStation was attached to the router via a short Ethernet cable running along the wall to improve their gaming experience.



Exercise #1 - Map Your Home WiFi

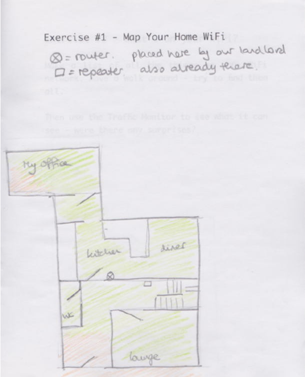
Using the **Signal Strength Meter** measure the strength of your WiFi around your home. Perhaps you could draw a map? Where is your WiFi router? Why is it there? Which is the worst place for reception - why might that be? Did you find anything unexpected?

There is extra paper in the box if you need it.

- Weak signal when Kitchen fridge is between router + device (on 2nd line)
- Varying signal when in rest of ~~K~~itchen 3rd to 5th line, swapping back + forth.
- Router is on window sill to be near the wall fitting
- All of living room is at about 6th line
- Bed 2 at about 4th line

Figure 60. Layout in Home D.

© Anonymous. Used with permission.



Exercise #1 - Map Your Home WiFi

⊗ = router. placed here by our landlord

□ = repeater also already there.

Figure 61. Layout in Home E. Good WiFi reception is shaded green, poorer reception in red.

© Anonymous. Used with permission.

In Home E Anika and Daniel were letting a house their landlord had previously occupied and where the router and a WiFi repeater had already been installed – see Figure 61. The position of the router in this home was notable in that it was relatively central and not on the periphery like most others. While this provides most of the house with a good signal, there is no office or living room at its centre to exploit the best performance, unlike say in Home D. Anika had attempted to install an extender in her office, which she conceptualised as a "*sort of fuel pot so we can use the Internet*", to alleviate a corner of relatively poor reception, "*but it actually makes things worse*". The study's request that Anika reconfigured the router and turned off the 5GHz network revealed that the administrative password was known only to the landlord, who had been previously occupied the house and had installed the router. This did not impact the performance of the Signal Strength Meter, but the Device Wheel and Traffic Monitor saw fewer devices than might otherwise have been expected.

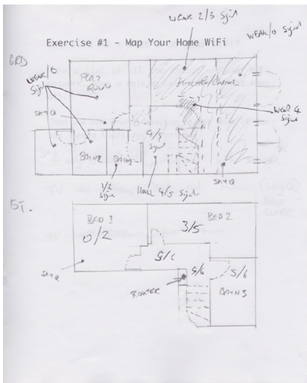


Figure 62. Layout in Home G.

© Anonymous. Used with permission.

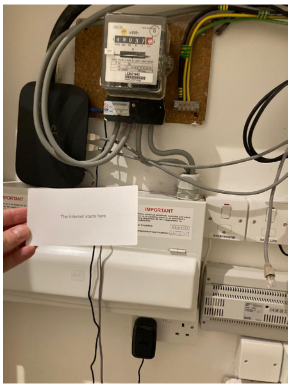


Figure 63. The Internet Starts Here. The service cupboard in Home G.

© Anonymous. Used with permission.

In Home G the readings of the signal strength meter did not portray Peter and Rachel's experience of their home network (Figure 62). They use a system called Sky Q to provide satellite television and WiFi Internet access to the rooms via Sky Q mini boxes; these three boxes connect to the router in the service cupboard (Figure 63), two by Ethernet cabling and one by WiFi. Every room, in this rented home, has Ethernet and satellite sockets installed in the walls. The Sky Q mini boxes are configured to advertise a different WiFi network name (SSID) than the router and the consequence is that the signal strength meter shows the strength of this router and not the Sky Q system. Similarly, the device wheel and traffic monitor assumed a single access point with a fixed MAC address and so were also unable to see any activity on this network. While the meters did not then reveal much of the network in use, something of the network was brought into focus by the failure of the meters and this structured our conversations revealing this network topology.

All the homes primarily used WiFi to connect their devices to the network and in each there was an identifiable router that defined the private network and was the home's primary point of connection with the public Internet. As described, several homes indicated a secondary use of 3G or 4G via smartphones. Every home then had some struggle with WiFi and each attempted some technical intervention to improve and reshape their network, to better fit the network signal within the walls for their work and play – made newly essential during pandemic lockdowns. While the Signal Strength Meter (in combination with a map) allowed some new reasoning about the immaterial network, like Chris, most participants felt the meter expressed some *“inner feeling of knowing where the hotspots were anyway*”. None of the participants reported any new tactical insights generated by the meters.

Struggling to Live with Others (Home B)

In Home B there was a recurring theme about ways of sharing. Chris and Claire have been tenants in the same flat for the past seven years and in that time they have shared with four other people, first with classmates and latterly with people they didn’t previously know. This has granted the couple a trusted status with their landlord which affords them some agency and the ability to enrol new housemates into their home. After Ella leaves shortly, they have decided to be the sole tenants. While the challenges of sharing seem most in focus in Home B, all the participants in this study demonstrate ways this is negotiated in rented homes. Homes A, E and G are centred around long-term intimate partnerships, Home D is a long-term friendship pairing, and Home C is an individual.

As previously discussed, the position of the router in Home B did create some disparities between the rooms occupied by Chris and Claire, and those of their housemates; although seemingly not to the problematic extent experienced by Steve. However, some further deliberation was revealed in Home B by the *Traffic Conditions* exercise in the booklet. This suggested that participants use the Traffic Monitor to “*see how quiet you can make your network*” and Chris said, “*If it was just the two of us, we would have been able to go around and turn things off and we could have basically turn the router off. I mean, even when turning the router off to change it from 5GHz, I made sure Ella was out.*” The temporary disappearance of the network was clearly consequential and to be avoided.

While the network did create some sharing dilemmas in Home B, this was much more explicit in their joint use of electricity. Chris said, “*This, again, comes back to living over the years with so many different people. The person who’s moved out has always been the person in charge of the electric. Not paying it, but organising it. And so we’re actually on pre-pay, like a top-up thing, a key that you plug in. And that has had like a number of cons. And we probably pay more for the electricity than we should do per kilowatt-hour, but as a result of it being such a kind of tangible and visible thing, knowing exactly how* *much electricity we use people are much better about it, apart from Ella. Much better at like turning lights off.*" The task of collecting money and taking the physical key to be topped-up at a local corner shop makes their use of electricity consequential for all the housemates, in a way that a direct debit would not. The frequency of this group activity makes periods of an individual's higher joint use apparent to all. This work does not reveal the reality of this utility in any partial way, by making its generation and distribution visible, but it does create an analogue that has a real cost to the occupants of Home B.

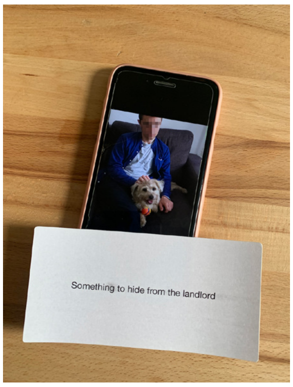


Figure 64. Something to hide from the landlord in Home B [face blurred for anonymity].

© Anonymous. Used with permission.

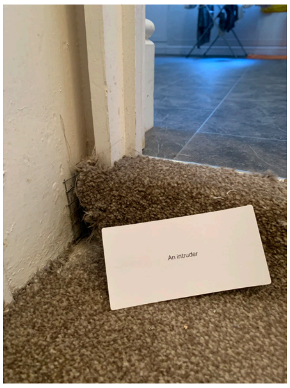


Figure 65. Intruders in Home B.

© Anonymous. Used with permission.

Several respondents mentioned the negotiation of sound in the home, especially when one person is working. Robert and Owen in Home D, own wireless noise-cancelling headphones, "*the quite expensive ones*", which were originally bought for open plan office work, but are now regularly used at home. Perhaps surprisingly nobody mentioned troubles with their *noisy neighbours*, although in retrospect perhaps only a few Provocation Cards might be interpreted in this way, and I did not pursue it in the interviews.

The final way Home B shared their home was more surprising, not with humans but with animals – both with pests and with pets. On several occasions during their tenancy rats have found their way from the alleyway behind the shops and into the flat through holes in the skirting board. Chris and Claire told several stories of finding rats in the kitchen and becoming aware of them under the floors, which necessitated the use of traps and visits from pest control services. Previous tenants had attempted to make a material adaption to the home, blocking the holes with meshing, as disclosed in the photograph taken for the prompt "*An intruder*" (Figure 65). More pleasantly, Claire's father's dog is a regular welcome visitor to the home but is "*Something to hide from the landlord*" (see Figure 64). None of the respondents disclosed they had pets living with them, some tenancy agreements prohibited it, but for others it was a choice.

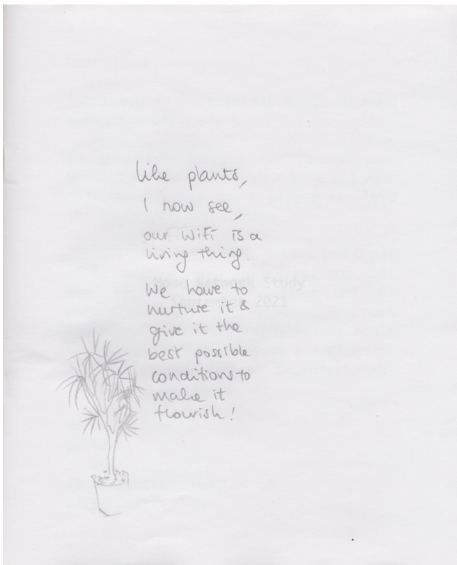
In Home E, Anika said, "*I have plants because I can't have pets. And it's not because I'm allergic. It's just because my partner doesn't [want them]. So, I do I really cherished the plants as sort of like a living thing in the house.*" The next theme will describe some parallels Anika found between caring for plants and caring for the network.

Network Mindfulness (Home C)

In Home C, Matthew's most intriguing comment came from his reflection on the experience of participating in the study and his use of the traffic monitor in particular, he said, "*I found it really interesting. I really enjoyed it. There's almost something mindful about how like thinking about your home WiFi like this. Taking the time to think about it, I found it quite relaxing, in a weird way. And it made me think more about the fact that that stuff's always going on, even when I sleep and there's no WiFi being used anywhere across the house. Yet, my smart speakers are still connected to it, my phone is still connected to it, my Nintendo Switch is apparently still connected to it! And yeah, it was just it was quite interesting to think about that. Because it again, it's something that you only think about when it's not working, and it's kind of working all the time.*" I suggested that an alternative reaction might be to be overwhelmed by the volume of WiFi data. Matthew responded, *"My perspective on that is that it's there is so much WiFi, but we were never going to escape so much WiFi. So, for me, using what feels like analogue devices to kind of see that and kind of visualise that in some way. There was something quite calming about that, I think.*" While I had designed the meters to be instrumental, Matthew saw a way that they might be everyday objects playing a part in a mindfulness practice.

In recent years mindfulness has gained popularity as a positive mental health practice, in which one is fully present in the moment, knowing one's thoughts, feelings and sensations, but not unduly reactive or overwhelmed by them. The concept of mindfulness was developed in the late 1970s and has its roots in ancient Buddhist meditation techniques (Henley, 2014). As Matthew frames it, mindfulness becomes a strategy for dealing with technical complexity, not by hiding or ignoring it, but by making it visible and gazing at it. This contributes then to my discussion of the visibility of work begun in Chapter Three.

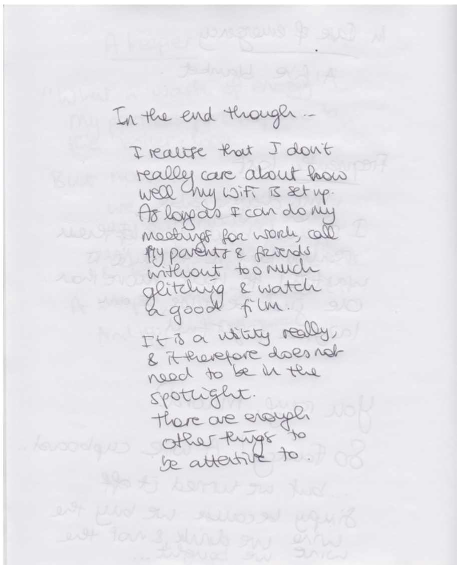
In Home E, Anika's comments about the nature of WiFi have some resonance with mindfulness and attention. After a few days of her engagement with the probes Anika wrote in the booklet (Figure 66) and then again at the end (Figure 67); in the first, she likens WiFi to a living thing (specifically to plants) to be nurtured (and to be attended to) in order that it might flourish, but in the end, she considered it a utility that need not be in the spotlight, saying in the interview that, "*I started thinking about the extenders* *fuelling the Internet to go across the house, and all the different devices that are on there. I was taking care of the meters by turning them on and off at night, then I realised, actually, I don't gain the same thing from the Internet as an emotional connection as I do from plants.*" Sadly, our interview did not pursue the question of how this caregiving differs between the Internet and plants, but in light of the first theme's struggle with WiFi (and in particular with people's puzzling experiences with extenders), it seems reasonable to suggest that the health or flourishment of WiFi is too inscrutable to reward such attention and attempts to care for it. Maintenance is the fifth theme and some of these questions are revisited there.



like plants,
I now see,
our WiFi is a
living thing.
We have to
nurture it &
give it the
best possible
conditions to
make it
flourish!

Figure 66. WiFi is a living thing, Home E.

© Anonymous. Used with permission.



In the end though...
I realise that I don't
really care about how
well my WiFi is set up.
As long as I can do my
meetings for work, call
my parents & friends
without too much
glitching & watch
a good film.
It is a utility really,
& it therefore does not
need to be in the
spotlight.
there are enough
other things to
be attentive to.

Figure 67. WiFi is a utility, Home E.

© Anonymous. Used with permission.

Automation (Home D)

In Home D, Robert was the only respondent to reflect on the possibilities of a smart home, "*My boss is really into it. He has like detectors on his windows and things. So, if they move too much, he's aware of it. And it's all these sorts of things throughout the house. It's kind of interesting, but I don't know how far I'd go.*" However, he had started to "*tinker*" with some home automation, "*This is ridiculous. But I had my fan there. And then I had a smart plug. And then when it was getting too hot, I could yell at [the Amazon Echo] to turn on. Which is great. But my smart plug broke. So, I've been having to get up [to turn it on]!*" See Figure 68 and Figure 69. Despite Robert's technical literacy, the system was fragile and the trouble with the smart plug remained undiagnosed, "*It just didn't seem to connect to anything. I don't know if it's a fuse or something, but I don't think it has a fuse. I'm not sure. I have to open it up, but I don't know how easy that is. It was kind of annoying because only lasted like a year.*"

Robert had speculated about what else could be automated, including his sound system, but hadn't "*figured that out*"; its configuration (volume, audio source, etc) could not be simply switched on and off like the fan. He had recognised that his use of the smart plug required a particular distribution of intelligence. He commented, "*You need a really stupid device for the plugs. Something I can leave it turned on on the thing, but then I turn on and off on the mains and goes on and off. And that was the hard part of it.*" Robert's approach to automation was reminiscent of the Goldberg Machines in Chapter Three, where simple actions are initiated by simple triggers.

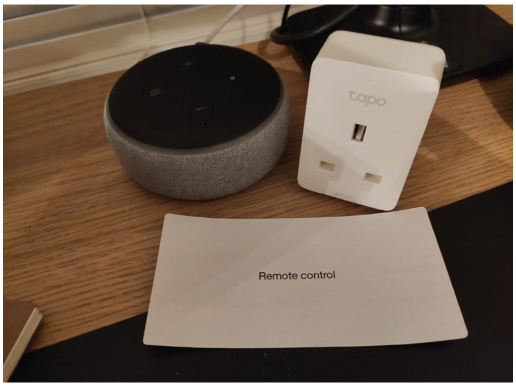


Figure 68. Remote control, in Home D.

© Anonymous. Used with permission.

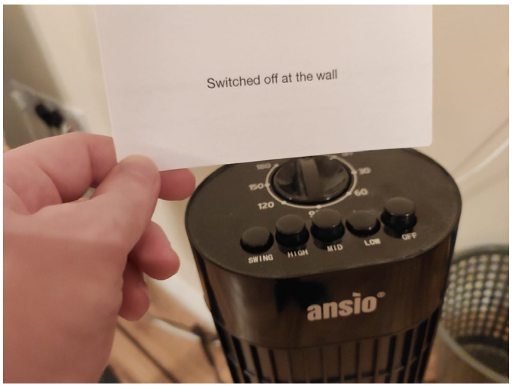


Figure 69. Switched off at the wall, in Home D.

© Anonymous. Used with permission.

In Home B, Chris and Claire also used automated sockets to control fans and heaters, "*so the fan doesn't go all night it turns off at like 3am.*" Their sockets are not network connected but are mechanical timers. The photographic response to the "oldest working appliance" card, see Figure 70, shows a set of four that were stored with the main fuse box. The interface for these timers allows the socket to be turned on or off in intervals of 15 minutes on a daily cycle, see Figure 71. However, they had originally been bought for another purpose. "*Those are actually from a previous house that we had with Euan, and we all went home for Christmas. And we all got really freaked out about getting burgled. So we basically sequenced the house to be a kind of choreography with sound and light. There was a radio that came on at a certain time and then there was lights front and back, at different times.*" Like Robert's automations, these were all devices with actions that could be initiated simply by switching them on.

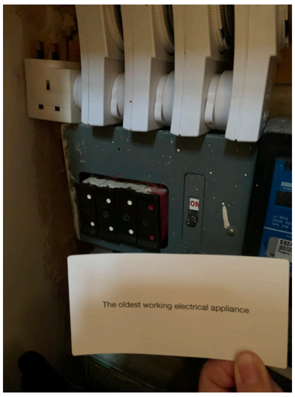


Figure 70. The oldest working appliance and stored mechanical timers, in Home B. © Anonymous. Used with permission.

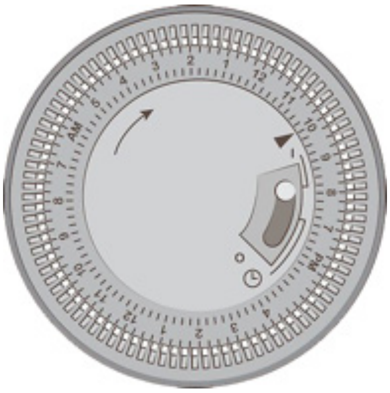


Figure 71. Mechanical timer switch interface. © wikiHow. Used with permission.

When asked if they had considered using WiFi sockets instead, Chris responded that he hadn't and referred to his "*old trusty*" mechanical switches – in marked contrast to Robert's experience with his broken smart plug.

Maintenance (Home E)

In Home E Anika was able to provide a perspective of experiences renting in the UK and in the Netherlands and this seemed most pertinent when discussing matters of maintenance. "*In the Netherlands your contract as a tenant is to protect the tenant. Whereas in the UK, it's to protect the landlord. So you feel like you're in a space where you don't belong. We rented a previous place and we had no curtains. And we weren't allowed to drill holes, I understand that it's because it wasn't a solid wall. But we had to pay 80 quid to have the landlady to come by and drill three holes in our wall so that we could hang the curtains. So, we didn't do that, we ended up hanging thin scarfs as we were allowed to put needles in the wallpaper. I then just put a lot of needles into it, but actually you ruin the wallpaper that way. And it's just like, why do I pay to live here? Why don't I have some rights in what I want with it? Those frustrations were a lot stronger in the UK, for me as a tenant compared to the being in the Netherlands, where I could just paint the walls or whatever, as long as I delivered back as a white box so someone else could make it their home again.*" Anika and Daniel's relationship with their current landlord is much improved, "*We were very lucky that we found this place that we are not going through an estate agent, we're renting directly off him. And it's just we understand that we both want the best for the house. And that he knows that it's us living in here now and not him. So yes, we won't replace the roof. We won't slam through a wall but if there's something broken, we'll fix it and we'll fix it our way.*" While Anika and Daniel's current arrangement with their new landlord granted them some opportunities to make physical change, Steve in Home A didn't "*really feel comfortable drilling holes*", as he considered ways to fix his network. There can be some latitude beyond the letter of the letting agreement depending on the relationship with the landlord.

All the homes in the study primarily used WiFi and while the wireless infrastructure generally afforded the renters a good deal of autonomy to install a network in a space they didn't own, it was hard for them to gauge the payoff of their maintenance work, or to speculate about future changes. As my account of the first theme described, every home had made some additional use of extenders, cabling or mesh networking but the success of these DIY attempts was invariably ambiguous. In attempting to articulate their network's performance both Steve in Home A and Matthew in Home B mentioned their broadband speeds, which they measured using online speed test tools. These tools suggest a simple pipeline model of the Internet where there are just two ends and some fixed physical infrastructure in-between, not unlike the telephone. Speed is measured by uploading and downloading a known amount of test data to and from some server on the Internet to some device on the home network over a short period, as such it is impossible to attribute this measure to any particular element of the dynamic network in-between – be that inside or outside the home. The WiFi meters were focused inside the home, but none explicitly measured data throughput and so would be unable to disclose a problem such as interference from a neighbour's router. While WiFi home networks can be installed regardless of the ownership of space, wireless networks are substantially more dynamic and environmentally situated, and so more inscrutable, than their wired counterparts. Wireless networking intrinsically complicates the maintenance of home networks.

Luxury (Home G)

The final theme of luxury is somewhat unexpected but is evident in Home G, quite an exceptional high-end rented home. Peter recognised this saying, "*I think there's an expectation in the market and the quality of stuff that should be installed.*" The flat had been completely redecorated before they had recently moved in, all the appliances were new, and the rooms were each installed with Ethernet cabling and satellite television. This was evidently the norm for properties in this high-end market. This is very different to the gradual pace of change witnessed in most other homes. The new cooker was particularly of interest and evidently amused Peter. For the prompt *The Internet stops here* he photographed his WiFi integrated cooker displaying the configuration screen for the network (see Figure 72), "*Why would you want your cooker connected to the WiFi? I've no idea, I've never got it connected up.*" he added. Luxury products like this communicate their aspirational qualities through features like Internet connectivity.

In Home E, Anika experienced a little second-hand, but ultimately unwanted luxury. In response to the *You rang m'lord?* Card, she photographed the wine cooler unit (see Figure 73). She explained, "*The landlord was living in this house, so it's not commercial venue to him. All of this stuff he has put in the house because he wanted it and it is so fancy. Like, all we've got a wine cupboard! How cool is that? But when we actually moved in, we said we've just got like turn this off! It's just going to consume energy!*" – "*I feel like we're being out poshed by the space we live in!*" Indeed, to Anika some of these unwanted luxuries became burdensome and this extended beyond the furniture and fittings to the floor plan, "*I've already said to my partner, you can't use the third bathroom! We only use it when there's guests, I'm not going to clean them all of the time. That's it like we use the bath in that bathroom, but we only use one of the two showers because it's just these luxuries that they are a burden if you don't have a servant, it's just a burden!*"

Both Homes E and G were substantially furnished by the landlord and to a high quality; including appliances like cookers, washing machines and refrigerators. While my own rented home is unfurnished (except for the cooker), most other homes were furnished to some degree. As Steve in Home A put it, "*The white goods and the big stuff are the landlord's, but lots of like the tables and smaller stuff is ours.*" While this offers an obvious convenience, when the quality is poor or it is not properly maintained, the tenant is not able to act unilaterally when they become broken or unwanted. As Robert indicated in Home D with the washing machine this can result in protracted negotiation (see Figure 74).

.

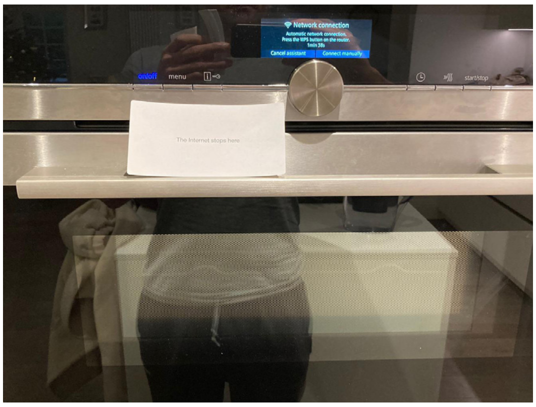


Figure 72. WiFi Cooker - The Internet stops here, in Home G. © Anonymous. Used with permission.

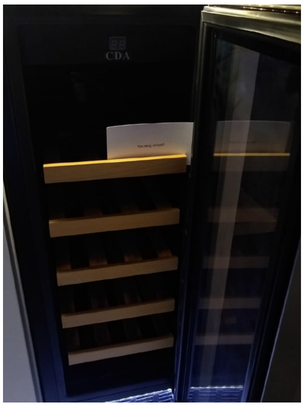


Figure 73. Wine Cooler- You rang m'lord?, in Home E. © Anonymous. Used with permission.

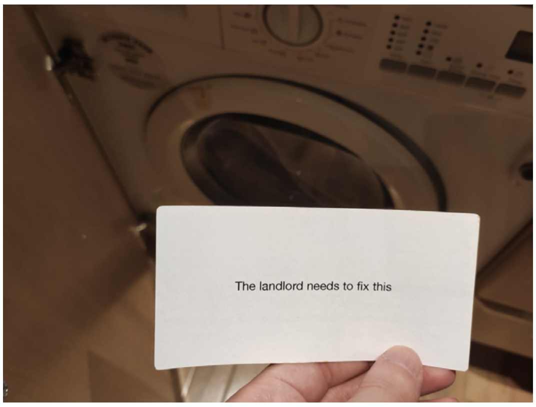


Figure 74. Broken Washing Machine - The landlord needs to fix this, in Home D.
© Anonymous. Used with permission.

Discussion

This section has two parts: a discussion of the themes of the domestication of the Internet and a discussion of the probe design that made these disclosures. The rich anecdotal thematic accounts offered previously are intended to stand alone and inspire future design work and while some extra contextualisation with relevant citations is offered here, this section's principal intention is to articulate forward connections to the Stuff of Home model proposed in Chapter Seven and to the articulation of a language for a network of one's own developed in Chapter Eight through 30 related patterns (in the appendix), including some common patterns of network configuration. These themes arise from the design of this study and in particular the design of the probe package and WiFi meters; so secondly, some refection is also offered here on the success of this design.

Themes

The first theme, *Struggling with WiFi*, reflects the primary concern of this study, describing how wireless networking is experienced in work and play through its immaterial form and how this is shaped by the material home. This substantially informs the Stuff of Home model, which adapts Brand's Shearing Layers to describe the domestication of the Internet. This pulls focus on the dynamics of domestic change dictated by material ownership (and renting) and immaterial technologies. To these ends, the UK pandemic lockdowns of 2020 and 2021 necessarily required many of the homes to adapt as working spaces, as they struggled to be productive. This theme also allows some patterns to be identified for the articulation of a language for a network of one's own, including the *Shape of Space* (in architectural and Hertzian terms) and the *Home WiFi Router* (as the home's primary point of connection and boundary with the public Internet).

The second theme, *Struggling to Live with Others*, informs the Stuff of Home model and in particular, it readopts Brand's notion of the Souls layers – the humans, pets and pests in the home. In addition, the emerging notion that there can be visible analogues to invisible work also informs the *Visible Work* pattern.

The third theme, *Network Mindfulness* , also inspires patterns that demonstrate Visible Work. Mindfulness becomes a strategy for dealing with technical complexity, not by hiding or ignoring it, but by making it calmly visible. This echoes Mark Weiser's Ubiquitous Computing notion of Calm Technology (Weiser and Brown, 1995), where calmness is a matter of directed attention. Thus far the concept of mindfulness has been dealt with rather abstractly by HCI scholars: as a reaction to digital narcissism (Rogers, 2014), as a matter of techno-spiritualism (Akama and Light, 2015) and as a disruption to mindless automatic interactions (Cox et al., 2016). With this concern for reflective frictionful interactions, Anna Cox and colleagues do establish a connection with Slow Technology (Hallnäs and Redström, 2001), but curiously not with Seamful Design (Chalmers and MacColl, 2003). Instead, the Mindful Computing pattern commits to disclosing Visible Work not for simple pragmatic interactional reasons, but rather as an engagement in politics. In that light, there is a tension in how calmly that struggle should be rendered.

The fourth theme, *Automation* , suggests ways of automating simple devices with a variety of motivations (some for comfort, some for security and some ludic). These are reminiscent of the Goldberg Machines in Chapter Three and inspire patterns that demonstrate Visible Work and a consideration of where logic and control exist in the network, which is taken up by the Stuff of Home model.

The fifth theme, *Maintenance* , is a central concern of Brand's How Buildings Learn (Brand, 1995) and naturally contributes to the Stuff of Home model, especially as it relates to the freedoms of renters who do not own the home in which they live. This theme also inspires the patterns of Tenancy and Pliable Walls. The insight that while wireless networking allows any tenant to install a network, in their home, it also fundamentally impairs attempts to technically maintain that network. Previous work has presented such digital housekeeping with (predominantly) physical wired networks as a specialist but somewhat straightforward task (Tolmie et al., 2007). The account made by this theme suggests that the immaterial maintenance of wireless networks is altogether more complex as people struggle with an invisible system with only crude tools and conceptions of the network. This challenges Andy Crabtree and colleagues' contention that networking had become unremarkable, that, "*for most people the home network has ceased to be a technological object and has become a sociological object*" (Crabtree et al., 2012, p. 563).

The final theme, *Luxury* , as it is experienced in Home G, offers an alternative view of domestication and renting, where the home, its décor and services are reset and remodelled by the landlord before each tenant moves in, such that one might be considered to be living in a showroom in which everything is contemporary, expect the architectural structures. This challenges the incremental assumptions of the Shearing Layers and common expectations that rented properties will deteriorate over time in want of maintenance. The notion of a furnished home further restricts tenants to only their own stuff. This suggests a kind of home-as-a-service pattern which while doubtlessly convenient, seems to rob tenants of their agency to configure their homes or enact even basic maintenance. This theme then informs both the Stuff of Home model and the network of one's own patterns.

Probe Design

The success of the probe design should be judged by the richness and relevance of the visual and written materials returned and the scope of the interview conversation they framed. To those ends, this probe study was successful in generating a wealth of insights into both contemporary networked homes and some of the struggles that constitute homelife, particularly (but not exclusively) for renters. It is somewhat difficult to unpick exactly how the meters, provocation cards and booklet operated individually, but all evidently contributed to the themes I have presented. As technically mediated probes, indeed pragmatic instruments, the meters were designed to elicit moments of reflection and insight on the part of the participant. The signal strength meter was well understood and prompted a clear exploration of the home, even if as Chris in Home B said, "*[It] confirmed a kind of like inner feeling of knowing where the hotspots were anyway.*" The traffic monitor prompted perhaps the most interest and ultimately Matthew in Home C's reflection on network mindfulness and the device wheel was perhaps the least revealing and as Chris put it "*more abstract*" than the others. However, the meters did not seem adequate to explore some of the real questions that emerged about the day to day operation of networks in these homes as they looked out onto the Internet, particularly about the efficacy of wireless network extenders and possible sources of interference. This leads me to conclude that wireless networks are inherently more entangled with their (dynamic) environments than their wired equivalents. Further exploration of this towards demonstrating ways to further disclose what is still immaterial and invisible, suggests a utility in developing ecological accounts or analysis from an Actor-Network Theory perspective. While I consider that a new study design could respond directly to this challenge, the form exercises and design of any meters are not immediately obvious to me. This is somewhat consistent with Chetty's identification of the *network control problem* and observation that available visualisations are, "*woefully inadequate for dealing with many aspects of the 'seeing' that participants desired in order to make their home network work.*" (Chetty, Sung and Grinter, 2007).

Limitations

This study was broadly intended to deliver a defamiliarisation of the networked home; working with a small number of participants who share some experiences of rented homes, there are evidently limits on what can be claimed by this study. Chapter Two attempted to offer a broad contemporary picture of the ways in which home life is neither simple nor static, drawing on scholarship, journalism, and some autobiographic reflections to draw out a set of domestic struggles. This study trades that broadness for specificity. While the demographics of participants were far from homogenous, albeit deliberately geographically constrained, some more diversity would have been welcome. As previously stated, notably absences included those experiencing unemployment, disability, larger households (especially those including young adults), elderly and older adults, and those engaging in religious practice. As noted, nobody spoke about their neighbourly relationship or their neighbour's networks; also no one talked about or alluded to their use of the Internet to access pornography. Some of these observations suggest alternative strategies in future studies of home networks.

Conclusion

To offer some brief words of conclusion, this study contributes a contemporary account of the domesticated Internet and the home networks in some British rented homes. These are predominantly wireless WiFi networks and this study demonstrates some of the ways they shape and are shaped by ownership and agency. Specifically, how immaterial WiFi networks do not require the modification of the material fabric of the home, in ways renters are prohibited, but how wireless networks are inherently entangled with their environments and so resist simple maintenance, in ways wired networks do not. This complicates previous accounts of digital housekeeping and suggests that the home network is rightly considered a technological object. Beyond this, the six themes and associated rich anecdotal material deliver a defamiliarisation of the networked home that informs the Stuff of Home model proposed in Chapter Seven and the articulation of a network of one's own developed in Chapter Eight. This has been accomplished by cultural probe Research Through Design inquiry that includes the design of three WiFi meters, instruments that allow participants to reveal aspects of their networks that would otherwise be invisible.

Chapter Seven: The Stuff of Home

This chapter proposes The Stuff of Home, a new framework to generate ecological understandings of the domestication of home networks and to make accounts of modern homes in general. This framework adapts Stewart Brand's Shearing Layers model (Brand, 1995) which was introduced in Chapter Two as a way to see the domestication of new technologies. The Shearing Layers were also used in Chapter Five to pull focus on paces of change present in the home and to inform my Pace Layer Prototyping. The analysis of the Network Home Study in Chapter Six pointed to some opportunities to develop this framework to speak more directly to the domestication of networks and technologies. Here, as a response, I shall explicate The Stuff of Home, which foregrounds Stuff and questions how it is accommodated by the home. In doing so I also make some of my longstanding commitments to Brand's ideas clear and so open to scrutiny.

This chapter has five short sections, in the first I give a brief contextualising biography of Stewart Brand to frame my discussion of the Shearing Layers and more broadly to acknowledge the influence of this figure in my thesis and the evolution of computing. I then offer a reading of the Shearing Layers which emphasises the dynamism of the home and the material affordance of its layers to change. I reflect on how its specific construction of layers applies to network homes and in doing so I highlight some difficulties it has in respect of my empirical studies (especially the Network Home Study in Chapter Six), my design practice, and sources from the literature. In reaction, the third section offers a new extended eight-layer shearing framework for the home – The Stuff of Home. This delivers a new vocabulary through which to express both that seen in the Home Network Study from Chapter Six and the patterns for alternative designs next developed in Chapter Eight. The Stuff of Home is intended to be a public form, for the use of the design and HCI communities, as such it is designed with this audience in mind. Finally, I apply this framework by using it to explain how Silicon Valley's expectations of the home and the network, result in the dispossession of Stuff in favour of precarious cloud-based Services. I suggest some ways to struggle with this in the terms of the framework, specifically how Services can instead be replaced by Stuff. To conclude I reflect on how these new domestic dynamics create new opportunities and existential precarities.

A Short Biography of Stewart Brand

At times this thesis has very deliberately adopted a biographical tone with respect to some of the characters in the stories told to suggest a little of their motives and position, including my own. The biography of Stewart Brand (born 1938) contributes not only the Shearing Layers to this thesis, but also to ecological thinking in Chapter Three and to accounts of hacking in Chapter Four. Brand filmed and was a consultant for Douglas Engelbart's seminal NLS (oN-Line System) presentation at the 1968 Fall Joint Computer Conference that became known as *The Mother of All Demos* 1968; demonstrating the use of hypertext, email, video collaboration and the mouse (Engelbart and English, 1968). Again in 1968 Brand published the first edition of the Whole Earth Catalog; the magazine was later described by John Markoff, of the New York Times, as "*the internet before the internet.*" (Cadwalladr, 2013). In 1972 Brand wrote an article about the hackers at MIT and the Spacewar game (Brand, 1972) and he convened the first Hackers Conference in 1984 at which he is selectively quoted as saying "*information wants to be free*" (Brand, 1985) – see Chapter Four. In 1985 he cofounded the WELL (Whole Earth"Lectronic Link) with Larry Brilliant, a pioneering online community then based on dial-up bulletin board technology (Hafner, 1997). In 1986 he was the journalist in residence MIT Media Lab as the notion of multimedia took hold (Brand, 1987). In 1995 he proposed the Shearing Layers in his book and subsequent television series, How Buildings Learn, on which I shall focus in the chapter that follows (Brand, 1995; Muncie, 1997). By any account this is an extraordinary résumé of an unusually influential figure, and a story now told in the biographical film *We Are As Gods* (Sussberg and Alvarado, 2020) and Markoff's biography *Whole Earth* (Markoff, 2022).

> *When I was young, there was an amazing publication called The Whole Earth Catalog, which was one of the bibles of my generation. It was created by a fellow named Stewart Brand not far from here in Menlo Park, and he brought it to life with his poetic touch. This was in the late 1960s, before personal computers and desktop publishing, so it was all made with typewriters, scissors and Polaroid cameras. It was sort of like Google in paperback form, 35 years before Google came along: It was idealistic, and overflowing with neat tools and great notions.*
>
> *Steve Jobs, CEO of Apple Computer, Stanford University commencement address June 2005*

While the biography of one man is a narrow lens, it speaks directly of a small (and undeniably privileged) community of people who have had a disproportionate influence on the ways personal computing and online communities have unfolded over the past 50 years, by extension the domestication of the Internet. I want to suggest that seeing the Shearing Layers in the context of Stewart Brand's own story makes evident some of its unspoken commitments – namely to ecology and counterculturalism. In Chapter Three I suggested that the ecological perspective was itself a strategy for generating design alternatives – itself countercultural. That chapter also described how Brand, a trained ecologist, had petitioned NASA in 1966 to publish a photograph of the whole Earth; the subsequent Earthrise (1968) and Blue Marble (1972) images were widely credited for their role in establishing the popularity of the ecology movement in the 1970s (Ahmed, 2018). The counterculturalist Whole Earth Catalog is infused with ecological thinking; not least in its name, the use of the Earthrise cover photograph and articles documenting biological ecosystems. Brand's own commitment to counterculturalism is further evident through his involvement with commune living, and with the hackers and engineers of Silicon Valley. Central to this ecological philosophy was the idea of *self-organising networks* of individuals, able to find stability without hierarchical control – this idea shaped the architecture of the early Internet. And yet, as Adam Curtis argues, by the 1970s both the science of ecology and social endeavours like the short-lived American commune movement, cast doubt on the notion of stable self-organised ecosystems (Curtis, 2011b). Read in this context Brand's Shearing Layers are in inescapably an ecological account of the complex ecosystem of a building – reappraised from a 1990s perspective in which ecological precarity has become increasingly evident. Brand argues that the building (and by extension the home) has to be maintained to keep the encroaching wild by way of the elements at bay – a wildness that G.K. Chesterton suggests is also to be found within (Chesterton, 1912).

With Brand's focus on the building scale, his writing draws on the work of two architects: Frank Duffy (Duffy, 1990), from which he adapts the layers model, and Christopher Alexander (Alexander et al., 1977; Alexander, 1979), with which he discusses how buildings operate in time and how their design can be appraised by identifying their use of patterns. Both architects, in their holistic approaches to scale and pace, could also be considered ecologists and both have a commitment to a formalisation, or at least articulation, of the design process – which also clearly informs Brand's Shearing Layers. This concern with the identification of processes and frameworks for design informs much of the current HCI discourse with respect to design; to this end Chapter Eight will contribute a pattern language inspired understanding of the networked home.

While Brand was intimate with the potential of the Internet and personal computing, it is not writ large in the Shearing Layers in 1995; the pace of his concern had slowed such that by 1996 Brand had cofounded the Long Now Foundation with Brian Eno and set about designing the world's slowest computer – a clock to designed to tick for 10,000 years (Brand, 1999). Meanwhile, Brand's Silicon Valley community (not least Steve Jobs) were busy with a countercultural revolution of their own design – one reliant on short-lived homogenous products and experiences, consumed at a global scale. Despite Silicon Valley's countercultural roots, their subsequent domestication and socialisation of the Internet have taken a different ideological and less ecological path – exemplified by Zuboff's Surveillance Capitalism thesis (Zuboff, 2019). In seeking an alternative perspective and ultimately a path forward in the chapters that follow, there is an irony in once more turning back to Brand for inspiration and some need to maintain a critical distance.

A Critique of Brand's Shearing Layers

Stewart Brand's essential idea expressed in the Shearing Layers is that buildings (and systems) are in a constant state of struggle, demanding maintenance to learn and so survive. The notion of shearing clearly resonates with Mouffe's struggle or agonism, in which nothing is ever truly settled and which in turn informs DiSalvo's Adversarial Design (DiSalvo, 2012). From the perspective of the home and the design of domestic technologies, we can helpfully conclude that "*the home is never static*" (Rodden and Benford, 2003). The Shearing Layers seem to give rather a good high-level account of how real homes gradually accommodate infrastructural change, like electrification, and resist the imposition of the kind of show home futures (and their uncomplicated residents) described in Chapter Three. By contrast, Silverstone's Domestication Theory (Silverstone, Hirsch and Morley, 1992), describes individual technologies, but it does not draw particular attention to the home, its architecture or the ecology of technologies operating in time. Real homes are palimpsests, constantly being rewritten at multiple paces.

To consider the construction of Brand's shearing layers in relation to the home and highlight some specific difficulties it has with the networked home, let us reiterate the forms in which they offered: as a diagram (Figure 75), as a list (see below) and for television (Muncie, 1997, pt. 6); each invites some interpretation and creates different public engagements.

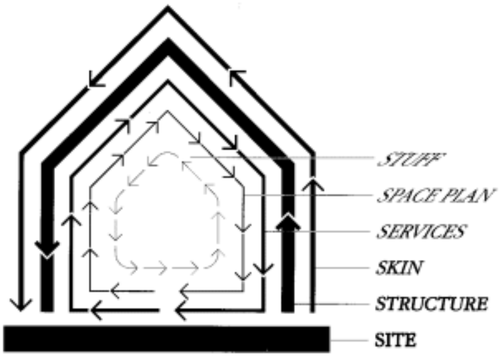


Figure 75. Shearing Layers Diagram. © Stewart Brand, 1995. Used with permission.

> ***Site*** *– This is the geographical setting, the urban location, and the legally defined lot, whose boundaries and context outlast generations of ephemeral buildings. "Site is eternal." Duffy agrees.*
>
> ***Structure*** *– The foundation and load-bearing elements are perilous and expensive to change, so people don't. These are the building. Structural life ranges from 30 to 300 years (but few buildings make it past 60, for other reasons).*
>
> ***Skin*** *– Exterior surfaces now change every 20 years or so, to keep up with fashion or technology, or for wholesale repair. Recent focus on energy costs has led to re-engineered Skins that are air-tight and better-insulated.*
>
> ***Services*** *– These are the working guts of a building: communications wiring, electrical wiring, plumbing, fire sprinkler systems, HVAC (heating, ventilating, and air conditioning), and moving parts like elevators and escalators. They wear out or obsolesce every 7 to 15 years. Many buildings are demolished early if their outdated systems are too deeply embedded to replace easily.*
>
> ***Space Plan*** *– The Interior layout—where walls, ceilings, floors, and doors go. Turbulent commercial space can change every 3 years or so; exceptionally quiet homes might wait 30 years.*
>
> ***Stuff*** *– Chairs, desks, phones, pictures; kitchen appliances, lamps, hairbrushes; all the things that twitch around daily to monthly. Furniture is called mobilia in Italian for good reason.*
>
> (Brand, 1995, p. 13)

A casual reading of the Shearing Layers diagram (Figure 75) might understand the model as simple static containment at ever-decreasing physical scales of simply delineated stable black boxes; the Internet is replete with reproductions of the diagram without the arrows (and so implied turbulence). Instead the diagram is designed to communicate the *shearing* forces and messy ongoing struggle between (and indeed within) the layers. The diagram perhaps misleading implies that only adjacent layers interact; whereas, for instance, a window (Structure) will more directly dictate the placement of chairs (Stuff). The question then is how these systems do not tear themselves apart. Brand's answer is that longevity depends on ongoing maintenance and this determines how the building learns and adapts. This is an inherently ecological account, where each layer has some shared material affordances to a fast or slow change – this was discussed at length in Chapter Three.

While Brand's Site, Structure and Skin are instrumental in shaping the activities of the home – they are of less immediate concern when designing for the home. Design research and commercial practice is instead often concerned with the inner three layers: Services, Space Plan and Stuff – the things that might change at the pace of a decade or faster. Indeed, Stuff tends to be a designer's focus. Surprisingly few have made use of the Shearing Layers as a lens for the home and computing from the perspective of HCI or design research. Rodden and Benford (Rodden and Benford, 2003) and Chetty et al (Chetty, Sung and Grinter, 2007) are the exceptions (see

Chapter Six). While Rodden and Benford's focus is on contextualising ubiquitous digital services, they do not consider the home network explicitly. Chetty et al are concerned with the network and its maintenance but as this work was done in 2007 many of the interviews relate to the physical challenges of Ethernet cabling and the little discussion of WiFi is limited to its then obvious insecurities. Neither trouble the Shearing Layer model in significant ways. While Desjardins does not identify the van conversion project as such, it presents an interesting challenge to this conception – a vehicle might change its Site on a daily basis, while its Structure and Skin remain relatively intransigent (Desjardins and Wakkary, 2016). Such homes have a quality of precarity – but while they are homes, they are not buildings.

Brand's Services as experienced by the home dweller are inaccessible and largely invisible, buried into the walls and under the floorboards; typically, those things considered to be utilities: electricity, gas, water and now the Internet. These utilities are standardized and reliable, delivered by external parties, and typically metered, through networks that connect homes to national infrastructures. Traditional fixed-line telephony fits the utility service model well – being charged by the minute, for a well-defined service, on infrastructure that is owned by the provider. However, utility services can sit rather uncomfortably with the Shearing Layers; at least in diagram form (Figure 75) the layers form a private containment of the home that excludes that beyond its walls. Brand's Services are perhaps better seen as a combination of service interfaces (light switches and fixed lamps, electrical sockets, wired telephone handsets, etc.) and the internal infrastructure (wiring, pipework, etc.) that resource them. This creates a rather insular view of services, which has trouble accounting with the global reach of the Internet. Wireless networking creates further challenges, being largely detached from the fabric of the home, no longer buried in its walls – yet the routers in the Network Home Study were often still tethered to the telephone socket in its original placement and this significantly shaped the availability and experience of the home WiFi network, through a material interaction with the building's slower layers. Furthermore, the precise service provided by the Internet is rather hard to define because it is experienced through a plethora of connected devices. All in all, the domestic wireless Internet troubles the Shearing Layers' account of Services.

Brand's Space Plan is also a little ambiguous in the domestic context, seeming to equate the potential to configure partitioning walls (likely stud walls), change the more permanent decorative fabrics of a room (like wallpaper) and nominate a room or space's function. As the Network Home Study witnessed these are rather different prospects, at least in British rented homes.

Brand conflates both small and large Stuff; "*all the things that twitch around*" and furniture. However, the Network Home Study showed that these can have rather different properties, where the larger furniture is owned and installed by the landlord and the tenant only owns the small Stuff. Even in owned homes, the larger furniture is less transient than the small. Where this Stuff is part of the Internet of Things and the logics of external agencies are embedded in and act through it, this picture is complicated further.

Maintenance is in many ways the central theme of Brand's How Building Learn thesis, of the book and television series (Brand, 1995; Muncie, 1997). This is echoed in the findings from the Network Home Study, which observes that while WiFi makes home networks possible in most circumstances, it also fundamentally complicates maintenance, preventing many from performing it in meaningful ways.

The Stuff of Home

In this section I present the Stuff of Home, an extended eight-layer shearing framework for modern homes that emphasises the fast and slow paces of change: Shell, Services, Space Plan, Scheme, Stuff, Software, Surfaces, Souls. These respond to the challenges of applying Brand's layers to modern networked homes that I identified in the previous section. This framework is named both to draw attention to the material/immaterial affordances of the home and to suggest the central role of Brand's Stuff, which tends to be a designer's focus – importantly it also acknowledges a new class of connected Stuff. I offer the Stuff of Home in the form of an alliterated list (see below) and diagram (Figure 76), in both the words and forms intentionally echo Brand's.

> ***Shell (Site, Structure, Skin)*** *– The geographical setting, the building and exterior surfaces of the home. The things that might change at the pace of a decade or slower and that are generally beyond the control of a resident who does not own their home.*
>
> ***Services*** *– What the home serves by an orchestration of external resources (water, gas, electricity, wired telephony, the Internet), internal infrastructure (plumbing, piping, heating, wiring) and service interfaces (taps, gas valves, radiators, mains electrical sockets and landline telephone/broadband sockets).*
>
> *While they are internally provisioned, they are typically externally resourced and so from residents' point of view they are both in the walls, accessible through the walls (maybe via a switch or a tap) and deliver resources from beyond the walls. A service's material infrastructure will likely be inaccessible to the resident for modification, indeed it may be prohibited by law without certification (e.g., gas pipes or electrical cables).*
>
> ***Space Plan*** *– The boundaries of rooms defined by the presence or absence of dividing walls, doors, fireplaces, mantelpieces etc. Ownership will dictate reconfiguration potentials. To some degree residents can freely nominate a room's function – depending on the availability of the services that function requires.*
>
> ***Scheme*** *– The fabric of the room, what might be broadly called interior decoration but is distinct from furniture (which is Stuff) – including: fitted carpets, wall decorations, paint, tiling and wallpaper. A renter's ability to manipulate the scheme will depend on the specifics of their tenancy agreement – in the most restrictive cases even the attachment of pictures to the wall is prohibited.*

***Stuff (with Stuffness)** – The chairs, desks, pictures; kitchen appliances, hairbrushes; all the things that twitch around daily to monthly to yearly. Much of this will be owned by residents, regardless of their tenancy, but not all. Some might be shared with others, rented (perhaps as a furnished apartment) or may simply have been abandoned by previous occupants. Some are connected electronic Stuff, dependent on external services, such as television sets, online game consoles and even the light bulb. Stuff is material, physical and visible.*

Stuffness is a way to describe the mobility and independence of all this Stuff. Stuffness is a product of physical properties (size, weight, material) as well as dependencies on higher layers of the framework, notably the availability of Services, which limit mobility. A large heavy table has less stuffness than a chair, a book has more stuffness than a cloud dependant eReader. Low stuffness is slower, it implies necessary participation in the ecosystem of the home and as such makes demands to be newly accommodated (and maintained). As new Stuff is domesticated and "made at home" there is a process of "becoming part of the furniture" or losing a degree of stuffness. Stuffness is then not solely determined by the physical properties of Stuff but instead a reflection of its evolving entanglement in the home.

***Software** – The embedded firmware code that runs on electronic Stuff and determines the behaviours that are not hardwired by electronic circuitry. A resident's ability to make changes to software will likely necessarily depend on some esoteric knowledge and the ability to make a hack. With Internet connected electronic Stuff, remote software routines can be entwined across the network – change might be initiated by a remote service provider with an "over-the-air" software update that reconfigures its behavioural logic, without the owner's explicit consent. Software is used inclusively to denote both the data and the program code that manipulates it – however, data is often easier to change than programs .*

***Surfaces + Volumes** – Fast changing surfaces may be rendered by electronic Stuff, often under the control of software, using a display technology like OLED or perhaps the mechanical hands of a wristwatch. For connected electronic Stuff this surface content may be resourced externally and be somewhat out of the control of the resident; television sets and radios being pre-Internet examples. Display technologies create surfaces, but audio and olfactory can also be seen in similar terms to create volumes in space. The projection of light, sound and smell can immaterially change the character of a room – re-rendering its Scheme. This enables residents to temporarily enact change on slower layers of the home, beyond a tenant's normal capacities. A WiFi router may also be seen to create a Hertzian volume in these terms – one that can be treated as if it were a Service.*

***Souls** – That in the home with its own agency and ability to rapidly manipulate Stuff. The residents, visitors, pets, pests and perhaps some autonomous Stuff, like robots. An adoption of Brand's own tentative suggestion, of souls being "servants to our Stuff"*

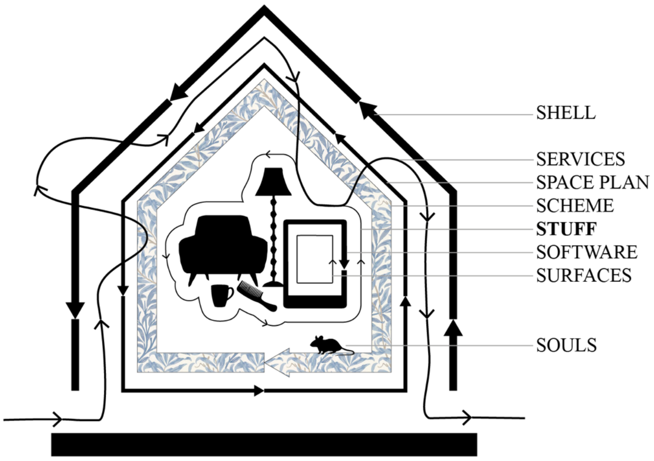


Figure 76. The Stuff of Home Diagram. © David Chatting.

These two forms of the framework emphasise different facets, the list communicates with more precision, but the diagram better captures the character of the layers and makes the centrally of Stuff obvious. The derivation of each layer deserves some brief words of explanation. Duffy's Shell is reintroduced as a useful shorthand for Brand's slowest layers: Site, Structure and Skin; which he had unpacked for his architectural purposes but are less available for our designerly intervention. Services are redefined to call attention to how they are externally resourced and that they are no longer fully contained by the walls. Service interfaces, like light switches, poke through to the room and they can radiate beyond the Shell, like a WiFi radio signal. Brand's Space Plan is split to introduce Scheme, which now describes the interior decoration of rooms. Stuff, now including connected electronic Stuff and is ordered by the new concept of the *stuffness*, which describes the mobility and independence of Stuff. The introduction of connected electronic Stuff requires two new layers: Software and Surfaces + Volumes and this reasoning follows from the Pace Layer Prototyping argument made in Chapter Five, where in order of ease of mutability it is: Surfaces + Volumes (like screens and speakers), Software (a device's firmware) and the physical Stuff's circuitry. Finally, as Brand himself tentatively suggested, Souls are included as a further layer to describe those with agency in the home – revealing the home's residents, and as the Network Home Study suggests its pets and pests. An important implication of the framework is that the faster the layer (with high degrees of stuffness), the more precarious it is, without roots in the home and subject to change.

Applications of the Framework

The Stuff of Home is intended as a general-purpose framework with which to consider domestication and the ways homes accommodate change. To make an example of its application I will use it to explain a modern dispossession of Stuff in favour of cloud-based services and then I shall suggest some ways to struggle with this in the terms of the framework.

Dispossession: How Stuff becomes Services

As the Network Home Study suggests, tenancy implies ownership often only of one's own Stuff and increasingly less control of the home's slower infrastructural layers. Indeed, in rented homes, it might just be the "*small stuff*" that is owned, where even the larger furniture is the landlord's. However, regardless of housing ownership, the domesticated Internet promoted by Silicon Valley expects to dispossess people of even the small Stuff they might expect to own, like photograph albums, music and film collections and to some extent books. In recent years much of this Stuff has been transformed first into digital forms and then transferred to the cloud – often with a monthly subscription required for continued access. This logic asserts that the Stuff that remains material, becomes imbued with electronics, software, the network and cloud services in ways that challenge notions of ownership. These cloud services are essentially remote Software routines that while agile and sophisticated, are also unusually precarious – untangled as they are from the physical slow infrastructure of traditional utility Services. Consider again the Nabaztag (2006), Little Printer (2012) and Jibo (2017), Stuff that was rapidly rendered useless by defunct cloud Services. Furthermore, the outcome of more connected electronic Stuff served by the cloud, without a network of one's own, is a home increasingly opened to the gaze and manipulation by commercial, governmental and criminal interests. This then is a process of dispossession and increasing precarity (Standing, 2014), where that of which one has direct ownership and control becomes diminished, regardless of housing tenancy. The survival of this once precious Stuff is now dependent on fragile remote services made of Software. What do we then truly own?

Besides a presumed Silicon Valley Surveillance Capitalist agenda, others also advocate for the dispossession of Stuff and transformation to digital forms on environmental grounds – especially mass-produced, homogenized, short-lived, resource wasteful, Stuff. This logic assumes that immaterial digital Stuff demands few material resources and so has a diminished ecological impact. However, the framework suggests instead that such Stuff has increased (but unseen) ongoing ecological dependencies beyond the walls of the home – put beyond a resident's maintaining reach and implying remote invisible labour (see Chapter Three).

Minimalists have long espoused stuffless lifestyles and James Wallman's book *Stuffocation: Living More with Less* (Wallman, 2014) extends this evocatively claiming that we are suffocating in stuff. Wallman's thesis is that we need to learn to value experiences over amassed physical belongings. However, in the context of this framework, these experiences are presumably frequently mediated, controlled and network-delivered by a third-party as part of a financial transaction and the data mined by Surveillance Capitalists.

Speeding Services Up and Slowing Stuff Down

There is an alternative logic to this dispossession of Stuff that is also implied by the Stuff of Home framework, that Services can also become Stuff or more generally that Stuff (especially electronic Stuff) can manipulate the slow layers of home through the Surfaces (and Volumes) they create. This suggests some ways to struggle with dispossession. While the framework implies that the consequence of Stuff becoming

Services makes them more dependant and slower to adapt to change, it also implies that when Services become Stuff they are sped up.

As a simple example, consider how an image projector (Stuff) can apparently edit a room's decorative Scheme by creating a lit Surface – for tenants this can afford a welcome degree of (superficial) control. Similarly, Hennessey and Papanek's Nomadic Furniture (Hennessey and Papanek, 1973) is a catalogue of plans for DIY furniture motivated by the author's experiences of living in rented accommodation in the 1970s. The plans are for inexpensive "*lightweight furniture that folds, inflates, knocks down, stacks, or is disposable and can be recycled*" and several of the designs go beyond the construction of new furniture or Stuff and offer ways for the renter to access and manipulate the home's Space Plan and Scheme. Freestanding shelving can create a layer in front of a wall or a divider, without attachment to the fabric of the room. Several plans for Living Cubes are shown (entertaining, children's, relaxation and work cubes), being described as "*indoor tents*" they can be seen as a rapidly produced configuration of Stuff that offers some control of the surrounding environment, in a room you don't own (see Figure 77).

While it is straightforward to see the Internet as a Service, it is hard to identify what the utility of this service is, beyond say connectivity. The Stuff of Home helpfully pulls focus on the Service Interfaces and the Stuff that are implicated by the Service, here notably the home router. The router is identifiably Stuff and will likely be owned and controlled by the resident regardless of their tenancy situation – as the framework notes, "*A WiFi router may also be seen to create a Hertzian volume in these terms – one that can be treated as if it were a Service.*" The stuffness of the router, its relative independence, creates an opportunity to construct a network of one's own – a Service made of Stuff.

Some Services Brand identifies, namely the home's HVAC systems (heating, ventilating, and air conditioning), have through the domestication of the Internet become connected via the home network, they have Service Interfaces that are indistinguishable from Stuff and run Software – consider the Nest Learning Thermostat (2011). This both opens these slow Service layers to the possibility of fast change being made by the resident over the network (perhaps by hacking) or by external agents (typically the Service provider). In the case of both the Internet and HVAC systems, this *stuffication* creates at least the technical possibility that some maintenance of Services might be enacted by the resident, regardless of their tenancy. The network reveals ways of intervening in these Services, something of their constituent systems – their use of resources and labour become somewhat more visible.

Figure 77. Nomadic Furniture: Relaxation and Work Cubes.

© James Hennessey and Victor Papanek, 1973. Redacted.

Reflection

This chapter proposed The Stuff of Home, a new framework to generate ecological understandings of the domestication of home networks and to make accounts of modern homes in general. This builds on a reading of Brand's Shearing Layers, emphasising the dynamism of the home and the material affordance of its layers to change. I applied this framework by using it to illustrate a current struggle for the dispossession of Stuff and in doing so I drew attention to the way in which Services are being sped up and Stuff is being slowed down by the network. The unresolved question is how such homes function in the long-term? Do these new dynamics create such precarity that homes stop learning or even risk collapse? Chapter Three argued that there is nothing inherently stable about such ecosystems. Brand says that maintenance of each layer is essential, but it was precisely the maintenance of wireless networks that the Network Home Study problematised in Chapter Six.

The notion of stuffness introduced here offers a way to account for the speeding up of Services and slowing down of Stuff, both to describe a process of domestication, but also as a factor to be manipulated through design. Explorations in Slow Technology

(Hallnäs and Redström, 2001; Odom *et al.*, 2014, 2018) can be seen in this light, where designed Stuff attempts to create slow and lasting interactional behaviours and create a semi-permanent niche in the home – to become *part of the furniture*. This also relates to questions of the *inquiring power* of Research Products raised in Chapter Four and the technically mediated probes in Chapter Six – where a design's stuffness can be manipulated to participate in and disclose parts of the ecosystem under study, with a new reach made possible by the network. Indeed, Stuff can blow a hole through the walls of the home and explore the World.

The Stuff of Home framework contributes to this thesis' contention that the home and home life are often rendered too simplistically in research and design; the enumeration of home struggles in Chapter Two was intended to impress its complexity. Chapter Three argued that the dominant narrative for mass-produced domestic technologies through the 20th Century was similarly untroubled, adopting normative and homogenising ideas of home; that is also to be found also in 30 years of HCI scholarship in Ubiquitous Computing. Such accounts tend to depend on rendering domestic systems invisible; whereas the Stuff of Home framework attempts to make some of the ecosystem of the home visible. As Chapter Three concluded, an ecological perspective is conducive to finding alternative design spaces.

While the Stuff of Home does account for what is inside the walls of the home and what connections that has to the outside by way of its use of Services, it does not productively deal with the concept of privacy as a matter of design, that is central in seeking a network of one's own – Chapter Eight will offer some design patterns that do, using the vocabulary that has been developed here.

Chapter Eight: Articulating a Network of One’s Own

In this penultimate chapter I want to articulate a network of one’s own and in doing so draw together some of the threads present in this thesis, making explicit some of its implications for design. While I introduced the idea of a network of one’s own in Chapter One, it has subsequentially been present, but not unpacked until now. It is of course a play on Virginia Woolf’s 1929 essay *A Room of One’s Own* (Woolf, 1929) and in making this parallel I am implying that there are creative and fulfilling ways for homelife to unfold when one owns the network. In this chapter then I want to illustrate what this could mean in practical terms. In doing so I want to demonstrate a synthesis of the varied perspectives and contributions of this thesis, derived from my scholarship and empirical work. The challenge is to find a designerly form through which these alternatives can be adequately communicated (in future public forms) to an audience of professional designers and technologists engaged in either commercial or academic practice. For this purpose I am going to present an application of Christopher Alexander’s design patterns (Alexander et al., 1977).

This chapter has three sections, in the first I shall briefly outline the concept of design patterns, then in the second I shall describe the process by which I developed 30 patterns for a network of one’s own, which are reproduced in the appendix, then to demonstrate these in action I will describe three in some detail. In the final section I shall offer some reflection on these patterns and the process by which they were authored.

While carefully and deliberately constructed these patterns do not attempt to definitively or exhaustively articulate a network of one’s own; they are in no sense a complete language but are instead partial and generative – a system of knowledge that captures some of what I have learnt. My intention then is to provide some intellectual scaffolding for future commercial and academic practice, be that my own or that of others.

Design Patterns

In seeking to communicate a set of alternative designs that express a network of one's own, workbooks or annotated portfolios (Gaver and Martin, 2000; Gaver, 2011; Gaver and Bowers, 2012) are an obvious application and are well understood by designers and design researchers. However, while they can form a generative intermediate-level knowledge (Höök and Löwgren, 2012), they don't obviously articulate either less concrete design principles or more technically specific detail. For instance, I want to find a format to express how a design sketch might relate to both the principle of the visibility of labour and the topology of networks. My suggestion is that an adaptation of Christopher Alexander's design patterns, described in the book *A Pattern Language* (Alexander *et al.*, 1977), can go some way to deliver this. In this section I am going to briefly outline Alexander's architectural notion of a pattern language and then discuss its subsequent interpretation in software engineering and HCI research, in doing so this exposes some of the opportunities and challenges for my endeavour.

Alexander and his co-authors lay out 253 architectural patterns that are intended to form a language in which to express projects, be they towns, buildings, or rooms (Alexander et al., 1977). For instance, *14 Identifiable Neighbourhood*, *167. Six Foot Balcony* and *251. Different Chairs*. Each pattern is named and numbered, presented formally in text and imagery over a few pages; importantly each explicitly acknowledges the scale at which it operates and the other patterns to which it interrelates. These patterns implicitly represent good or successful solutions to common problems. The book's continued popularity has influenced both architectural practice and design theory, but less obviously software development and object-orientation in particular. Alexander's design patterns have been a persistent but until now a relatively weak theme in this thesis. Chapter Three suggested that design patterns can be straightforwardly read as an ecological account of vernacular architectural practice in complement to Stewart Brand's Shearing Layers; indeed Brand cites Alexander throughout How Buildings Learn (Brand, 1995). Chapter Four ascribed some of the recent popularity of hackerspaces to the codification of a set of (largely architectural and social) design patterns (Haas, Weiler and Ohlig, 2007) for communal spaces .

Through the *gang of four's* hugely influential book *Design Patterns* (Gamma et al., 1994), design patterns have come to be well understood by the software engineering community. This book explicitly interprets Alexander's concept and formally catalogues 23 patterns for object-oriented software describing how each can be identified and implemented. This is accomplished through names and numbers, textual description, diagramming, and code examples in the C++ language – each in the same formal way. In the more than 25 years since the book was published the concept of design patterns has been widely adopted in software engineering. In the 1990s software was still predominately an artisan craft, but today's Computer Science undergraduates are routinely taught design patterns and coding has largely become a practice of architecting reused distributed components, as described in Chapter Three. An example pattern is *observer* or *publish and subscribe* described in relation to the network architecture of MQTT in Chapter Five. While inspired by Alexander, all these 23 patterns operate at a similar (code-level) scale. User interactions are today also regularly expressed in the terms of design patterns (Tidwell, 2005). Aaron Marcus' article in Interactions Magazine (Marcus, 2004) helpfully outlines some ways this can be accomplished but also articulates some of the trouble of dealing with scale. Marcus comments, "The subjects of cognitive psychology, persuasion, customer service, and so on may inevitably involve principles that are not so neatly hierarchical and thus may be harder to describe in the conventions of patterns." (Marcus, 2004, p. 34). The resulting patterns are then limited to the superficial appearance and consequential affordances of interfaces. While today's software design and UI patterns successfully communicate technically specific detail, they have largely lost Alexander's concern for multiple scales and so have a diminished ecological expression.

Elements of the HCI research community have had a long-standing enthusiasm for Alexander's pattern language – distinct but in dialogue with commercial software patterns. Here design patterns are seen as a way to publicly communicate both design proposals and ethnographies of existing practices arising from academic inquiry. These two meanings were identified at the CHI 1997 workshop *Putting it all together: Towards a Pattern Language for Interaction Design*, (Bayle *et al.*, 1998) as *design* and *activity* patterns. Thomas Erickson of IBM Research would later claim that design patterns and pattern languages could serve as a lingua francas for diverse stakeholders in participatory design projects (Erickson, 2000). Andy Crabtree and colleagues (including Tom Rodden) developed activity patterns, or patterns of social action, as a framework to structure their ethnographic fieldwork (Crabtree, Hemmings and Rodden, 2002; Crabtree *et al.*, 2007). While Erickson's lingua francas (Erickson, 2000) is closest to my motivation here, its focus is the design of physical spaces and its application to interaction design remains speculative.

Perhaps the most compelling prior application of design patterns in the HCI research literature relates to three studies of patterns for ubiquitous computing (Chung *et al.*, 2004; Saponas *et al.*, 2006; Denef and Keyson, 2012). Eric Chung and colleagues developed and evaluated 45 pre-patterns for ubiquitous computing at multiple scales, these address, "*application genres, physical-virtual spaces, interaction and systems* *techniques for managing privacy, and techniques for fluid interactions.*" (Chung *et al.*, 2004, p. 234). Each pre-patterns was presented in a consistent format on a single page, although only a few examples were reproduced within the constraints of the conference paper. The notion of a pre-pattern as a nascent pattern was further explored by Scott Saponas and colleagues (including Gregory Abowd) in the domain of the digital home (Saponas *et al.*, 2006). Here 48 pre-patterns were developed and then evaluated by working with 44 user interface and industrial design practitioners to ideate designs for future homes. Their study concluded that the pre-patterns proved useful and attempted to discern objective measures of the quality of the resulting designs. Finally, through an ethnography of frontline firefighters, Sebastian Denef and David Keyson developed an activity pattern language of 16 patterns for ubiquitous computing; concluding that the resulting patterns constructed a meaningful shared understanding for diverse participants in a stakeholder design workshop (Denef and Keyson, 2012).

However, by the end of this period the use of design patterns in HCI design research was receiving more critical attention. Jonas Löwgren presented nine inspirational patterns for embodied interaction, which attempted to draw out the inspirational rather than objectively solutional qualities of patterns (Löwgren, 2007). Molly Wright Steenson (Steenson, 2009) critiqued some of Alexander's underlying commitments to a systematic (if not mechanistic) approach to generative design, not unlike Herbert Simon's Design Science (Simon, 1969), described in Chapter Four. This exposes some tensions in reconciling patterns with pragmatic research through design – with which I identify. In this spirit, Kristina Höök and Jonas Löwgren describe their *strong concepts* as, "*a new label in order to escape the established connotations and practices of design patterns*" (Höök and Löwgren, 2012, p. 23:6). Strong concepts are *generative intermediate-level knowledge* between theory and instances[82] and as such have a constrained focus on specificity and scale; their published format is not as prescribed as design patterns. By this time Löwgren had concluded that his inspirational patterns (Löwgren, 2007) had in hindsight, "*failed miserably in terms of communal interest and uptake.*" (Höök and Löwgren, 2012, p. 23:6). Similarly, in 2013, Yue Pan and Erik Stolterman published an interview study with 24 HCI researchers with experience of using patterns, concluding that despite continued interest, "*PL [Pattern Language] in HCI has not served as a real practical design tool in almost any case.*" (Pan and Stolterman, 2013, p. 1997). This is attributed in part to the sheer effort and rigour required to author something that might constitute a complete language.

[82] Instances of design are conceptualised as Stolterman's *ultimate particulars* (Stolterman, 2008).

In the subsequent ten years I would suggest that the HCI design community's interest in pattern languages has declined and that design patterns have come to be understood in rather colloquial ways. The remaining efforts have tended to have a more modest ambition to identify patterns, rather than to devise languages. For instance, Colin Gray's *dark patterns* (Gray *et al.*, 2018) identifies the reuse of malevolent patterns for persuasive user interfaces – particularly for online sales. While this necessarily exposes some of the high-level motivations of interface design beyond the surface appearance, and helpfully implicitly questions for whom a pattern is a good solution, it does not engage directly with either Alexander et al. or Gamma et al.. Instead dark patterns draw on the popular website of the same name (Brignull, 2010) and Andrew Koenig's notion of the AntiPattern[83] (Koenig, 1995), both of which have roots in software engineering understandings and practices of design patterns.

Pragmatically Alexander's design patterns seem to offer a framework I can adapt for my own purposes with a focus on format, scale, and interrelation – true to an ecological perspective on the home. However, there are evidently some theoretical and practical issues regarding completeness that need to be addressed. Mindful of this, in the next section I will describe the process by which I developed 30 patterns intended to be useful and illustrative of interrelated levels of knowledge, but still contingent, hopeful that this seeds future piecemeal efforts by others that addresses their struggles at hand. In doing I hope to critically reengage HCI Design Research with Alexander's design patterns.[84]

[83] Koenig's AntiPattern, "*gives something that looks superficially like a solution but isn't one.*" (Koenig, 1995) – an unsuccessful pattern. This explicitly cites the *gang of four*'s book (Gamma *et al.*, 1994). The term AntiPattern was later popularised by Brown et al. (Brown *et al.*, 1998) in their book of the same name, but while their definition is broadly compatible with Koenig's concept, Koenig is not acknowledged.

[84] My design patterns for a network of one's own anticipate an exploration of alternative design patterns for Ubiquitous Computing I have begun in collaboration with Nick Taylor and Jon Rogers (Chatting, Taylor and Rogers, 2021).

Developing a Pattern Language for a Network of One’s Own

This section describes the process by which I developed 30 patterns for a network of one’s own (reproduced in the appendix) and describes three in action. In sum, these patterns begin to articulate in practical terms a network of one’s own and are intended to constitute a partial language open to future interpretation and incremental addition. This necessary incompleteness seems to be consistent with Alexander’s intention – more so than one familiar only with the HCI literature might assume, see below:

> *We shall now describe a rough procedure by which you can choose a language for your own project, first by taking patterns from this language we have printed here, and then by adding patterns of your own.*
>
> 1 *First of all, make a copy of the master sequence (pages xix-xxxiv) on which you can tick off the patterns which will form the language for your project. If you don’t have access to a copying machine, you can tick off patterns in the list printed in the book, use paper clips to mark pages, write your own list, use paper markers whatever you like. But just for now, to explain it clearly, we shall assume that you have a copy of the list in front of you.*
>
> 2 *Scan down the list, and find the pattern which best describes the overall scope of the project you have in mind. This is the starting pattern for your project. Tick it. (If there are two or three possible candidates, don’t worry: just pick the one which seems best: the others will fall in place as you move forward.)*
>
> 3 *Turn to the starting pattern itself, in the book, and read it through. Notice that the other patterns mentioned by name at the beginning and at the end, of the pattern you are reading, are also possible candidates for your language. The ones at the beginning will tend to be “larger” than your project. Don’t include them, unless you have the power to help create these patterns, at least in a small way, in the world around your project. The ones at the end are “smaller.” Almost all of them will be important. Tick all of them, on your list, unless you have some special reason for not wanting to include them.*
>
> 4 *Now your list has some more ticks on it. Turn to the next highest pattern on the list which is ticked, and open the book to that pattern. Once again, it will lead you to other patterns. Once again, tick those which are relevant — especially the ones which are “smaller” that come at the end. As a general rule, do not tick the ones which are “larger” unless you can do something about them, concretely, in your own project.*
>
> 5 *When in doubt about a pattern, don’t include it. Your list can easily get too long: and if it does, it will become confusing. The list will be quite long enough, even if you only include the patterns you especially like.*
>
> 6 *Keep going like this, until you have ticked all the patterns you want for your project.*
>
> 7 *Now, adjust the sequence by adding your own material. If there are things you want to include in your project, but you have not been able to find patterns which correspond to them, then write them in, at an appropriate point in the sequence, near other patterns which are of about the same size and importance. For example, there is no pattern for a sauna. If you want to include one, write it in somewhere near bathing room (144) in your sequence.*
>
> 8 And of course, if you want to change any patterns, change them. There are often cases where you may have a personal version of a pattern, which is more true, or more relevant for you. In this case, you will get the most “power” over the language, and make it your own most effectively, if you write the changes in, at the appropriate places in the book. And, it will be most concrete of all, if you change the name of the pattern too —
>
> so that it captures your own changes clearly.

A Pattern Language – a rough procedure (Alexander et al., 1977, pp. xxxviii–xl)

With this procedure in mind, I selected and recontextualised Alexander’s architectural patterns for the domesticated Internet, before integrating my own patterns for a network of one’s own. This section shall now describe how these patterns were found and then how they operate in action.

Finding Patterns

For my language, following Alexander’s procedure, the identification of the starting pattern (step two) is rather straightforward: *141. A Room of One’s Own*! Indeed it is easy to read a patternal intent in Woolf’s essay, “*Even allowing a generous margin for symbolism, that five hundred a year stands for the power to contemplate, that a lock on the door means the power to think for oneself*’ (Woolf, 1929). This established, by the consideration of each referenced related pattern, and those related to these, a set of eight patterns quite straightforwardly emerges (Step 6) with each indentation indicating another iteration of related pattern selection:

```
          79. Your Own Home
          127. Intimacy Gradients
141. A Room of One’s Own
                    149. Reception Welcomes You
          191. The Shape of Indoor Space
                    197. Thick Walls
                    242. Front Door Bench
                    253. Things from Your Life
```

While *79. Your Own Home* pattern is not referenced by the starting pattern it speaks so directly to my endeavour that it demands to be included.

Each selected pattern needs a degree of recontextualisation for the domesticated Internet to scaffold the new patterns (Step 7). Taken in turn I used Alexander’s original text seeking resonances with the networked home, synergies with existent designs and opportunities to express the themes of this thesis. In my pattern language, while some of the names of these related patterns are changed, they retain their relative order and Alexander’s numbering is shown in brackets. Any recontextualisation of the original is noted in the new pattern’s description. Crucially *141. A Room of One’s Own* becomes *13. A Network of One’s Own (141)*.

Integrating my own patterns for the domesticated Internet (Steps 7 and 8), the language consists of 30 provisional patterns – these are indexed below and available in the appendix. The material for these new patterns is drawn from across this thesis – referencing understandings from the literature, my own studies, proposed and existent designs, network architectures, code, and electronics. Some of these patterns are counter-patterns, that denote an alternative to another; unlike anti-pattern (Koenig,

1995) this need not imply the pattern to be either unsuccessful or badly intentioned. Some proto-patterns are implied by the existing patterns but are currently unresolved and are offered as starting point for future work.

Like Alexander, each pattern is presented in the same formal way. Each is named and numbered, briefly then more elaborately described; this description includes details of where the pattern is to be found in the world and how it comes to be included. Importantly each pattern explicitly references the other patterns to which it relates – those both more abstract and more specific. The more technically specific patterns owe more to the gang of four's Design Patterns (Gamma et al., 1994). Like Alexander the ordering and numbering do not imply a hierarchical containment but do indicate a scale and degree of abstractness and allow the patterns to be grouped into broad thematic sets:

The Internet

1. The Internet
2. The Cloud

The Home
3. Tenancy
4. Your Own Home (79)

Ways of Being Seen
5. Incremental Intimacy Gradient (127)
6. Invisible Work
7. Visible Work
8. Panoptical Surveillance Capitalism

Computing Paradigms
9. Ubiquitous Computing
10. Virtual Reality
11. Mindful Computing
12. Goldberg Machines

Networked Homes
13. A Network of One's Own (141)
14. The Home WiFi Router
15. Reception Welcomes You (149)
16. Wide Area Network

Boundaries
17. The Shape of Space (191)
18. Pliable Walls (197)
19. Front Door Bench (242)
20. Positioning, Ranging and Boundary Making

Stuff
21. Nomadic Furniture
22. Stuff from Your Life (253)

Designs
23. Voice Assistant
24. Amazon Dash Button
25. Dolmio Pepper Hacker
26. Pi-hole
27, The Approximate Library

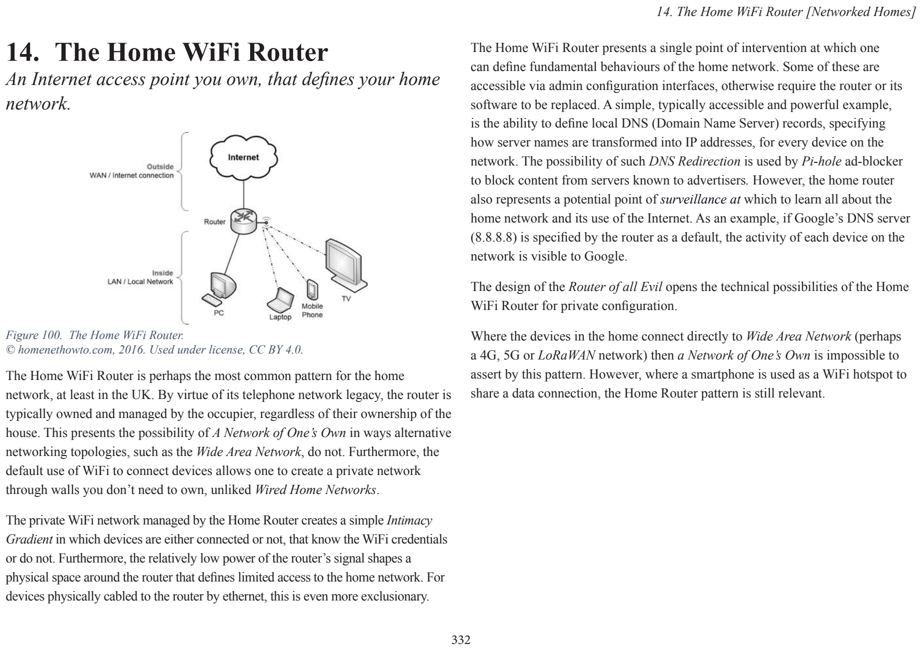
Technical Acts
28. Rogue Access Point
29. DNS Redirect
30. WiFi Deauthentication

Patterns in Action

To demonstrate these patterns in action I have selected three that describe existent designs: *14. The Home WiFi Router*, *24. Amazon Dash Button* and *25. Dolmio Pepper Hacker*. The intention is to demonstrate where one can do some of the work of design with this partial language. While these patterns describe existent designs, the process by which they are formatted and annotated as patterns within the language creates a form not unlike a workbook proposal and the group resembles an annotated portfolio. If successful, the language should allow alternatives to be expressed and critical perspectives to be taken, both in terms of technical specificity and high-level design principles.

14. The Home WiFi Router

The first pattern I have selected is *14. The Home WiFi Router* (Figure 78); this is one of the most common patterns for the home network and technically represents the possibility to assert a network of one's own. The *Network of Own's Own* pattern is central to this exercise and this thesis, so the use of this example importantly demonstrates how such a high-level and nuanced concept might be expressed at the scale of specific technical designs. It also reveals the challenge to this agency that alternative networking topologies, namely Wide Area Networks, embody. As the pattern describes, the use of WiFi allows residents to create a network through walls they don't need to own, with a router they do typically own and manage – meaning that, with sufficient technical knowhow, the router and so the network can be configured at will.



14. The Home WiFi Router [Networked Homes]

14. The Home WiFi Router

An Internet access point you own, that defines your home network.

Figure 100. The Home WiFi Router.
© homenethowto.com, 2016. Used under license, CC BY 4.0.

The Home WiFi Router is perhaps the most common pattern for the home network, at least in the UK. By virtue of its telephone network legacy, the router is typically owned and managed by the occupier, regardless of their ownership of the house. This presents the possibility of *A Network of One's Own* in ways alternative networking topologies, such as the *Wide Area Network*, do not. Furthermore, the default use of WiFi to connect devices allows one to create a private network through walls you don't need to own, unliked *Wired Home Networks*.

The private WiFi network managed by the Home Router creates a simple *Intimacy Gradient* in which devices are either connected or not, that know the WiFi credentials or do not. Furthermore, the relatively low power of the router's signal shapes a physical space around the router that defines limited access to the home network. For devices physically cabled to the router by ethernet, this is even more exclusionary.

The Home WiFi Router presents a single point of intervention at which one can define fundamental behaviours of the home network. Some of these are accessible via admin configuration interfaces, otherwise require the router or its software to be replaced. A simple, typically accessible and powerful example, is the ability to define local DNS (Domain Name Server) records, specifying how server names are transformed into IP addresses, for every device on the network. The possibility of such *DNS Redirection* is used by *Pi-hole* ad-blocker to block content from servers known to advertisers. However, the home router also represents a potential point of *surveillance at* which to learn all about the home network and its use of the Internet. As an example, if Google's DNS server (8.8.8.8) is specified by the router as a default, the activity of each device on the network is visible to Google.

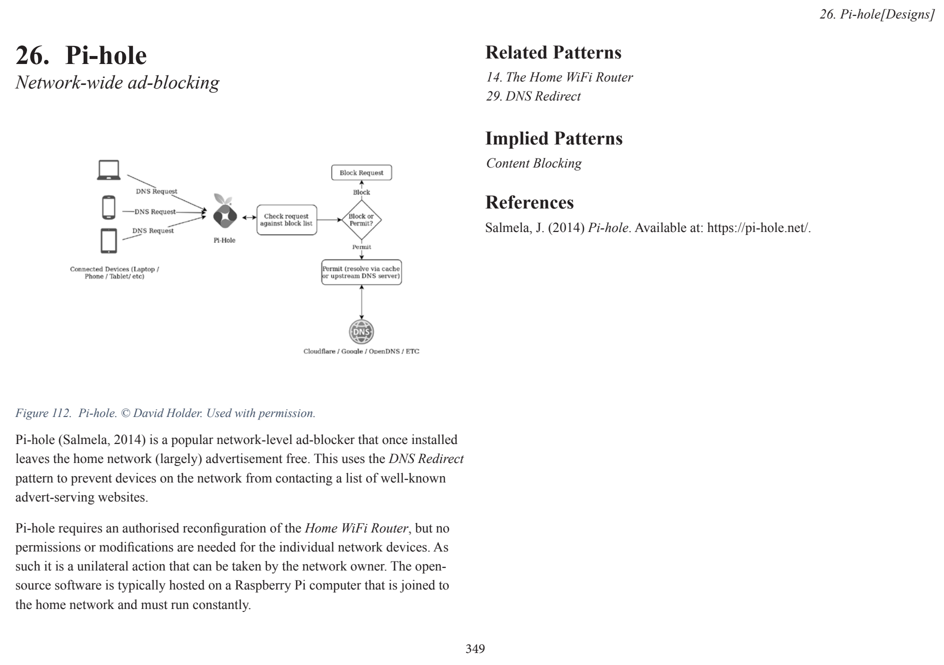
The design of the *Router of all Evil* opens the technical possibilities of the Home WiFi Router for private configuration.

Where the devices in the home connect directly to *Wide Area Network* (perhaps a 4G, 5G or *LoRaWAN* network) then *a Network of One's Own* is impossible to assert by this pattern. However, where a smartphone is used as a WiFi hotspot to share a data connection, the Home Router pattern is still relevant.

332

Figure 78. The Home Router design pattern

An example of one such technical router configuration is the popular network-level ad-blocker Pi-hole (Salmela, 2014), which provides a practical way to prevent advertisers from occupying attention inside the home, a form of struggle with the market. Described as a pattern (see Figure 79), it becomes clear that Pi-hole suggests a way to block any server on the Internet, simply with its inclusion on a so-called blocklist and without any modification of the individual devices using the network. The Pi-hole software is documented in close technical detail and is easy to identify its use of the *DNS Redirect* pattern (see Figure 80). As described in Chapter Five in relation to the Kindle hacks, DNS is a key infrastructure of the Internet that translates domain names into IP addresses, but crucially this is first attempted at the local router. Read as a set of associated patterns suggests numerous ways one might assert a network of one's own, when one can configure the Home WiFi Router. These included how parental, political or religious motivations might determine the contents of these blocklists, rather than unwanted advertisers. Furthermore, as the *DNS Redirect* pattern, suggests there are more nuanced ways in which aspects of the Internet can be replicated inside the home network and so configured to one's own specification, with only an authorised reconfiguration of the router. However, this is all reliant on the home network following the *Home WiFi Router* pattern and alternative network topologies, like *16. Wide Area Network*, do not make the same affordances.



26. Pi-hole[Designs]

26. Pi-hole

Network-wide ad-blocking

DNS Request
DNS Request
DNS Request
Connected Devices (Laptop / Phone / Tablet/ etc)
Pi-Hole
Check request against block list
Block or Permit?
Block
Block Request
Permit
Permit (resolve via cache or upstream DNS server)
DNS
Cloudflare / Google / OpenDNS / ETC

Figure 112. Pi-hole. © David Holder. Used with permission.

Pi-hole (Salmela, 2014) is a popular network-level ad-blocker that once installed leaves the home network (largely) advertisement free. This uses the *DNS Redirect* pattern to prevent devices on the network from contacting a list of well-known advert-serving websites.

Pi-hole requires an authorised reconfiguration of the *Home WiFi Router*, but no permissions or modifications are needed for the individual network devices. As such it is a unilateral action that can be taken by the network owner. The open-source software is typically hosted on a Raspberry Pi computer that is joined to the home network and must run constantly.

Related Patterns

14. The Home WiFi Router
29. DNS Redirect

Implied Patterns

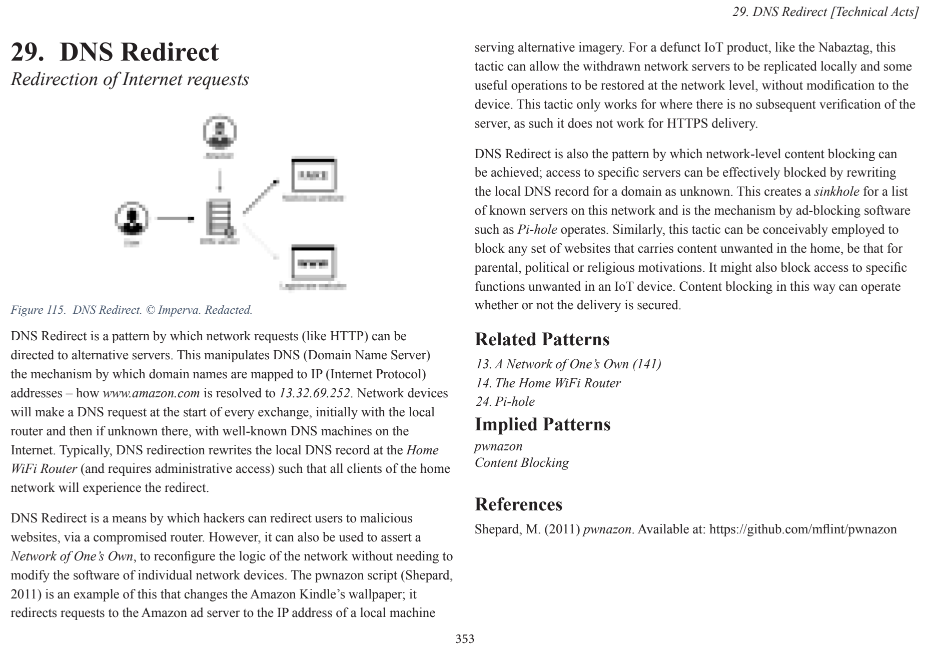
Content Blocking

References

Salmela, J. (2014) *Pi-hole*. Available at: https://pi-hole.net/.

349

Figure 79. Pi-hole design pattern



29. DNS Redirect [Technical Acts]

29. DNS Redirect

Redirection of Internet requests

Figure 115. DNS Redirect. © Imperva. Redacted.

DNS Redirect is a pattern by which network requests (like HTTP) can be directed to alternative servers. This manipulates DNS (Domain Name Server) the mechanism by which domain names are mapped to IP (Internet Protocol) addresses – how *www.amazon.com* is resolved to *13.32.69.252*. Network devices will make a DNS request at the start of every exchange, initially with the local router and then if unknown there, with well-known DNS machines on the Internet. Typically, DNS redirection rewrites the local DNS record at the *Home WiFi Router* (and requires administrative access) such that all clients of the home network will experience the redirect.

DNS Redirect is a means by which hackers can redirect users to malicious websites, via a compromised router. However, it can also be used to assert a *Network of One's Own*, to reconfigure the logic of the network without needing to modify the software of individual network devices. The pwnazon script (Shepard, 2011) is an example of this that changes the Amazon Kindle's wallpaper; it redirects requests to the Amazon ad server to the IP address of a local machine serving alternative imagery. For a defunct IoT product, like the Nabaztag, this tactic can allow the withdrawn network servers to be replicated locally and some useful operations to be restored at the network level, without modification to the device. This tactic only works for where there is no subsequent verification of the server, as such it does not work for HTTPS delivery.

DNS Redirect is also the pattern by which network-level content blocking can be achieved; access to specific servers can be effectively blocked by rewriting the local DNS record for a domain as unknown. This creates a *sinkhole* for a list of known servers on this network and is the mechanism by ad-blocking software such as *Pi-hole* operates. Similarly, this tactic can be conceivably employed to block any set of websites that carries content unwanted in the home, be that for parental, political or religious motivations. It might also block access to specific functions unwanted in an IoT device. Content blocking in this way can operate whether or not the delivery is secured.

Related Patterns

13. A Network of One's Own (141)
14. The Home WiFi Router
24. Pi-hole

Implied Patterns

pwnazon
Content Blocking

References

Shepard, M. (2011) *pwnazon*. Available at: https://github.com/mflint/pwnazon

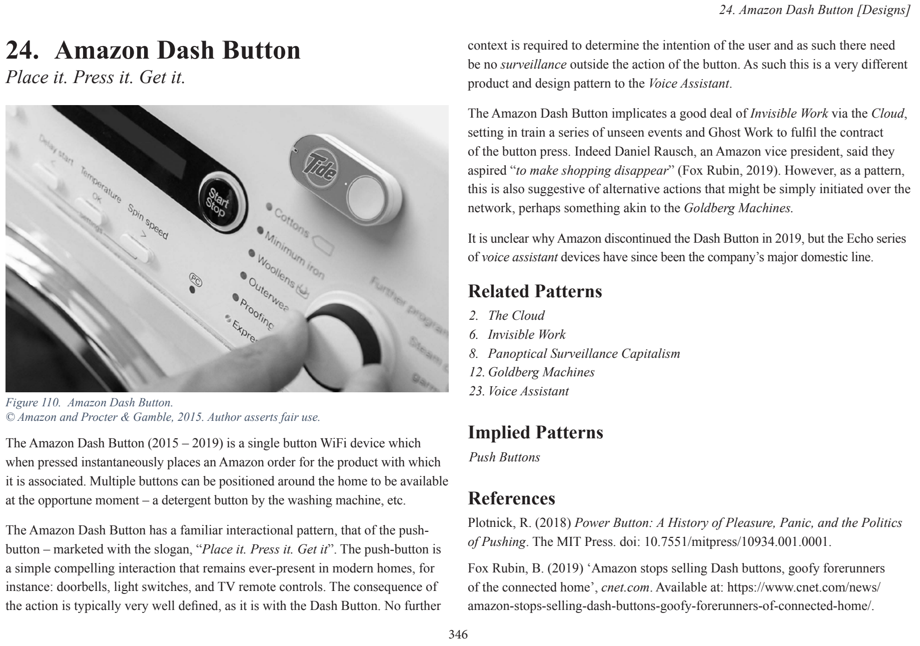
353

Figure 80. DNS Redirect design pattern

24. Amazon Dash Button

The second pattern I have selected is the *24. Amazon Dash Button* (see Figure 81); this is a single button WiFi device that when pressed instantaneously places an Amazon order for the product with which it is associated. My intention in this example is to demonstrate that an existent design can be reconsidered as a pattern for reuse and related to high-level concepts, specifically here to Invisible Work and push button interactions; then to speculate, using the pattern language, why Amazon no longer sells or supports this product.

As an existent design, the Amazon Dash Button can be decomposed into some essential interactions and operations to reveal its higher-level patterns. This implicates a more general *Push Button* pattern which makes apparent some of the qualities of push buttons discussed in Chapter Three, specifically how they tend to make work less visible and more contractual. Indeed, Daniel Rausch, an Amazon vice president for the product, said they aspired "*to make shopping disappear*" (Fox Rubin, 2019). The work consequent of a button press happens in and behind the cloud, specifically in the AWS (Amazon Web Services) cloud, via which networks of machines and people are invisibly orchestrated to deliver the desired product to the right home. Amazon's marketing materials simply present this process as, "*Place it. Press it. Get it.*" The *Invisible Work* pattern here attempts to disclose some of these properties (see Figure 82).



24. Amazon Dash Button [Designs]

24. Amazon Dash Button

Place it. Press it. Get it.

Figure 110. Amazon Dash Button.
© Amazon and Procter & Gamble, 2015. Author asserts fair use.

The Amazon Dash Button (2015 – 2019) is a single button WiFi device which when pressed instantaneously places an Amazon order for the product with which it is associated. Multiple buttons can be positioned around the home to be available at the opportune moment – a detergent button by the washing machine, etc.

The Amazon Dash Button has a familiar interactional pattern, that of the push-button – marketed with the slogan, "*Place it. Press it. Get it*". The push-button is a simple compelling interaction that remains ever-present in modern homes, for instance: doorbells, light switches, and TV remote controls. The consequence of the action is typically very well defined, as it is with the Dash Button. No further context is required to determine the intention of the user and as such there need be no *surveillance* outside the action of the button. As such this is a very different product and design pattern to the *Voice Assistant*.

The Amazon Dash Button implicates a good deal of *Invisible Work* via the *Cloud*, setting in train a series of unseen events and Ghost Work to fulfil the contract of the button press. Indeed Daniel Rausch, an Amazon vice president, said they aspired "*to make shopping disappear*" (Fox Rubin, 2019). However, as a pattern, this is also suggestive of alternative actions that might be simply initiated over the network, perhaps something akin to the *Goldberg Machines*.

It is unclear why Amazon discontinued the Dash Button in 2019, but the Echo series of *voice assistant* devices have since been the company's major domestic line.

Related Patterns

2. The Cloud
6. Invisible Work
8. Panoptical Surveillance Capitalism
12. Goldberg Machines
23. Voice Assistant

Implied Patterns

Push Buttons

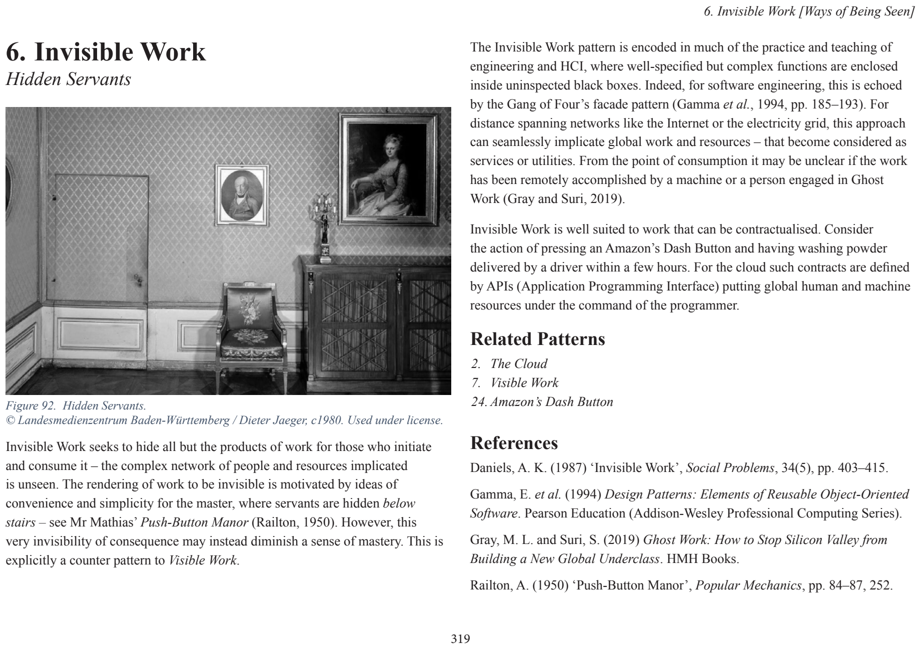
References

Plotnick, R. (2018) *Power Button: A History of Pleasure, Panic, and the Politics of Pushing*. The MIT Press. doi: 10.7551/mitpress/10934.001.0001.

Fox Rubin, B. (2019) 'Amazon stops selling Dash buttons, goofy forerunners of the connected home', *cnet.com*. Available at: https://www.cnet.com/news/amazon-stops-selling-dash-buttons-goofy-forerunners-of-connected-home/.

346

Figure 81. Amazon Dash Button design pattern



6. Invisible Work [Ways of Being Seen]

6. Invisible Work

Hidden Servants

Figure 92. Hidden Servants.
© Landesmedienzentrum Baden-Württemberg / Dieter Jaeger, c1980. Used under license.

Invisible Work seeks to hide all but the products of work for those who initiate and consume it – the complex network of people and resources implicated is unseen. The rendering of work to be invisible is motivated by ideas of convenience and simplicity for the master, where servants are hidden *below stairs* – see Mr Mathias' *Push-Button Manor* (Railton, 1950). However, this very invisibility of consequence may instead diminish a sense of mastery. This is explicitly a counter pattern to *Visible Work*.

The Invisible Work pattern is encoded in much of the practice and teaching of engineering and HCI, where well-specified but complex functions are enclosed inside uninspected black boxes. Indeed, for software engineering, this is echoed by the Gang of Four's facade pattern (Gamma *et al.*, 1994, pp. 185–193). For distance spanning networks like the Internet or the electricity grid, this approach can seamlessly implicate global work and resources – that become considered as services or utilities. From the point of consumption it may be unclear if the work has been remotely accomplished by a machine or a person engaged in Ghost Work (Gray and Suri, 2019).

Invisible Work is well suited to work that can be contractualised. Consider the action of pressing an Amazon's Dash Button and having washing powder delivered by a driver within a few hours. For the cloud such contracts are defined by APIs (Application Programming Interface) putting global human and machine resources under the command of the programmer.

Related Patterns

2. The Cloud
7. Visible Work
24. Amazon's Dash Button

References

Daniels, A. K. (1987) 'Invisible Work', *Social Problems*, 34(5), pp. 403–415.

Gamma, E. *et al.* (1994) *Design Patterns: Elements of Reusable Object-Oriented Software*. Pearson Education (Addison-Wesley Professional Computing Series).

Gray, M. L. and Suri, S. (2019) *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass*. HMH Books.

Railton, A. (1950) 'Push-Button Manor', *Popular Mechanics*, pp. 84–87, 252.

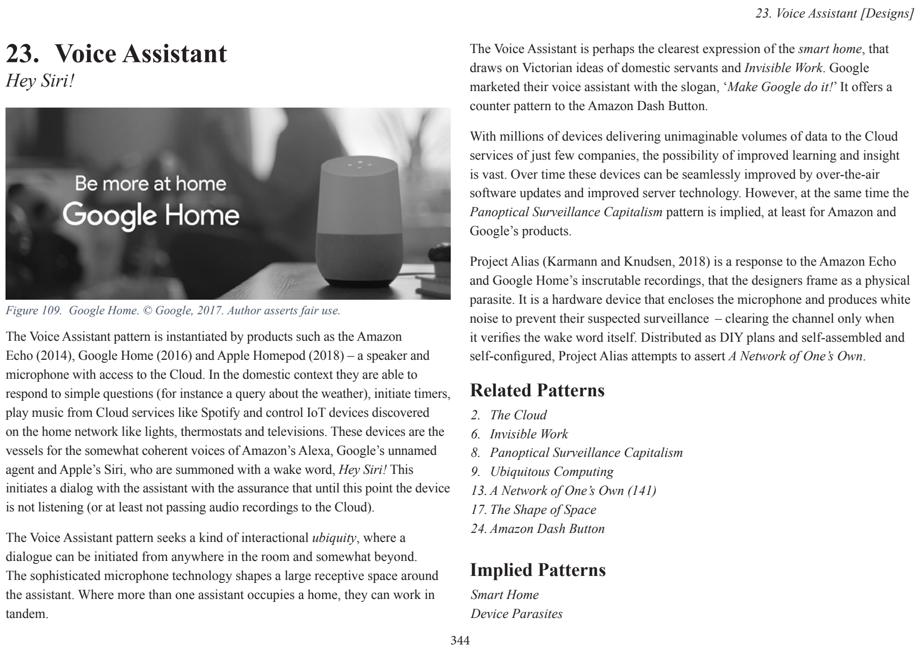
319

Figure 82. Invisible Work design pattern

Despite a history of domestic push buttons that dates back to the Victorian Country Houses (see Chapter Three) the Amazon Dash Button was received with some puzzlement. Launched on 1st April 2015, the BBC sought reassurances from Amazon that this was not an April Fool's joke (Lee, 2015); by the time the product was discontinued in

2019 CNET described them as the "*goofy forerunners of the connected home*" (Fox Rubin, 2019). Somehow these buttons represent an alternative concept to what a smart home is supposed to be, at least in the eyes of some media commentators. This might, in part, be through their association with products like washing powder, toilet paper and contraceptives – mundanities that are meant to be invisible in the aspirational smart home, not materialised as colourful buttons. Seen instead as an instance of the Push Button pattern, the Amazon Dash Button is then suggestive of alternative less commercial transaction that might be simply initiated over the network, perhaps something akin to the *Goldberg Machines* pattern.

Amazon reportedly sold millions of Dash Buttons (Fox Rubin, 2019), where their cost to the consumer (£4.99 in the UK) was deducted from the first order; seemingly a loss leader strategy aimed to stimulate repeated frequent sales and so profit. While it is unclear what motivated Amazon's decision to discontinue the product in 2019 and later to withdraw the cloud services on which it depends, when framed as a design pattern within this language one can make some speculations about its business strategy and perceptions of the market. Domestically the company has since continued to expand its range of Echo devices, each following the *Voice Assistant* pattern (see Figure 83). These voice interactions are far less contractual and far more dependent on observed context than a push button. In this respect voice assistants are instances of the *Ubiquitous Computing* pattern. Furthermore, when processed in the Cloud, recorded speech creates a rich potential for *Surveillance Capitalism* (see Figure 84), far more than discrete button events. Simply put, was the Amazon Dash Button discontinued because it didn't afford enough surveillance?



23. Voice Assistant [Designs]

23. Voice Assistant

Hey Siri!

Figure 109. Google Home. © Google, 2017. Author asserts fair use.

The Voice Assistant pattern is instantiated by products such as the Amazon Echo (2014), Google Home (2016) and Apple Homepod (2018) – a speaker and microphone with access to the Cloud. In the domestic context they are able to respond to simple questions (for instance a query about the weather), initiate timers, play music from Cloud services like Spotify and control IoT devices discovered on the home network like lights, thermostats and televisions. These devices are the vessels for the somewhat coherent voices of Amazon's Alexa, Google's unnamed agent and Apple's Siri, who are summoned with a wake word, *Hey Siri!* This initiates a dialog with the assistant with the assurance that until this point the device is not listening (or at least not passing audio recordings to the Cloud).

The Voice Assistant pattern seeks a kind of interactional *ubiquity*, where a dialogue can be initiated from anywhere in the room and somewhat beyond. The sophisticated microphone technology shapes a large receptive space around the assistant. Where more than one assistant occupies a home, they can work in tandem.

The Voice Assistant is perhaps the clearest expression of the *smart home*, that draws on Victorian ideas of domestic servants and *Invisible Work*. Google marketed their voice assistant with the slogan, '*Make Google do it!*' It offers a counter pattern to the Amazon Dash Button.

With millions of devices delivering unimaginable volumes of data to the Cloud services of just few companies, the possibility of improved learning and insight is vast. Over time these devices can be seamlessly improved by over-the-air software updates and improved server technology. However, at the same time the *Panoptical Surveillance Capitalism* pattern is implied, at least for Amazon and Google's products.

Project Alias (Karmann and Knudsen, 2018) is a response to the Amazon Echo and Google Home's inscrutable recordings, that the designers frame as a physical parasite. It is a hardware device that encloses the microphone and produces white noise to prevent their suspected surveillance – clearing the channel only when it verifies the wake word itself. Distributed as DIY plans and self-assembled and self-configured, Project Alias attempts to assert *A Network of One's Own*.

Related Patterns

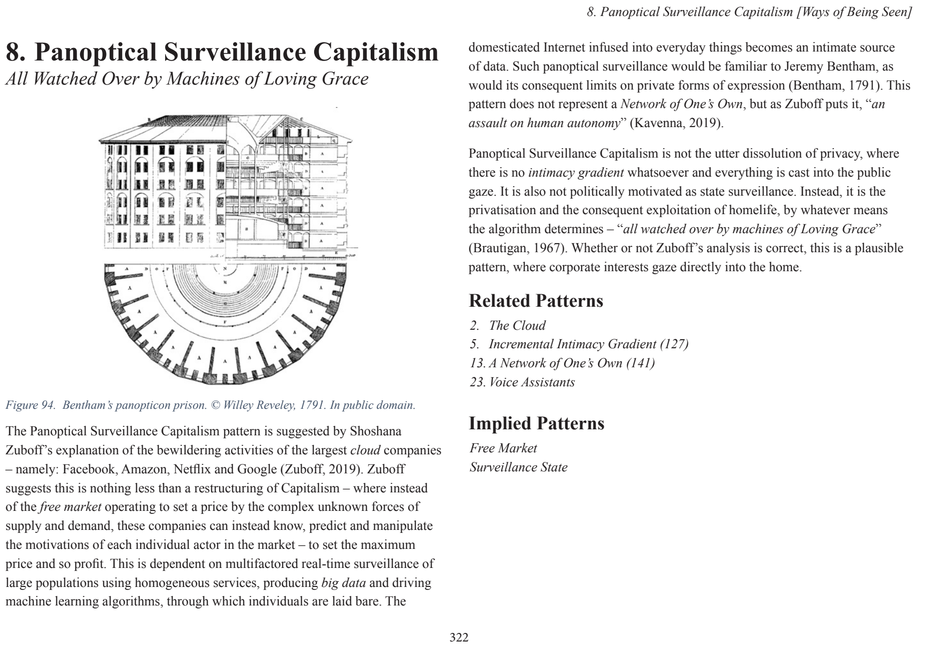
2. The Cloud
6. Invisible Work
8. Panoptical Surveillance Capitalism
9. Ubiquitous Computing
13. A Network of One's Own (141)
17. The Shape of Space
24. Amazon Dash Button

Implied Patterns

Smart Home
Device Parasites

344

Figure 83. Voice Assistant design pattern



8. Panoptical Surveillance Capitalism [Ways of Being Seen]

8. Panoptical Surveillance Capitalism

All Watched Over by Machines of Loving Grace

Figure 94. Bentham's panopticon prison. © Willey Reveley, 1791. In public domain.

The Panoptical Surveillance Capitalism pattern is suggested by Shoshana Zuboff's explanation of the bewildering activities of the largest *cloud* companies – namely: Facebook, Amazon, Netflix and Google (Zuboff, 2019). Zuboff suggests this is nothing less than a restructuring of Capitalism – where instead of the *free market* operating to set a price by the complex unknown forces of supply and demand, these companies can instead know, predict and manipulate the motivations of each individual actor in the market – to set the maximum price and so profit. This is dependent on multifactored real-time surveillance of large populations using homogeneous services, producing *big data* and driving machine learning algorithms, through which individuals are laid bare. The domesticated Internet infused into everyday things becomes an intimate source of data. Such panoptical surveillance would be familiar to Jeremy Bentham, as would its consequent limits on private forms of expression (Bentham, 1791). This pattern does not represent a *Network of One's Own*, but as Zuboff puts it, "*an assault on human autonomy*" (Kavenna, 2019).

Panoptical Surveillance Capitalism is not the utter dissolution of privacy, where there is no *intimacy gradient* whatsoever and everything is cast into the public gaze. It is also not politically motivated as state surveillance. Instead, it is the privatisation and the consequent exploitation of homelife, by whatever means the algorithm determines – "*all watched over by machines of Loving Grace*" (Brautigan, 1967). Whether or not Zuboff's analysis is correct, this is a plausible pattern, where corporate interests gaze directly into the home.

Related Patterns

2. The Cloud
5. Incremental Intimacy Gradient (127)
13. A Network of One's Own (141)
23. Voice Assistants

Implied Patterns

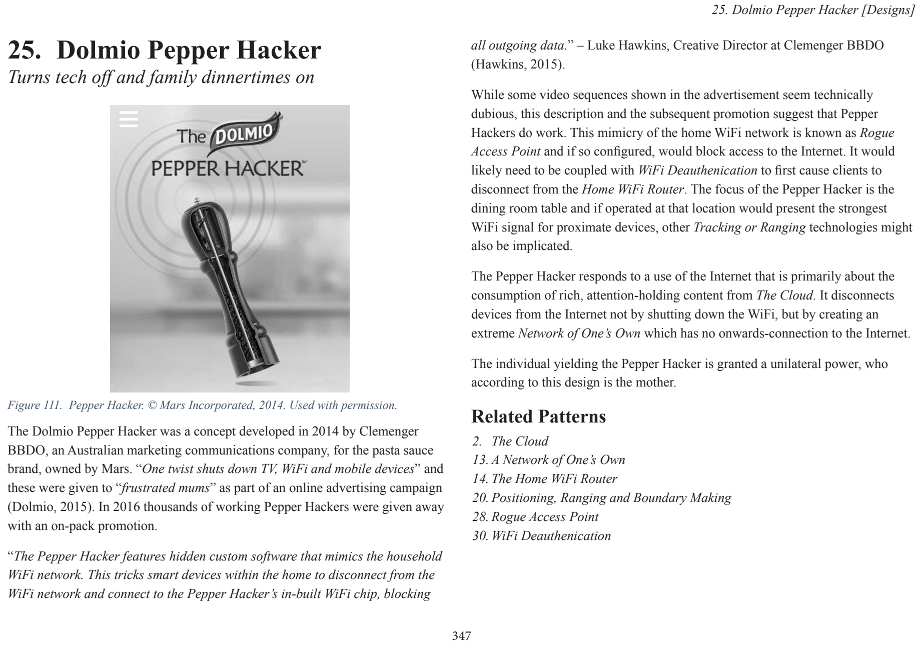
Free Market
Surveillance State

322

Figure 84. Panoptical Surveillance Capitalism design pattern

In 2014 Amazon launched another product with a button-based interaction, the Amazon Dash Wand, originally branded just the Amazon Dash. When the button was pressed the customer could either "*Scan It or Say It*" using the integrated barcode reader to scan the desired product or speak its name into the microphone. Unlike the Amazon Dash Button ordered items would then appear in a shopping basket to be reviewed on an app before the order is confirmed. The second generation of the device released in 2017 integrated Alexa and allowed some dialogue, but unlike the *Voice Assistant* pattern it was initiated by a deliberate button press and not a wake word for a ubiquitous microphone. By 2020 Amazon had also discontinued this product and withdrawn its cloud services (Gebhart, 2020); again this push button product seems not to have created the value demanded by Amazon. Using this pattern language, one might speculate that the Amazon Dash Wand was not surveillant enough. However, one push button interaction remains part of Amazon's domestic product portfolio, the Ring video doorbell (acquired in 2018), yet this home surveillance product generates rich video and enables the company's mesh wide area networking, Amazon Sidewalk (see *16. Wide Area Network*).

25. Dolmio Pepper Hacker



25. Dolmio Pepper Hacker [Designs]

25. Dolmio Pepper Hacker

Turns tech off and family dinnertimes on

Figure 111. Pepper Hacker. © Mars Incorporated, 2014. Used with permission.

The Dolmio Pepper Hacker was a concept developed in 2014 by Clemenger BBDO, an Australian marketing communications company, for the pasta sauce brand, owned by Mars. "*One twist shuts down TV, WiFi and mobile devices*" and these were given to "*frustrated mums*" as part of an online advertising campaign (Dolmio, 2015). In 2016 thousands of working Pepper Hackers were given away with an on-pack promotion.

"*The Pepper Hacker features hidden custom software that mimics the household WiFi network. This tricks smart devices within the home to disconnect from the WiFi network and connect to the Pepper Hacker's in-built WiFi chip, blocking all outgoing data.*" – Luke Hawkins, Creative Director at Clemenger BBDO (Hawkins, 2015).

While some video sequences shown in the advertisement seem technically dubious, this description and the subsequent promotion suggest that Pepper Hackers do work. This mimicry of the home WiFi network is known as *Rogue Access Point* and if so configured, would block access to the Internet. It would likely need to be coupled with *WiFi Deauthenication* to first cause clients to disconnect from the *Home WiFi Router*. The focus of the Pepper Hacker is the dining room table and if operated at that location would present the strongest WiFi signal for proximate devices, other *Tracking or Ranging* technologies might also be implicated.

The Pepper Hacker responds to a use of the Internet that is primarily about the consumption of rich, attention-holding content from *The Cloud*. It disconnects devices from the Internet not by shutting down the WiFi, but by creating an extreme *Network of One's Own* which has no onwards-connection to the Internet.

The individual yielding the Pepper Hacker is granted a unilateral power, who according to this design is the mother.

Related Patterns

2. The Cloud
13. A Network of One's Own
14. The Home WiFi Router
20. Positioning, Ranging and Boundary Making
28. Rogue Access Point
30. WiFi Deauthenication

347

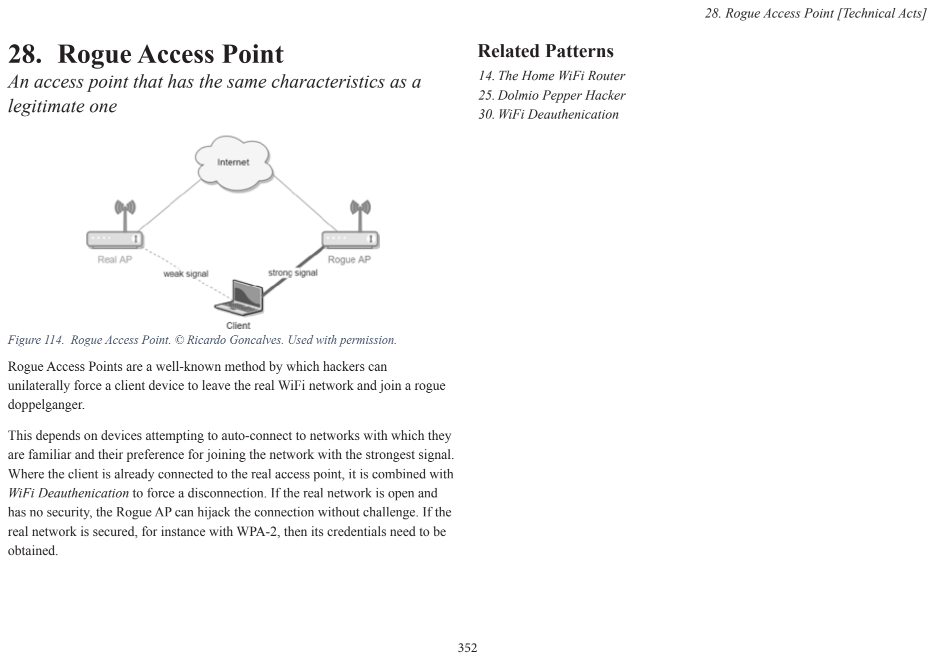
Figure 85. Dolmio Pepper Hacker design pattern

The final pattern I have selected is the *25. Dolmio Pepper Hacker* that with "*One twist shuts down TV, WiFi and mobile devices*" and "*turns tech off and family dinnertimes on*" (see Figure 85). This example is used to demonstrate how conceptual designs, for which few technical details are resolved, can become annotated with alternative technologies, revealing their various opportunities and implications; especially here for technologies that configure the network in some way.

The Pepper Hacker has an ambiguous technical resolution, it is a prop in an advertisement (where some video sequences shown seem technically dubious) and seemingly a functioning product that was later given away with an on-pack promotion. Promotional imagery (including that in Figure 85) suggests circuity and components that make some technical sense but are clearly illustrative[85]. Luke Hawkins, Creative Director at Clemenger BBDO, gave this plausible partial technical description, "*The Pepper Hacker features hidden custom software that mimics the household WiFi network. This tricks smart devices within the home to disconnect from the WiFi network and connect to the Pepper Hacker's in-built WiFi chip, blocking all outgoing data.*" (Hawkins, 2015).Read through the design patterns, this mimicry of the home

[85] Several promotional images show a well-known XBee module, an unrelated wireless technology.

WiFi network is recognisable as a *Rogue Access Point (see* Figure 86*)* and would indeed block access to content, if configured without Internet connectivity. It would not however dramatically blank the screens. The Rogue Access Point pattern makes it clear that an individual can operate this hack unilaterally with only the knowledge of the network name and password. According to the promotion this individual is the mother, and this design clearly asserts a network of her own.



28. Rogue Access Point [Technical Acts]

28. Rogue Access Point

An access point that has the same characteristics as a legitimate one

Figure 114. Rogue Access Point. © Ricardo Goncalves. Used with permission.

Rogue Access Points are a well-known method by which hackers can unilaterally force a client device to leave the real WiFi network and join a rogue doppelganger.

This depends on devices attempting to auto-connect to networks with which they are familiar and their preference for joining the network with the strongest signal. Where the client is already connected to the real access point, it is combined with *WiFi Deauthenication* to force a disconnection. If the real network is open and has no security, the Rogue AP can hijack the connection without challenge. If the real network is secured, for instance with WPA-2, then its credentials need to be obtained.

Related Patterns

14. The Home WiFi Router
25. Dolmio Pepper Hacker
30. WiFi Deauthenication

352

Figure 86. Rogue Access Point design pattern

As the Rogue Access Point pattern describes, for the desired effect of instantaneously "*turning tech off*", *WiFi Deauthenication* would also likely be employed, to first cause devices to be disconnected from the *Home WiFi Router*, before joining the mimicked network. Furthermore, the Rogue Access Point would need to have a stronger signal than the Home Router (as seen by the targeted devices), to cause the switch; this would be achieved if the Pepper Hacker was operated in proximity, say at the dining room table, targeting the devices in that room. This is quite a rudimentary form of spatial reasoning and the *Positioning, Ranging and Boundary Making* pattern suggests a set of more sophisticated alternatives that might begin to suggest ways of realising (amongst other designs) some of James Pierce's speculative engagements with digitally disconnected space (Pierce, 2016). However, as the pattern makes clear, some of these methods of spatial reasoning begin to imply forms of surveillance.

Reflection

In this chapter I have offered a commentary for my design of 30 patterns, to be found in the appendix, that attempt to articulate in practical terms a network of one's own and in doing so draw together some of the threads present in this thesis, derived from my scholarship and empirical work, making explicit some of its implications for design. I have presented an application of Christopher Alexander's design patterns (Alexander et al., 1977) as an exploration of a designerly form for this purpose.

Unlike previous HCI and design research uses of patterns, I have maintained Alexander's commitment to multiple scales – those which express high-level concepts like the principle of the visibility of labour and those which describe the technicality of the topology of networks. While Alexander does acknowledge the partial nature of pattern languages, previous attempts in the HCI seem to have become overwhelmed in attempting to create complete languages. My use of patterns is more pragmatic, plural, partial and open to incremental work; consistent with my ambition to suggest alternative outcomes for networked homes and challenge a homogenised future. However, while it was a reasonably straightforward and pleasurable task, the generation of the patterns to this resolution still represents months of work – disregarding the scholarship and empirical work that shape them. I hope they can be used in directed commercial or academic work that finds some alternative avenues for design, being incrementally adapted for the purpose at hand.

Chapter Nine: Conclusion

In this final chapter, I am going to look back this on thesis and consider the journey that I have undertaken for the best part of five years. First, I shall make a brief summary of the thesis, and then I shall offer some backstory, before recapping its most significant contributions. These established I shall revisit the central question of a network of one's own and finally speculate about future directions that this work suggests.

Summary

This thesis is a design research practice-led inquiry into the domesticated Internet. It first sought to complicate simplistic corporate and academic visions of the home by naming some of the struggles it encounters – not least to assert a private home and network of one's own. I argued that a century of domestic technologies has emphasised invisibility, ubiquity, and automation in ways that obscure a network of exploited people and finite resources. Furthermore, these technological ambitions are accompanied by machine surveillance, in ways newly enabled by the domesticated Internet, that threaten the privacy of the home.

In response, this thesis has shown some practical ways to design alternatives that assert a network of one's own and makes the work it implicates visible. The methodological approach is broadly Research Through Design supplemented by a practice described as *designerly hacking*, through which hidden technical potential is revealed and given meaning. Two empirical studies were described that together make an account of the technical possibility and social reality of the networked home: an autobiographical technical exploration of my home and network with the making of hacks and supporting research products privately and in public; and a cultural probe engagement with six rented households surfacing contemporary accounts of the domesticated Internet and in particular the challenges and opportunities of wireless networking. Together this yielded a series of technical and social insights for design that I communicate in two forms: a framework for understanding change in the networked home (*The Stuff of Home*) and a set of 30 design patterns for a network of one's own.

Well, how did I get here?

This at times has been a rather personal story and I hope in the telling my motivations, attitudes, privileges and position have been sufficiently clear. As a *mid-career* PhD thesis, I see this work as a continuation of my professional practice and a grounding for what is to come. The domestication of the Internet is a revolution[86] I have witnessed, and in some small ways contributed to, in my professional lifetime.

As I have undertaken this work I have become fascinated by some of the interwoven threads of history, which can be seen to shape the world at large and also put me where I find myself today socially, politically and academically. I want to acknowledge that these concerns have shaped a rather unusual thesis, that at times has moved rather rapidly through chains of historical, technical and popular culture references and anecdotes – from both academic and practice-driven perspectives and some of which I have first-hand experience. This somewhat surprising set of connections makes my foundational point that the home is wild and complex, made more so with the arrival of the domesticated Internet.

The ideas for this thesis first started to come together during the final months of the Family Rituals project with David Kirk at Open Lab, Newcastle University (Kirk *et al.*, 2016). I became very interested in how our bespoke designs demanded to be accommodated in the homes of our participants and then incorporated in new shared rituals, within the space of just a few weeks. I started to think about Stewart Brand's Shearing Layers (Brand, 1995; Muncie, 1997) and how new Stuff becomes part of home life, something I came to understand as domestication. Over the next year and through my visiting position at the Interaction Research Studio, these ideas developed into a proposal for a workshop at CHI 2017. Andy Boucher, Audrey Desjardins and I organised *Making Home: Asserting Agency in the Age of IoT* in an Airbnb house in Denver, Colorado with the intention of discussing domestic technologies in a domestic context (Chatting, Wilkinson, *et al.*, 2017). The call for participation highlighted challenges to domestic agency (but notably not privacy) in terms of the book of collected essays Quantified Home (Space Caviar, 2014) and Standing's Precariat (Standing, 2014). The workshop was attended by 18 international researchers and by all measures was a success.

My subsequent application for AHRC Design Star funding echoed the CHI workshop themes with the proposed thesis title, *Making Home: Agency, Precarity and the Internet of Things*. As originally framed the thesis was a "*practice-based PhD … a design-led exploration of the Smart Home and the Internet of Things (IoT)*". As the work started to

[86] I am a little conflicted about declaring this a "revolution" as that seems to imply stability in the present order, nonetheless, it is rhetorically convenient.

unfold the focus shifted from the nebulous Smart Home to the domesticated Internet and a concern for the network rather than just the things. In these early articulations, there were promises of interventions and activism on the behalf of renters and the precariat, through the design and deployment of toolkits, concluding with some grand final design. This became problematised for me through my new understandings of Mouffe's agonism and my orientation towards Critical Design – a single final exemplary design seemed increasingly out of place. Instead, the expression of my design practice became necessarily more exploratory and prototypical, rather than highly finished. While renting remains a persistent theme in this thesis, it is not as central as first proposed. Similarly, precarity makes an important contribution to the Stuff of Home framework for domestication (Chapter Eight), but as a way to discuss stability in general, rather than in Standing's sociological conception. This kind of emergence in design research is described by Bill Gaver, Peter Krogh, Andy Boucher and myself (Gaver *et al.*, 2022).

I can't recall exactly how I came to Virginia Woolf's Room of One's Own[87], but it suggested a way to think about privacy in practical terms, where I hadn't been able to make agency work so productively[88]. Quite quickly the title a *Network of One's Own* suggested itself and made explicit the network as the principal matter of my inquiry. By this time too, Zuboff had published Surveillance Capitalism (Zuboff, 2019) which suggested clear reasons to assert privacy and preserve the sanctity of the home with respect to the network. With privacy comes the implication of gaze and visibility, which gave my analysis of the automated home and technologies like Ubicomp a new, and I believe productive dimension. In all these ways this thesis engages with feminist texts and perspectives, but I am aware of my current relative ignorance of feminist technoscience as a broader field of study. As the thesis has now finally emerged it calls on me to familiarise myself with this literature as I plan my future work. This will include the writings of Donna Haraway and Karen Barad, and make further engagements with Lucy Suchman's work.

[87] It would most likely have been a BBC Radio Four programme – it is on almost all the time in my house.

[88] Had agency have been further pursued I would have expected to have engaged more strongly with the work of Michel Foucault.

Contributions

This thesis' contributions can be grouped into four categories: a review of contemporary and historic sources that reveal often unseen struggles and work in the home, a design research methodology that seeks alternatives by revealing complex systems, two design research empirical studies that show contemporary home networks in new technical and social ways, and two new frameworks for making account of and doing design in the home network which draws together the themes across the thesis.

Showing the Home in Struggle

Chapters One, Two and Three (part one) contribute a review of contemporary and historic sources that reveal some of the often unseen struggles and work in the home, which contrasts with often repeated ideals of the home as a peaceful and static place. This is important as it establishes the domesticated Internet as neither inevitable, singular, nor permanent – a place where design can operate.

To deliver this Chapter Two catalogues seven types of struggle: the domestication of new, economic precarity, living in independence and with others, the demands of productivity, interactions with the market and living in private. This synthesised a range of contemporary and historic sources from academic and popular authors. Importantly for the narrative that followed, it established Brand's Shearing Layers (Brand, 1995; Muncie, 1997) and Zuboff's Surveillance Capitalism (Zuboff, 2019) in terms of struggle. Then Chapter Three, using Daniel's conception of Invisible Work (Daniels, 1987), reveals some of the often unseen work of the home. Using an inclusive definition of the automated home, the chapter explores invisibility in the context of the Victorian country house and modern Ghost Work (Gray and Suri, 2019), then through the mass electrification of the suburban home in the 20th Century and a post-war push button culture, then in 1980s dreams of Smart Homes and finally in the Ubiquitous Computing agenda of the 1990s. Crucially this makes explicit how many of these ubiquitous, ambient, calm, unremarkable or even enchanted technologies require forms of surveillance; how the invisible computer demands a visible user. Once the gaze of the machine is identified some struggle can be enacted, either through everyday tactics or designed alternatives. To my knowledge, this is the first time these elements have been brought together in this way and I hope this analysis will be of value to both HCI and STS scholars alike.

I have long had a frustration with simplistic visions of future homes and a somewhat sceptical view of Ubiquitous Computing. Through this process I feel I am more justified in this. With respect to the mass-produced commercial Internet of Things available today, it becomes very clear that these represent a rather narrow conception of home. If homogenised products require simple homogenised homes and lives, what alternative forms of production might better respond to the struggles of the home? I shall make some tentative suggestions in my final discussion of a network of one's own.

Methods for Seeking Alternative

Chapters Three (part two) and Four contributed a methodologic response to the techno-social complexity of the home and its networks. First, existing strategies for making alternative designs that reveal the struggles and the work of the networked home were described; these promote ecologic, ludic and heterogenic understandings. Then to seek some technical alternative in the networked home, I described a new research through design method of designerly hacking, which was situated in the context of the practices of hacking since the late 1950s and academic discourses, including DiSalvo's Adversarial Design (DiSalvo, 2012). Designerly hacking breaks up and reveals complex technical systems (often in private) before putting them back together as public designerly forms; in doing so it is intended to enable designers to engage with new technical alternatives. Here to seek alternatives to the complex sociotechnical infrastructures of Surveillance Capitalism and give them a designerly currency. This contributes to a small body of existing design research work that integrates accounts of hacking in research through design.

As I have suggested with my example of the BT Balance prototype, I consider aspects of designerly hacking to have been part of my practice for many years, in ways I expect are common for those with a similar technical and design education. However, in formalising the methodology here, and putting it in a theoretical framework, I am aware of some new priorities. Principally, how one can intentionally put a hack back together, so this new possibility makes an offer to a less technically engaged design audience, but without presenting too much specificity and limiting imaginative outcomes? Furthermore, when framed in terms of Latourian black boxes and Actor-Network Theory, this hacking (and especially hacks of network technologies) become a mode of exploration, consistent with a Research Through Design inquiry.

Contemporary Accounts

Chapters Five and Six contributed two complementary empirical design research studies that applied these methods and that together made an account of the technical possibility and social reality of the networked home. Chapter Five was an autobiographical study of my own home and network, seeking to find contemporary technical alternatives and demonstrating designerly hacking. This chapter documented some of the many hacks of my house that I made privately and with workshop participants, and finally those which were resolved for a wider public audience – namely the Approximate Library. In doing so I addressed some of the practical challenges of autobiographical work which is self-resourced and self-directed, a model of working I hope others will find enabling. In reflecting on the design of the Router of All Evil and breadsticks, I proposed Pace Layer Prototyping to consider the design of prototypes using material (and immaterial) affordances to adapt and so in some senses learn at different paces of change. This philosophy informed the subsequent design of the WiFi Meters in the Network Home Study and I hope might be widely applicable in Research Through Design inquiries. The technical possibility this process disclosed directly informed many of the subsequent design patterns for a network of one's own.

Chapter Six described the Networked Home Study, an engagement with six rented households through cultural probe activities and three bespoke WiFi measurement instruments. This contributed a scholarly contemporary account of the domesticated Internet, specifically of home WiFi networks, which I believe was previously absent – indeed had previously been described as *unremarkable* (Crabtree *et al.*, 2012). Instead, this study presented six themes and associated rich anecdotal material that complicates the conceptions of the home network and accounts of domestication. These themes informed both the Stuff of Home framework and the design patterns articulating a network of one's own, but notably *Network Mindfulness* and *Maintenance* seem to speak to questions at the heart of this thesis.

The *Network Mindfulness* theme seems to suggest a new strategy for dealing with technical complexity, not by hiding or ignoring it, but by making it visible and gazing at it. As a design pattern this then offers a new direction for designing for visible work. While HCI has previously considered Mindfulness , these have been rather abstract and with a concern for mental health. The *Maintenance* theme calls into question the ability of (even relatively knowable) people to maintain wireless networks and I shall return to this point in my final discussion of a network of one's own.

Finally, the Networked Home Study has opened a discussion of technically mediated probes, instruments and meters – not prototypical designs but probes designed with a specific inquiring power. While these did help participants reveal aspects of their networks that would otherwise be invisible, a set of new designs now suggest themselves to me. For instance, a meter to show some of the contended nature of WiFi with some kind of measure of radio interference, and another meter to reveal some of the dynamic qualities of the Internet beyond the home – this is work for the future.

Frameworks for Design

Chapters Seven and Eight contribute two complementary ways to understand and design alternative networked homes that draw on the learnings from the studies and scholarship – together they are intended to communicate the main understandings that this thesis has generated. In Chapter Seven, *The Stuff of Home* framework is presented with which to understand the domestication of the Internet and its relationship with infrastructure; it directly extends Stewart Brand's Shearing Layer model (Brand, 1995) responding to the challenges of the networked home. Chapter Eight then articulated 30 design patterns for a network of one's own that contribute both a starting point for design that emphasises the visibility of work and a re-examination of Christopher Alexander's notion of a pattern language (Alexander *et al.*, 1977).

The Stuff of Home framework contributes a way of understanding the home in ecological terms, which I have described as a tactic for making alternative designs. The analysis of the home points to new dynamics created by the network, not least Silicon Valley's expectation to dispossess homes of their Stuff in favour of mediated experiences. Significantly it also draws attention to the ways in which the network both speeds up Services and slows down Stuff, arguably destabilising the home. I shall return to this question in my discussion of a network of one's own in the next section.

The design patterns for a network of one's own are intended to be generative of new designs both by myself and others. I found the authoring of these patterns a deeply satisfying activity and one rather hard to stop, with new patterns constantly suggesting themselves. I was pleased how so many of the themes and exemplars that my scholarship and practice have exposed could quite straightforwardly be integrated into this system of knowledge. Furthermore, I found that when the patterns were put into action annotating existent designs and proposals, the process gave me new insights. Some of the patterns like Goldberg Machines and Mindful Computing are already suggestive to me of new designs. Through this work (and likely through future publications) I hope that I can engage the HCI community in a renewed critical discourse regarding the use of design patterns. I believe my work has shown there is potential in reengaging with some of Alexander's original intentions, specifically in how patterns can address different scales from the abstract to the specific and how a language need not (perhaps can not) be complete. However, this should not be approached uncritically, some of Alexander's patterns are somewhat problematic, for instance, *27. Men and Women*.

Taken together the Stuff of Home and the design patterns represent two ways to understand the home and then design for it. With their reliance on Brand's Shearing

Layers and Alexander's Pattern Language, they can be seen to represent rather systematic, even scientific, approaches. This highlights a seeming contradiction between the Research Through Design approach to which I have committed and these outcomes. Chapter Four set up a dichotomy between the traditions of Research Through Design and Design Science; with my designerly hacking being explicitly motivated by RTD. While I see neither the Shearing Layers nor Pattern Languages as an uncritical and uncreative design-thinking-by-numbers process, they are still philosophical systems that I have been enticed by, when I had set out to find wild, strange, and unsystematic alternatives. This tension interests me, but resolving it here is beyond the scope of the thesis.

A Network of One's Own?

So finally, to return to the question of how one might assert a network of one's own. As the Hack My House explorations and the Router of All Evil demonstrated, the home WiFi router technically represents the possibility to assert a network of one's own and is currently one of the most common patterns for the home network. As the Stuff of Home model suggests, WiFi allows residents to create networks through walls they don't need to own, with a router they do typically own and manage. The question is then how one configures this possibility, whether that is through private interventions and hacks (that imply forms of technical know-how) or whether this is embedded in products manufactured at some commercial scale (for a wider audience). On the face of it, it makes sense to focus on the latter, to show how professional designers can find alternative logics and embed them into the products they make, as this promises the ability to work at scale. However, this introduces a problem that has, up to now been somewhat implicit: commercial products have a commercial imperative. The Amazon Dash Button, Dolmio Pepper Hacker and Pi-hole patterns (24-26) demonstrate three different revenue models: single purchase, promotional and free software. However, where a product is dependent on externally maintained resources (like servers), perhaps only the rental, advertising or surveillance business models can offer the sustainable income that commercial companies demand. The list of well-motivated but now defunct Internet of Things is perhaps a testament to that. Indeed, Zuboff suggests that Surveillance Capitalism itself was born of a commercial necessity to find an income stream for Google's free search product.

So, while this thesis has demonstrated ways of finding new technical and social possibilities for a network of one's own, commercial designs embedding these values must also have viable (and unproblematic) business models to operate in the market for any sustained time – and these are hard to identify. Is one's only response unilaterally to build one's own pirate utopia free and self-resourced (assuming one has the technical skill to do so)? The DIY model might offer a viable alternative where designers can make kits and plans, and individuals (with relatively less technical skill) can find their own ways to resource and sustain them. In recent years the Interaction Research Studio has developed a series of self-build designs, the product of designerly intention and training, but assembled and configured by a public with everyday technical skills. These projects have included: ProbeTools (Boucher *et al.*, 2018), the Yo-Yo Machines (W. Gaver *et al.*, 2022) and the My Naturewatch Camera (Gaver *et al.*, 2019) which was made by about 3,500 people. These show a potential wild, ludic, avenue for future work that considers further the possibility of home networked devices with designerly authorship but interpreted for individual homes . My future work is then drawn towards DIY and self-built outcomes.

And yet, with many of these liberties afforded by the home WiFi router, a struggle continues with mesh (like Amazon Sidewalk) and wide area network technologies (like 5G), where it is far from obvious how one might assert a network of one's own when one is dispossessed of a private network. This would require another set of strategies that might be shown by a process of designerly hacking.

Finally, there is perhaps a more existential problem facing the networked home – that of the problem of the maintenance of WiFi, which questions if wireless networks can ever be one's own. Maintenance was a strong theme that came from the Home Network Study, as already described here, it raises questions about the ability of (even relatively knowable) people to maintain wireless networks. Wireless is inherently more contested, being a shared medium, more open to interference and more entangled with the complexities of the physical world than a cable simply establishing a dedicated connection. While wireless may open the possibility of a network of one's own for people who are tenants in their homes, the complex invisible dynamics of these networks are too inscrutable to make many simple fixes and changes. It is at this late point in thesis that I have made the connection with the maintenance literature and in particular with Steven Jackson's article *Rethinking Repair* (Jackson, 2014). In retrospect, Jackson's account resonates so many of the themes expressed here, not least with the instability of complex systems – which is easily read in parallel with the ecological concern of Chapter Three and the work of Stewart Brand (which is cited), for whom maintenance is also a central issue. It also makes connections with the feminist literature with which I seek to engage further. Most ominously it tells of the catastrophic breakdown of systems that cannot be maintained. Does the wireless home network threaten the home itself?

Future Struggles

And so this thesis is done. As one might expect, given the agonistic position I have taken, there is no final victory to report and while there are practical ways to design networks that better respect the sanctity of the home right now, these struggles are ongoing and as Wilson's Temporary Autonomous Zones suggest there are new challenges over the horizon. I intend to find ways to publish the contributions of this work to a wider design audience in the hope that others will find it of use in their work. As for me, I have pointed to multiple ways to continue this work, but most immediately I want to address the final question of wireless maintenance raised here – I am curious what instruments one could make that would better disclose some of this complexity. In the meantime, this summer I'm planning to move out of my flat and buy a home of my own – wish me luck!

References

Abowd, G. D. (2012) ‘What next, Ubicomp? Celebrating an intellectual disappearing act’, in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp ’12*. New York, New York, USA: ACM Press, p. 31. doi: 10.1145/2370216.2370222.

Adelson, F. B. (2019) ‘Grandfather of invention : Art of Rube Goldberg on view in Philadelphia’.

Agre, P. E. (1997) *Computation and Human Experience*. Cambridge University Press. doi: 10.1017/CBO9780511571169.

Ahmed, K. (2018) ‘Seeing the Whole Earth from Space Changed Everything’, *Medium*. Available at: https://medium.com/the-long-now-foundation/earth-and-civilization-in-the-macroscope-82243cad20bd.

Aipperspach, R., Hooker, B. and Woodruff, A. (2008) ‘The Heterogeneous Home’, in *UbiComp 2008: Ubiquitous Computing*, pp. 222–231. doi: 10.1145/1409635.1409666.

Akama, Y. and Light, A. (2015) ‘Towards mindfulness: Between a detour and a portal’, *Conference on Human Factors in Computing Systems - Proceedings*, 18, pp. 625–634. doi: 10.1145/2702613.2732498.

Alexander, C. *et al.* (1977) *A Pattern Language: Towns, Buildings, Construction*. OUP USA (Center for Environmental Structure Berkeley, Calif: Center for Environmental Structure series).

Alexander, C. (1979) *The Timeless Way of Building*. Oxford University Press (Center for Environmental Structure Berkeley, Calif: Center for Environmental Structure series).

Amar, Y. *et al.* (2018) ‘An Analysis of Home IoT Network Traffic and Behaviour’. Available at: http://arxiv.org/abs/1803.05368.

Ambient Devices (2020). Available at: http://www.ambientdevices.com/.

Andersen, K. and Wilde, D. (2012) ‘Circles and Props: Making Unknown Technology’, *Interactions*. New York, NY, USA: Association for Computing Machinery, 19(3), pp. 60–65. doi: 10.1145/2168931.2168944.

Anderson, C. (2003) ‘The Wi-Fi Revoluition: The wireless Internet has arrived – and now the sky’s the limit.’, *WIRED*. Available at: https://www.wired.com/2003/05/wifirevolution/.

Anderson, R. J. (1994) 'Representations and Requirements: The Value of Ethnography in System Design', *Human–Computer Interaction*, 9(2), pp. 151–182. doi: 10.1207/s15327051hci0902_1.

Arnall, T., Knutsen, J. and Martinussen, E. S. (2013) 'Immaterials: Light painting WiFi', *Significance*, 10(4), pp. 38–39. doi: 10.1111/j.1740-9713.2013.00683.x.

Ashton, K. (2009) 'That ' Internet of Things ' Thing', *RFiD Journal*. Available at: http://www.rfidjournal.com/articles/view?4986

Ashton, K. (2016) *Beginning the Internet of Things*. Available at: https://medium.com/@kevin_ashton/beginning-the-internet-of-things-6d5ab6178801

Asthana, A., Sobti, A. and Kane, A. (2014) 'Postman'. Available at: https://www.postman.com/.

Auger, J., Hanna, J. and Encinas, E. (2017) 'Reconstrained Design: Confronting Oblique Design Constraints', *Nordes*, 7(1).

Austin, J. *et al.* (2016) 'A Smart-Home System to Unobtrusively and Continuously Assess Loneliness in Older Adults', *IEEE Journal of Translational Engineering in Health and Medicine*. IEEE, 4(January), pp. 1–11. doi: 10.1109/JTEHM.2016.2579638.

Back, M. *et al.* (2001) 'Reading Experiences for a Museum Exhibition', *Computer*, 34(1), pp. 80–87.

Bayle, E. *et al.* (1998) 'Putting it all together', *ACM SIGCHI Bulletin*, 30(1), pp. 17–23. doi: 10.1145/280571.280580.

Beaumont, K. (2003) *The Man Behind the Movement*, *MIT Technology Review*. Available at: https://www.technologyreview.com/2003/11/01/233698/the-man-behind-the-monster/.

Beaver, J., Boucher, A. and Pennington, S. (eds) (2007) *The Curious Home*. Interaction Research Studio. Available at: https://research.gold.ac.uk/4722/1/curioushome_spreads_3.pdf.

Bell, G., Blythe, M. and Sengers, P. (2005) 'Making by making strange: Defamiliarization and the design of domestic technologies', *ACM Transactions on Computer-Human Interaction*, 12(2), pp. 149–173. doi: 10.1145/1067860.1067862.

Bell, G. and Dourish, P. (2006) 'Yesterday's tomorrows: Notes on ubiquitous computing's dominant vision', *Personal and Ubiquitous Computing*, 11(2), pp. 133–143. doi: 10.1007/s00779-006-0071-x.

Bell, G. and Dourish, P. (2007) 'Back to the shed: Gendered visions of technology and domesticity', *Personal and Ubiquitous Computing*, 11(5), pp. 373–381. doi: 10.1007/s00779-006-0073-8.

Bentham, J. (1791) *Panopticon Or the Inspection House*. T. Payne (Panopticon Or the Inspection House).

Berg, A. (1995) 'A Gendered Socio-Technical Construction: The Smart House', in Heap, N. (ed.) *Information technology and society: a reader*. London: Sage.

Berglund, P. (2005) 'Bubblegym'.

Berners-Lee, T. (1989) 'Information Management: A Proposal. Internal Project Proposal', *Cern*, (May), p. 20.

Bey, H. (1991) *T.A.Z.: The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism*. Autonomedia (New autonomy series).

Bey, H. (1993) 'Permanent TAZs', *The Anarchist Library*, pp. 1–7. Available at: http://dreamtimevillage.org/articles/permanent_taz.html.

Bishop, D. and Hulbert, T. (2009) *Luckybite BirdBox*. Available at: https://vimeo.com/20639763.

Blankenship, L. (1986) *The Conscience of a Hacker*. Available at: http://phrack.org/issues/7/3.html.

Blevis, E. *et al.* (2015) 'Ecological Perspectives in HCI', in *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 2401–2404. doi: 10.1145/2702613.2702634.

Blevis, E., Lim, Y. and Stolterman, E. (2006) 'Regarding software as a material of design', *Proceedings of Design Research …*, (2004), pp. 1–20. Available at: http://dspace.kaist.ac.kr/handle/10203/5536.

Boehner, K., Gaver, W. and Boucher, A. (2012) 'Probes', in *Inventive Methods*. Routledge, pp. 199–215. doi: 10.4324/9781315884394.

Borning, A. *et al.* (2020) 'SurveillanceCapitalism@CHI: Civil Conversation around a Difficult Topic', in *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery (CHI EA '20), pp. 1–6. doi: 10.1145/3334480.3381068.

Boucher, A. *et al.* (2018) 'TaskCam: Designing and Testing an Open Tool for Cultural Probes Studies', in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery (CHI '18), pp. 1–12. doi: 10.1145/3173574.3173645.

Boucher, A. *et al.* (2019) 'ProbeTools', *Interactions*, 26(2), pp. 26–35. doi: 10.1145/3305358.

Boutin, P. (2011) *The Struggle to Spread the Minority Report Interface*, *MIT Technology Review*. Available at: https://www.technologyreview.com/2011/04/22/195179/the-struggle-to-spread-the-minority-report-interface/.

Bowers, J. (2012) 'The logic of annotated portfolios: Communicating the value of "research through design"', *Proceedings of the Designing Interactive Systems Conference, DIS '12*, pp. 68–77. doi: 10.1145/2317956.2317968.

Bowles, N. (2018) 'Thermostats, Locks and Lights: Digital Tools of Domestic Abuse', *The New York Times*, pp. 1–5. Available at: https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

Brambilla, M. (1993) *Demolition Man*.

Brand, S. (ed.) (1968) *Whole Earth Catalog*.

Brand, S. (1972) 'Spacewar - Fanatic Life and Symbolic Death Among the Computer Bums', *Rolling Stone*. Available at: https://www.wheels.org/spacewar/stone/rolling_stone.html.

Brand, S. (1985) 'Keep Designing', *Whole Earth Review*.

Brand, S. (1987) *The Media Lab: Inventng the future at M.I.T.*

Brand, S. (1995) 'How Buildings Learn: what happens after they're built', *Penguin Books*, p. 720. doi: 10.2307/990971.

Brand, S. (1999) *The Clock Of The Long Now: Time And Responsibility*. Basic Books.

Brand, S. (2018) 'Pace Layering: How Complex Systems Learn and Keep Learning', *Journal of Design and Science*. doi: 10.21428/7f2e5f08.

Brandt, R. L. (2011) *One Click: Jeff Bezos and the Rise of Amazon.com*. Portfolio/Penguin.

Bridle, J. (2018) *New Dark Age: Technology and the End of the Future*. Verso Books.

Bridle, J. (2019) 'The Age of Surveillance Capitalism by Shoshana Zuboff review – we are the pawns', *The Guardian*, p. 1. Available at: https://www.theguardian.com/books/2019/feb/02/age-of-surveillance-capitalism-shoshana-zuboff-review.

Brignull, H. (2010) *Dark Patterns - User Interfaces Designed to Trick People*. Available at: http://darkpatterns.org/.

Broll, G. and Benford, S. (2005) 'Seamful Design for Mobile Games', *Design*, pp. 1–19. doi: 10.1007/11558651_16.

Brown, W. J. *et al.* (1998) *AntiPatterns: Refactoring Software, Architectures, and Projects in Crisis*. New York: John Wiley and Sons.

Burgess, M. (2018) *From Fitbit to PlayStation, the justice system is drowning in digital evidence*, *WIRED UK*. Available at: https://www.wired.co.uk/article/uk-police-courts-data-justice-trials-digital-evidence-rape-cases-cps.

Burke, M. (2019) *Man hacks Ring camera in 8-year-old girl's bedroom, taunts her: 'I'm Santa Claus'*, *nbcnews.com*. Available at: https://www.nbcnews.com/news/amp/ncna1100586.

Burrington, I. (2016) *Networks of New York: An Illustrated Field Guide to Urban Internet Infrastructure*. Melville House.

Butler, P. (2019) 'Social care chiefs: funding crisis puts tens of thousands at risk', *The Guardian*. Available at: https://www.theguardian.com/society/2019/jun/26/social-care-funding-crisis-putting-tens-of-thousands-at-risk.

Cadwalladr, C. (2012) 'Anonymous: behind the masks of the cyber insurgents', *The Guardian*. Available at: https://www.theguardian.com/technology/2012/sep/08/anonymous-behind-masks-cyber-insurgents.

Cadwalladr, C. (2013) 'Stewart Brand's Whole Earth Catalog, a book that changed the world', *The Guardian*. Available at: https://www.theguardian.com/books/2013/may/05/stewart-brand-whole-earth-catalog.

Callon, M. and Latour, B. (1981) 'Unscrewing the Big Leviathan: How Actors Macro-Structure Reality and How Sociologists Help Them to do so', *Advances in Social Theory and Methodology: Toward an integration of micro and macro-sociologies*. Edited by K. Knorr-Cetina and A. V Cicourel. Boston, London and henley: Routledge and Kegan Paul, pp. 277–303.

Campbell, C. (2019) 'How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens', *Time*. Available at: https://time.com/collection/davos-2019/5502592/china-social-credit-score/.

Candy, S. (2010) *The futures of everyday life: Politics and the design of experiential scenarios*, *University of Hawaiʻi at Mānoa*.

Chalmers, M. and MacColl, I. (2003) 'Seamful and Seamless Design in Ubiquitous Computing', *Workshop At the Crossroads: The Interaction of HCI and Systems Issues in UbiComp.*, (January), p. 8. doi: 10.1.1.104.9538.

Chan, T. F. (2018) 'A Chinese university suspended a student's enrolment because of his dad's bad social credit score', *Business Insider Australia*. Available at: https://

www.businessinsider.com.au/china-social-credit-affects-childs-university-enrolment-2018-7?r=US&IR=T.

Chang, A. *et al.* (2001) 'LumiTouch: An emotional communication device', *Conference on Human Factors in Computing Systems - Proceedings*, pp. 313–314. doi: 10.1145/634067.634252.

Chang, A. (2012) 'Deep Inside a Facebook Hackathon, Where the Futureof Social Media Begins', *Wired*. Available at: https://www.wired.com/2012/07/facebook-gears-up-next-big-thing-in-three-day-camp-hackathon/.

Chatting, D. (2017) 'Home Network Map : An Instrument for Design-Led Inquiry', *CHI 2017 Making Home workshop*.

Chatting, D., Wilkinson, G., *et al.* (2017) 'Making home: Asserting agency in the age of IoT', in *Conference on Human Factors in Computing Systems - Proceedings*. doi: 10.1145/3027063.3027081.

Chatting, D., Kirk, D. S. S., *et al.* (2017) 'Making Ritual Machines: The Mobile Phone as a Networked Material for Research Products', *Conference on Human Factors in Computing Systems - Proceedings*. New York, NY, USA, New York, USA: ACM (CHI '17), 2017-May, pp. 435–447. doi: 10.1145/3025453.3025630.

Chatting, D., Yurman, P., *et al.* (2017) 'Ritual Machine V: Where are You?', *Proceedings of the 3rd Conference on Biennial Research Through Design*, pp. 131–147. doi: 10.6084/m9.figshare.4746958.v1.

Chatting, D. J. (2008) 'Action and reaction for physical map interfaces', in *TEI'08 - Second International Conference on Tangible and Embedded Interaction - Conference Proceedings*. doi: 10.1145/1347390.1347432.

Chatting, D. and McCahill, C. (2005) *Powerbook Puppet*. Available at: http://davidchatting.com/powerbookpuppet/

Chatting, D., Taylor, N. and Rogers, J. (2021) 'Design for Reappearance in Smart Technologies', in *CSCW 2021 Workshop on Designing for Data Awareness*.

Chesterton, G. K. (1912) *What's Wrong with the World?*

Chetty, M. *et al.* (2010) 'Who's hogging the bandwidth', in *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*. New York, New York, USA: ACM Press, p. 659. doi: 10.1145/1753326.1753423.

Chetty, M., Sung, J. and Grinter, R. (2007) 'How smart homes learn: The evolution of the networked home and household', *UbiComp 2007: Ubiquitous Computing*, pp. 127–144. doi: 10.1007/978-3-540-74853-3.

Chung, E. S. *et al.* (2004) ‘Development and evaluation of emerging design patterns for ubiquitous computing’, *DIS2004 - Designing Interactive Systems: Across the Spectrum*, pp. 233–242. doi: 10.1145/1013115.1013148.

Clarke, A. C. (1962) *Profiles of the Future: An Inquiry Into the Limits of the Possible*. Harper & Row.

Coke, E. (1644) *The Third Part of the Institutes of the Laws of England: Concerning High Treason, and Other Pleas of the Crown, and Criminal Causes*. A. Crooke.

Combs, G. (1998) ‘Wireshark’.

Corcoran, B. E. and Schwartz, J. (1997) ‘The House that Bill Gates’s Money Built’, *The Washington Post*, 28 August. Available at: https://www.washingtonpost.com/archive/politics/1997/08/28/the-house-that-bill-gatess-money-built/083910d4-78c8-4d09-ab66-820cfb103e46/.

Cornwall, H. (1985) *Hacker’s Handbook*.

Cox, A. L. *et al.* (2016) ‘Design Frictions for Mindful Interactions’, pp. 1389–1397. doi: 10.1145/2851581.2892410.

Crabtree, A. *et al.* (2007) ‘Patterns of technology usage in the home: Domestic legacy and design’, *Relation*, 10(1.104), p. 6083. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.19.5687&amp;rep=rep1&amp;type=pdf.

Crabtree, A. *et al.* (2012) ‘Unremarkable networking: The home network as a part of everyday life’, *Proceedings of the Designing Interactive Systems Conference, DIS ’12*, pp. 554–563. doi: 10.1145/2317956.2318039.

Crabtree, A. *et al.* (2018) ‘Building accountability into the Internet of Things: the IoT Databox model’, *Journal of Reliable Intelligent Environments*, 4(1), pp. 39–55. doi: 10.1007/s40860-018-0054-5.

Crabtree, A., Hemmings, T. and Rodden, T. (2002) ‘Pattern-based support for interactive design in domestic settings’, *Proceedings of the Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques, DIS*, pp. 265–275. doi: 10.1145/778712.778749.

Crabtree, A., Hemmings, T. and Rodden, T. (2003) ‘Informing the Development of Calendar Systems for Domestic Use’, *Computer Supported Cooperative Work: CSCW: An International Journal*.

Crampton Smith, G. (1997) ‘Computer-related design at the Royal College of Art: 1997 graduation projects’, *Interactions*, 4(6), pp. 27–33. doi: 10.1145/267505.267511.

Criado-Perez, C. (2019) *Invisible Women: Exposing Data Bias in a World Designed for Men*. Chatto & Windus.

Cross, N. (1982) 'Designerly ways of knowing', *Design Studies*, 3(4), pp. 221–227. doi: 10.1016/0142-694X(82)90040-0.

Csete, A. (2012) 'gqrx'.

Cunningham, S. and Jones, M. (2005) 'Autoethnography: A Tool for Practice and Education', *Proceedings of the 6th ACM SIGCHI New Zealand chapter's international conference on Computer-human interaction (CHINZ '05)*, pp. 1–8. doi: 10.1145/1073943.1073944.

Curtis, A. (2011a) 'All Watched Over by Machines of Loving Grace'. BBC.

Curtis, A. (2011b) 'How the "ecosystem" myth has been used for sinister means'. Available at: https://www.theguardian.com/environment/2011/may/29/adam-curtis-ecosystems-tansley-smuts.

Dahl, R. (2009) 'Node.js'.

Dahley, A., Wisneski, C. and Ishii, H. (1998) 'Water Lamp and Pinwheels: Ambient Projection of Digital Information into Architectural Space', *CHI '98 extended abstracts on Human factors in computing systems*.

Dalsgaard, P. (2017) 'Instruments of inquiry: Understanding the nature and role of tools in design', *International Journal of Design; Vol 2, No 1 (2008)*, 11(1), pp. 21–33.

Daniels, A. K. (1987) 'Invisible Work', *Social Problems*, 34(5), pp. 403–415.

Davies, C. (2007) *The hidden censors of the Internet*, *WIRED*. Available at: https://www.wired.co.uk/article/the-hidden-censors-of-the-internet.

Davoli, L. and Redström, J. (2014) 'Materializing Infrastructures for Participatory Hacking', *Proceedings of the 2014 conference on Designing interactive systems - DIS '14*, pp. 121–130. doi: 10.1145/2598510.2602961.

Denef, S. and Keyson, D. V. (2012) 'Talking about implications for design in pattern language', *Conference on Human Factors in Computing Systems - Proceedings*, pp. 2509–2518. doi: 10.1145/2207676.2208418.

Denefleh, T. *et al.* (2019) 'Sensorstation: Exploring Simple Sensor Data in the Context of a Shared Apartment', *Proceedings of the 2019 on Designing Interactive Systems Conference - DIS '19*, (Figure 1), pp. 683–695. doi: 10.1145/3322276.3322309.

Deschamps-Sonsino, A. (2018) *Smarter Homes: How Technology Will Change Your Home Life*. Apress.

Desjardins, A. (2016) *Design-in-Living*. Simon Fraser University.

Desjardins, A. *et al.* (2017) 'Exploring DIY tutorials as a way to disseminate research through design', *Interactions*, 24(4), pp. 78–82. doi: 10.1145/3098319.

Desjardins, A. *et al.* (2019) 'Alternative avenues for IoT: Designing with non-stereotypical homes', *Conference on Human Factors in Computing Systems - Proceedings*. doi: 10.1145/3290605.3300581.

Desjardins, A. and Ball, A. (2018) 'Revealing Tensions in Autobiographical Design in HCI', *Proceedings of the 2018 on Designing Interactive Systems Conference 2018 - DIS '18*, pp. 753–764. doi: 10.1145/3196709.3196781.

Desjardins, A. and Wakkary, R. (2016) 'Living In A Prototype', *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, pp. 5274–5285. doi: 10.1145/2858036.2858261.

Desjardins, A., Wakkary, R. and Odom, W. (2015) 'Investigating Genres and Perspectives in HCI Research on the Home', in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*, pp. 3073–3082. doi: 10.1145/2702123.2702540.

Dewey, J. (1929) *Experience and Nature*.

DiSalvo, C. (2009) 'Design and the construction of publics', *Design Issues*, 25(1), pp. 48–63. doi: 10.1162/desi.2009.25.1.48.

DiSalvo, C. (2012) *Adversarial Design*. The MIT Press.

von Donnersmarck, F. H. (2006) *Das Leben der Anderen*.

Dourish, P. (2017) *The Stuff of Bits: An Essay on the Materialities of Information*. 1st edn. The MIT Press.

Dourish, P. and Bell, G. (2007) 'The infrastructure of experience and the experience of infrastructure: Meaning and structure in everyday encounters with space', *Environment and Planning B: Planning and Design*, 34(3), pp. 414–430. doi: 10.1068/b32035t.

Dreyfuss, E. (2018) *The Internet Became Less Free in 2018 . Can We Fight Back ?*, *WIRED*. Available at: https://www.wired.com/story/internet-freedom-china-2018/.

Duffy, F. (1990) 'Measuring building performance', *Facilities*, 8(5), pp. 17–20. doi: 10.1108/eum0000000002112.

Dunne, A. (2006) *Hertzian Tales: Electronic Products, Aesthetic Experience, and Critical Design*, *Critique*. The MIT Press.

Dunne, A. and Gaver, W. W. (1997) 'The pillow: Artist-designers in the digital age', *Conference on Human Factors in Computing Systems - Proceedings*, 22-27-Marc(March), pp. 361–362. doi: 10.1145/1120212.1120434.

Dunne, A. and Raby, F. (2001) *Design Noir: The Secret Life of Electronic Objects*. August.

Dunne, A. and Raby, F. (2013) *Speculative Everything: Design, Fiction, and Social Dreaming*. MIT Press (The MIT Press).

Durrant, A. *et al.* (2017) 'Transitions in Digital Personhood', in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. New York, New York, USA: ACM Press, pp. 6398–6411. doi: 10.1145/3025453.3025913.

Eclipse (2009) 'mosquitto'.

Edward T. Hall (1963) 'A System for the Notation of Proxemic Behavior', *American Anthropologist*, 65(5), pp. 1003–1026.

Eich, B. (1995) 'JavaScript'.

Eisenberg, M. A. (2015) *Does Alexa Observe Shabbat?* Available at: https://medium.com/@mikeeisenberg/does-alexa-observe-shabbat-330f521bf6a2.

Ems, L. (2014) 'Amish Workarounds: Toward a Dynamic, Contextualized View of Technology Use', *Journal of Amish and Plain Anabaptist Studies*, 2(1), pp. 42–58. doi: 10.18061/1811/59690.

Engelbart, D. and English, W. (1968) *A research center for augmenting human intellect*.

Erickson, T. (2000) 'Lingua francas for design: Sacred places and pattern languages', *Proceedings of the Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques, DIS*, pp. 357–368.

Feder, B. (2003) 'Glass That Glows and Gives Stock Information', *The New York Times*, pp. 8–11.

Felberbaum, M. (2004) 'This Ain't Woody Allen's Orb', *WIRED*. Available at: https://www.wired.com/2004/04/this-aint-woody-allens-orb/.

Field, R. (1987) *Knowledge Navigator*.

Fielding, R. T. (2000) *REST: Architectural Styles and the Design of Network-based Software Architectures*. University of California, Irvine. Available at: http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm.

Fischli, P. and Weiss, D. (1987) *The Way Things Go*.

Foote, B. and Yoder, J. (1997) 'Big ball of mud', *Pattern languages of program design*, (217), pp. 244–4695. Available at: http://www.laputan.org/mud/mud.html.

Forlizzi, J. (2008) 'The Product Ecology', *International Journal of Design*, 2(1), pp. 11–20.

Forlizzi, J. *et al.* (2018) 'Let's Get Divorced', in *Proceedings of the 2018 ACM Conference Companion Publication on Designing Interactive Systems*. New York, NY, USA: ACM, pp. 395–397. doi: 10.1145/3197391.3197395.

Forlizzi, J. and DiSalvo, C. (2006) 'Service robots in the domestic environment', in *Proceeding of the 1st ACM SIGCHI/SIGART conference on Human-robot interaction - HRI '06*. New York, New York, USA: ACM Press, pp. 258–265. doi: 10.1145/1121241.1121286.

Formo, J. (2012) 'Ericsson's UX Lab & BERG explores the Internetworks of Things'. Available at: https://web.archive.org/web/20130605052549/http://www.ericsson.com/uxblog/2012/05/ux-lab-x-berg-explores-iot/.

Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison*. New York: Pantheon Books.

Fowler, G. A. (2019) 'Alexa has been eavesdropping on you this whole time', *The Washington Post*. Available at: https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/.

Fox Rubin, B. (2019) 'Amazon stops selling Dash buttons, goofy forerunners of the connected home', *cnet.com*. Available at: https://www.cnet.com/news/amazon-stops-selling-dash-buttons-goofy-forerunners-of-connected-home/.

Främling, K. and Nyman, J. (2010) *Openwattson*.

Franz, G. and Papert, S. (1988) 'Computer as Material: Messing about with Time.', *Teachers College Record*, pp. 408–17. Available at: http://www.papert.org/articles/ComputerAsMaterial.html.

Frayling, C. (1993) 'Research in Art and Design'.

Gamma, E. *et al.* (1994) *Design Patterns: Elements of Reusable Object-Oriented Software*. Pearson Education (Addison-Wesley Professional Computing Series).

Gatehouse, C. and Chatting, D. (2020) 'Inarticulate Devices', in *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. New York, NY, USA: ACM, pp. 2119–2131. doi: 10.1145/3357236.3395426.

Gates, B. and Ottavino, J. (1995) *Road Ahead*. HighBridge Company.

Gaver, B. and Bowers, J. (2012) 'Annotated portfolios', *Interactions*, 19(4), pp. 40–49.

doi: 10.1145/2212877.2212889.

Gaver, B., Dunne, T. and Pacenti, E. (1999) ‘Design: Cultural probes’, *interactions*, 6(February), pp. 21–29. doi: 10.1145/291224.291235.

Gaver, B. and Martin, H. (2000) ‘Alternatives: exploring information appliances through conceptual design proposals’, *Proceedings of the SIGCHI conference on Human Factors in Computing Systems - CHI ’00*, 2(1), pp. 209–216. doi: 10.1145/332040.332433.

Gaver, W. (2002) ‘Designing for Homo Ludens’, *I3 Magazine*, pp. 2–6. doi: 10.1145/2207676.2208538.

Gaver, W. *et al.* (2004) ‘The Drift Table: Designing for Ludic Engagement’, *Extended abstracts of the 2004 conference on Human factors and computing systems - CHI ’04*, pp. 885–990. doi: 10.1145/985921.985947.

Gaver, W. *et al.* (2008) ‘Threshold Devices: Looking out from the Home’, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM (CHI ’08), pp. 1429–1438. doi: 10.1145/1357054.1357278.

Gaver, W. *et al.* (2010) ‘The prayer companion: Openness and specificity, materiality and spirituality’, *Conference on Human Factors in Computing Systems - Proceedings*, 3, pp. 2055–2064. doi: 10.1145/1753326.1753640.

Gaver, W. (2011) ‘Making Spaces: How Design Workbooks Work’, *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI ’11*, pp. 1551–1560. doi: 10.1145/1978942.1979169.

Gaver, W. (2012) ‘What should we expect from research through design?’, *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI ’12*, p. 937. doi: 10.1145/2207676.2208538.

Gaver, W. *et al.* (2019) ‘My Naturewatch Camera: Disseminating Practice Research with a Cheap and Easy DIY Design’, in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, pp. 1–13.

Gaver, W. *et al.* (2022) ‘Yo–Yo Machines’, in *CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 1–17. doi: 10.1145/3491102.3517547.

Gaver, W., Hooker, B. and Dunne, A. (2001) *The Presence Project*. Royal College of Art (Rca Crd Projects Series).

Gaver, W. W. (1991) ‘Technology Affordances’, *Conference on Human Factors in Computing Systems - Proceedings*, pp. 79–84. doi: 10.1145/108844.108856.

Gaver, W. W. *et al.* (2004) ‘Cultural probes and the value of uncertainty’, *Interactions*, 11(5), p. 53. doi: 10.1145/1015530.1015555.

Gaver, W. W. (2006) ‘The video window: My life with a ludic system’, *Personal and Ubiquitous Computing*, 10(2–3), pp. 60–65. doi: 10.1007/s00779-005-0002-2.

Gaver, W. W. *et al.* (2013) ‘Indoor Weather Stations: Investigating a Ludic Approach to Environmental HCI Through Batch Prototyping’, *CHI ’13 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 3451–3460. doi: 10.1145/2466416.2466474.

Gaver, W. W. *et al.* (2022) ‘Emergence as a Feature of Practice-based Design Research’, in *Designing Interactive Systems Conference 2022*. doi: 10.1145/3532106.3533524.

Gaver, W. W. and Boucher, A. (2021) ‘Yo-Yo Machines: Self-Build Peripheral Awareness Communication Devices’, *Interactions*. New York, NY, USA: Association for Computing Machinery, 28(6), pp. 22–25. doi: 10.1145/3490446.

Geary, J. (2012) ‘Tracking the trackers: What are cookies? An introduction to web tracking’. Available at: https://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro.

Gebhart, A. (2020) ‘Amazon does away with the Dash Wand’, *cnet.com*. Available at: https://www.cnet.com/home/smart-home/amazon-does-away-with-the-dash-wand/.

Gershenfeld, N. (1999) *When Things Start to Think*. Henry Holt and Company.

Gibson, J. J. (1979) *The Ecological Approach to Visual Perception*. Lawrence Erlbaum Associates (Resources for ecological psychology).

Gillard, M. (2020) ‘Who’s Using Amazon Web Services?’, *Contino.io*. Available at: https://www.contino.io/insights/whos-using-aws.

Goddard, W. and Cercos, R. (2015) ‘Playful hacking within research-through-design’, *OzCHI 2015: Being Human - Conference Proceedings*, pp. 333–337. doi: 10.1145/2838739.2838802.

Goldberg, R. (1931) ‘The Self-operating napkin: The Inventions of Professor Lucifer G. Butts, A.K.’, *Collier’s*.

Goode, L. and Simonite, T. (2021) ‘Jeff Bezos steps down as Amazon boss’, *WIRED*. Available at: https://www.wired.com/story/bezos-departure-ceo-shows-amazon-cloud-company/.

Graham-Harrison, E. and Cadwalladr, C. (2018) ‘Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach’, *The Guardian*.

Gray, C. M. *et al.* (2018) ‘The dark (patterns) side of UX design’, *Conference on Human Factors in Computing Systems - Proceedings*, 2018-April, pp. 1–14. doi: 10.1145/3173574.3174108.

Gray, M. L. and Suri, S. (2019) *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass*. HMH Books.

Greenberg, S. and Fitchett, C. (2001) ‘Phidgets: Easy development of physical interfaces through physical widgets’, *UIST (User Interface Software and Technology): Proceedings of the ACM Symposium*, 3(2), pp. 209–218.

Greene, S., Thapliyal, H. and Carpenter, D. (2016) ‘IoT-based fall detection for smart home environments’, in *2016 IEEE international symposium on nanoelectronic and information systems (iNIS)*, pp. 23–28.

Greenwald, G. (2013) ‘NSA collecting phone records of millions of Americans daily - revealed’, *The Guardian*, pp. 1–5. Available at: http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Gregg, M. and DiSalvo, C. (2013) ‘The Trouble with White Hats’, *The New Inquiry*, (1959), pp. 6–8. Available at: https://thenewinquiry.com/the-trouble-with-white-hats/.

Gringoli, F. *et al.* (2019) ‘Free your CSI: A channel state information extraction platform for modern Wi-Fi chipsets’, *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, pp. 21–28. doi: 10.1145/3349623.3355477.

Grinter, R. E. *et al.* (2005) ‘The Work to Make a Home Network Work’, *Ecscw*, pp. 469–488. doi: 10.1007/1-4020-4023-7_24.

Grönvall, E. (2018) ‘WiredRadio’, in *Proceedings of the 2018 ACM Conference Companion Publication on Designing Interactive Systems*. New York, NY, USA: ACM, pp. 123–127. doi: 10.1145/3197391.3205423.

Grönvall, E., Fritsch, J. and Vallgårda, A. (2016) ‘FeltRadio’, pp. 829–840. doi: 10.1145/2901790.2901818.

Haas, T., Weiler, L. and Ohlig, J. (2007) *Building a Hacker Space*. Available at: https://wiki.hackerspaces.org/images/8/8e/Hacker-Space-Design-Patterns.pdf.

Haddon, L. (2011) ‘Domestication Analysis, Objects of Study, and the Centrality of Technologies in Everyday Life’, *Canadian Journal of Communication*, 36(2), pp.

2015–2017. doi: 10.22230/cjc.2011v36n2a2322.

Hafner, K. (1997) ‘The Epic Saga of The Well’, *WIRED*. Available at: http://www.wired.com/wired/archive/5.05/ff_well_pr.html.

Hallnäs, L. and Redström, J. (2001) ‘Slow technology - Designing for reflection’, *Personal and Ubiquitous Computing*, 5(3), pp. 201–212. doi: 10.1007/PL00000019.

Hancock, T. and Bezold, C. (1994) ‘Possible futures, preferable futures.’, *The Healthcare Forum journal*, 37(2), pp. 23–29.

Harper, R. (2001) ‘Smart Homes at the Start of the 21St Century’, *Ingenia*, pp. 46–50.

Harper, R. (2003) *Inside the Smart House*. Berlin, Heidelberg: Springer-Verlag.

Hartmans, A. (2018) ‘All the companies and divisions under Google’s parent company, Alphabet’. Available at: https://www.businessinsider.com/alphabet-google-company-list-2017-4.

Hauser, S. *et al.* (2018) ‘Deployments of the table-non-table’, in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 1–13. doi: 10.1145/3173574.3173775.

Hawkins, L. (2015) *DOLMIO Pepper Hacker*. Available at: https://www.lukehawkins.com.au/DOLMIO-Pepper-Hacker.

von Hayek, F. A. (1937) ‘Economics and Knowledge’, *Economica*. [London School of Economics, Wiley, London School of Economics and Political Science, Suntory and Toyota International Centres for Economics and Related Disciplines], 4(13), pp. 33–54. Available at: http://www.jstor.org/stable/2548786.

He, N. and Hilleli, E. (2021) *Invisible Roomates*. Available at: https://eranhilleli.com/invisible-roommates.

Henchey, N. (1978) ‘Making Sense of Future Studies’, *Alternatives*. Alternatives Inc, 7(2), pp. 24–27. Available at: http://www.jstor.org/stable/45030200.

Henley, J. (2014) ‘Mindfulness: a beginner’s guide’, *The Guardian*. Available at: https://www.theguardian.com/lifeandstyle/shortcuts/2014/jan/07/mindfulness-beginners-guide-meditation-technique-treatment-depression.

Hennessey, J. and Papanek, V. (1973) *Nomadic Furniture*. Knopf Doubleday Publishing Group.

Herman, J. (2010) ‘Why Everything Wireless Is 2.4 GHz’, *WIRED*. Available at: https://www.wired.com/2010/09/wireless-explainer/.

Hern, A. and Waterson, J. (2020) ‘Ofcom to be put in charge of regulating internet in UK’, *The Guardian*. Available at: https://www.theguardian.com/media/2020/feb/12/ofcom-to-be-put-in-charge-of-regulating-internet-in-uk.

Hertz, G. (2012) *Critical Making*. Telharmonium Press.

Hill, D. (2003) *iPod and adaptive design*. Available at: https://www.cityofsound.com/blog/2003/11/ipod_and_adapti.html.

Hill, K. and Mattu, S. (2018) *The House That Spied on Me*, *Gizmodo*. Available at: https://gizmodo.com/the-house-that-spied-on-me-1822429852.

Hogge, B. (2010) ‘Open Data Study’. Available at: http://www.soros.org/initiatives/information/focus/communication/articles_publications/publications/open-data-study-20100519/open-data-study-100519.pdf.

Honig, B. (1993) *Political Theory and the Displacement of Politics*. Cornell University Press.

Höök, K. and Löwgren, J. (2012) ‘Strong concepts’, *ACM Transactions on Computer-Human Interaction*, 19(3), pp. 1–18. doi: 10.1145/2362364.2362371.

Huizinga, J. (1955) *Homo Ludens: A Study of the Play-element in Culture*. Beacon Press (Beacon Paperback 15--Sociology).

Hutchins, E. (1995) *Cognition in the Wild*. MIT Press (A Bradford book).

Hvistendahl, M. (2017) ‘Inside China’s Vast New Experiment in Social Ranking’. Available at: https://www.wired.com/story/age-of-social-credit/.

Ingold, T. (2012) ‘Toward an ecology of materials’, *Annual Review of Anthropology*, 41, pp. 427–442. doi: 10.1146/annurev-anthro-081309-145920.

Intille, S. S. (2002) ‘Designing a home of the future’, *IEEE Pervasive Computing*, 1(2), pp. 76–82. doi: 10.1109/MPRV.2002.1012340.

Irani, L. C. and Silberman, M. S. (2013) ‘Turkopticon: Interrupting worker invisibility in Amazon Mechanical Turk’, *Conference on Human Factors in Computing Systems - Proceedings*, pp. 611–620. doi: 10.1145/2470654.2470742.

Ishii, H. *et al.* (1998) ‘ambientROOM’, in *CHI 98 Conference Summary on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 173–174. doi: 10.1145/286498.286652.

Ishii, H. (2004) ‘Bottles: A transparent interface as a tribute to Mark Weiser’, *IEICE Transactions on Information and Systems*, E87-D(6), pp. 1299–1311.

Ishii, H., Ren, S. and Frei, P. (2001) ‘Pinwheels: visualizing information flow in an architectural space', *CHI '01 extended abstracts on Human factors in computing systems*, pp. 111–112. doi: 10.1145/634067.634135.

Ishii, H. and Ullmer, B. (1997) 'Tangible bits: Towards seamless interfaces between people, bits and atoms', *Conference on Human Factors in Computing Systems - Proceedings*, (March), pp. 234–241.

Jackson, S. J. (2014) 'Rethinking Repair', *Media Technologies*, pp. 221–240. doi: 10.7551/mitpress/9780262525374.003.0011.

Jacobson, V., Leres, C. and McCanne, S. (1989) 'tcpdump'.

Jarman, R. and Gerhardt, J. (2007) *Magnetic Movie*. Available at: https://semiconductorfilms.com/art/magnetic-movie/.

Jeanneret, C.-E. (1923) *Vers une architecture*. Crès.

Jeffries, S. (2014) 'Ten tips for a better work-life balance', *The Guardian*. Available at: https://www.theguardian.com/lifeandstyle/2014/nov/07/ten-tips-for-a-better-work-life-balance.

Jenkins, T. (2015) 'Designing the "things" of the IoT', *TEI 2015 - Proceedings of the 9th International Conference on Tangible, Embedded, and Embodied Interaction*, pp. 449–452. doi: 10.1145/2677199.2691608.

Jenkins, T. (2017) 'Living apart, together: Cohousing as a site for ICT design', *DIS 2017 - Proceedings of the 2017 ACM Conference on Designing Interactive Systems*, 1, pp. 1039–1051. doi: 10.1145/3064663.3064751.

Jenkins, T. (2018) 'Cohousing IoT: Design prototyping for community life', *TEI 2018 - Proceedings of the 12th International Conference on Tangible, Embedded, and Embodied Interaction*, 2018-Janua, pp. 667–673. doi: 10.1145/3173225.3173244.

Joint Committee on Housing (1948) *Study and Investigation of Housing*. U.S. Government Printing Office.

Junestrand, S. and Tollmar, K. (1999) 'Video mediated communication for domestic environments — architectural and technological design', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 1670(Dahlbom), pp. 177–190. doi: 10.1007/10705432_16.

Kaltheuner, F. (2018) *Privacy is power*, *Politico*. Available at: https://www.politico.eu/article/privacy-is-power-opinion-data-gdpr/.

Kavenna, J. (2019) 'Shoshana Zuboff: "Surveillance capitalism is an assault on human autonomy"', *The Guardian*, 12, pp. 1–8. Available at: https://www.

theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy.

Kay, A. C. (1972) ‘A Personal Computer for Children of All Ages’, in *Proceedings of the ACM Annual Conference - Volume 1*. New York, NY, USA: Association for Computing Machinery (ACM ’72). doi: 10.1145/800193.1971922.

Kidd, C. D. *et al.* (1999) ‘The aware home: A living laboratory for ubiquitous computing research’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 1670(January), pp. 191–198. doi: 10.1007/10705432_17.

Kirk, D. S. *et al.* (2016) ‘Ritual Machines I & II: Making technology at home’, *Conference on Human Factors in Computing Systems - Proceedings*, pp. 2474–2486. doi: 10.1145/2858036.2858424.

Klein, C. (2005) ‘Motion’.

Knell, D. (2012) *The Hack Day Manifesto*. Available at: https://hackdaymanifesto.com/.

Kobie, N. (2019) *The complicated truth about China’s social credit system*, *WIRED*. Available at: https://www.wired.co.uk/article/china-social-credit-system-explained.

Koenig, A. (1995) ‘Patterns and antipatterns’, *Journal of Object-Oriented Programming*. SIGS PUBLICATIONS INC 588 BROADWAY SUITE 604, NEW YORK, NY 10012-5408, 8(1), pp. 46–48.

Koskinen, I. *et al.* (2012) *Design Research Through Practice: From the Lab, Field, and Showroom*. 1st edn. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc.

Kozlowska, H. (2018) *The Cambridge Analytica scandal affected nearly 40 million more people than we thought*, *Quartz*. Available at: https://qz.com/1245049/the-cambridge-analytica-scandal-affected-87-million-people-facebook-says/.

Kozubaev, S. and Disalvo, C. (2019) ‘Spaces and Traces : Implications of Smart Technology in Public Housing’, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1–13.

Laidler, J. (2019) ‘High tech is watching you’, *The Harvard Gazette*. Available at: https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/.

Lapsley, P. (2013) *Exploding the Phone: The Untold Story of the Teenagers and Outlaws who Hacked Ma Bell*. Grove/Atlantic, Incorporated.

Larsson, B. and Zuckschwerdt, C. W. (2012) ‘rtl_433’.

Latour, B. (1987) *Science in Action. How to follow scientists and engineers through society*, *Technology and Culture*. Harvard University Press.

Le, D. (2013) *China employs two million microblog monitors state media say*, *BBC News*. Available at: https://www.bbc.co.uk/news/world-asia-china-24396957.

Lee, D. (2015) *Amazon's 'Dash' buttons explained*. Available at: https://www.bbc.co.uk/news/av/technology-32153581.

Levy, S. (1984) *Hackers: Heroes of the Computer Revolution*. Doubleday.

Levy, S. (2014) 'Hackers at 30: "Hackers" and "Information Wants to Be Free"', *WIRED*. Available at: https://www.wired.com/story/hackers-at-30-hackers-and-information-wants-to-be-free/.

Lewis, R. (2018) 'Alternative Influence: Broadcasting the Reactionary Right on YouTube', *Data & Society*, p. 60. Available at: https://datasociety.net/research/media-manipulation.

Lichstein, H. (1963) 'Telephone hackers active', *The Tech*, 20 November, p. 1. Available at: http://tech.mit.edu/V83/PDF/V83-N24.pdf.

Lodato, T. J. and DiSalvo, C. (2016) 'Issue-oriented hackathons as material participation', *New Media and Society*, 18(4), pp. 539–557. doi: 10.1177/1461444816629467.

Lopez-Neira, I. *et al.* (2019) '"Internet of Things": How Abuse is Getting Smarter', *SSRN Electronic Journal*, pp. 22–26. doi: 10.2139/ssrn.3350615.

Löwgren, J. (2007) 'Inspirational Patterns for Embodied Interaction', *Knowledge, Technology & Policy*, 20(3), pp. 165–177. doi: 10.1007/s12130-007-9029-1.

Löwgren, J. and Stolterman, E. (2007) *Thoughtful Interaction Design: A Design Perspective on Information Technology*. The MIT Press.

Lyon, G. "Fyodor" (1997) 'nmap'.

Ma, Y., Zhou, G. and Wang, S. (2019) 'WiFi sensing with channel state information: A survey', *ACM Computing Surveys*, 52(3). doi: 10.1145/3310194.

MacAskill, E., Thielman, S. and Oltermann, P. (2017) 'WikiLeaks publishes "biggest ever leak of secret CIA documents"', *The Guardian*, pp. 1–4. Available at: https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance.

Mahdawi, A. (2018) 'Is your friend getting a cheaper Uber fare than you are?', *The Guardian*. Available at: https://www.theguardian.com/commentisfree/2018/apr/13/

uber-lyft-prices-personalized-data.

Maloney, D. (2021) *A Smart Light Bulb Running Doom is a Pretty Bright Idea*, *hackaday.com*. Available at: https://hackaday.com/2021/06/15/a-smart-light-bulb-running-doom-is-a-pretty-bright-idea/.

Marcus, A. (2004) 'Patterns within Patterns', *Interactions*. New York, NY, USA: Association for Computing Machinery, 11(2), pp. 28–34. doi: 10.1145/971258.971268.

Markoff, J. (2022) *Whole Earth: The Many Lives of Stewart Brand*. Penguin Publishing Group.

Martinussen, E. S. and Arnall, T. (2009) 'Designing with RFID', *Proceedings of the 3rd International Conference on Tangible and Embedded Interaction, TEI'09*, pp. 343–350. doi: 10.1145/1517664.1517734.

McCarthy, L. (2018) 'Feeling at Home: Between Human and AI', *Immerse*. Available at: https://immerse.news/feeling-at-home-between-human-and-ai-6047561e7f04.

McGuirk, J. (2015) 'Honeywell, I'm Home! The Internet of Things and the New Domestic Landscape', *e-flux*, 64. Available at: http://www.e-flux.com/journal/64/60855/honeywell-i-m-home-the-internet-of-things-and-the-new-domestic-landscape/.

Le Meur, L. (2009) *Save the Rabbit! The Wifi Rabbit Nabaztag just Filed for Bankruptcy Save the Rabbit!*, *Loïc Le Meur Blog*. Available at: https://web.archive.org/web/20090813103457/http://www.loiclemeur.com/english/2009/08/save-the-rabbit-the-wifi-rabbit-nabaztag-just-filed-for-bankruptcy.html.

Meyer, R. (2016) 'The Curious Mystery of the Map in Pokémon Go', *The Atlantic*. Available at: https://www.theatlantic.com/technology/archive/2016/07/where-did-pokemon-go-get-its-map/490799/.

Misra, T. (2019) *When Facial Recognition Tech Comes to Housing*, *citylab.com*.

Morozov, E. (2013) 'The Meme Hustler - The Baffler', *The Baffler*. Available at: http://www.thebaffler.com/salvos/the-meme-hustler.

Morozov, E. (2019) 'Capitalism s New Clothes', *The Baffler*, pp. 1–5. Available at: https://thebaffler.com/latest/capitalisms-new-clothes-morozov.

Mortier, R. *et al.* (2012) 'Control and understanding: Owning your home network', *2012 4th International Conference on Communication Systems and Networks, COMSNETS 2012*. IEEE, pp. 1–10. doi: 10.1109/COMSNETS.2012.6151322.

Mouffe, C. (2000) *The Democratic Paradox*. Verso.

Mouffe, C. (2007) ‘Artistic activism and agonistic spaces’, *Art & Research*, 1(2), pp. 1–5.

Mozer, M. C. (1998) ‘The neural network house: An environment that adapts to its inhabitants’, *American Association for Artificial Intelligence Spring Symposium on Intelligent Environments*, (December), pp. 110–114. doi: SS-98-02/SS98-02-017.

Muncie, J. (1997) ‘How Buildings Learn’. BBC. Available at: https://www.youtube.com/watch?v=AvEqfg2sIH0.

Nardi, T. (2019) *RTL-SDR : Seven Years Later*, *hackaday.com*. Available at: https://hackaday.com/2019/07/31/rtl-sdr-seven-years-later/.

Nardi, T. (2021) *ESP8266 Network Meters Show Off Unique Software*, *hackaday.com*. Available at: https://hackaday.com/2021/08/10/esp8266-network-meters-show-off-unique-software/.

Naughton, J. (2020) *Data protection laws are great. Shame they are not being enforced*, *The Guardian*. Available at: https://www.theguardian.com/commentisfree/2020/may/02/data-protection-laws-are-great-shame-they-are-not-being-enforced.

Neustaedter, C. and Sengers, P. (2012) ‘Autobiographical Design in HCI Research: Designing and Learning through Use-It-Yourself’, in *Proceedings of the Designing Interactive Systems Conference on - DIS ’12*, pp. 514–523. doi: 10.1145/2317956.2318034.

Ng, A. (2019) *Tenants find a win after settlement orders landlords give physical keys over smart locks*, *cnet.com*.

Norman, D. A. (1988) *The Psychology of Everyday Things*. Basic Books.

Norman, D. A. (1998) *The Invisible Computer*. Cambridge, MA, USA: MIT Press.

Nye, D. E. (1992) *Electrifying America: Social Meanings of a New Technology, 1880-1940*. MIT Press.

O’Brien, D. (2004) ‘Life Hacks’.

O’Leary, N. and Conway-Jones, D. (2013) ‘Node-RED’.

O’Reilly, T. (2005) *What is Web 2.0?: Design patterns and business models for the next generation of software*. Available at: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html.

Odom, W. *et al.* (2016) ‘From Research Prototype to Research Product’, *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI ’16*, pp. 2549–2561. doi: 10.1145/2858036.2858447.

Odom, W. *et al.* (2018) 'Attending to Slowness and Temporality with Olly and Slow Game', pp. 1–13. doi: 10.1145/3173574.3173651.

Odom, W. T. *et al.* (2014) 'Designing for slowness, anticipation and re-visitation', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 1961–1970. doi: 10.1145/2556288.2557178.

Ofcom (2007) *The Communications Market : Broadband*. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/16185/broadband_rpt.pdf.

Oliver, J. (2015) *Detect and disconnect WiFi cameras in that AirBnB you're staying in*. Available at: https://julianoliver.com/output/log_2015-12-18_14-39.

Oliver, J., Savičić, G. and Vasiliev, D. (2011) *The Critical Engineering Manifesto*.

Oogjes, D., Odom, W. and Fung, P. (2018) 'Designing for an other Home', *Proceedings of the 2018 on Designing Interactive Systems Conference 2018 - DIS '18*, pp. 313–326. doi: 10.1145/3196709.3196810.

Orpwood, R. *et al.* (2005) 'The design of smart homes for people with dementia - User-interface aspects', *Universal Access in the Information Society*, 4(2), pp. 156–164. doi: 10.1007/s10209-005-0120-7.

Orwell, G. (1949) *Nineteen Eighty-Four*. London: Secker & Warburg.

Owad, T. (2005) 'Tilt Interface', *Make Magazine*, 3, p. 156.

Palmer, M. and West, I. (2016) *Technology in the Country House*. Historic England (Historic England Series).

Pan, Y. and Stolterman, E. (2013) 'Pattern Language and HCI: Expectations and Experiences', *Conference on Human Factors in Computing Systems - Proceedings*, 2013-April, pp. 1989–1998. doi: 10.1145/2468356.2468716.

Parramore, L. (2010) 'Eli Pariser on the future of the Internet', *Salon*. Available at: http://www.salon.com/2010/10/08/lynn_parramore_eli_pariser/.

Patrizio, A. (1999) *DVD Piracy : It Can Be Done*, *WIRED*. Available at: https://www.wired.com/1999/11/dvd-piracy-it-can-be-done/.

Perec, G. (1974) *Species of Spaces and Other Pieces*. Penguin New York.

Peterson, T. F. (2003) *Nightwork A History of Hacks and Pranks at MIT*, *The MIT Press*.

Petsko, G. A. (2011) 'The blue marble', *Genome Biology*, 12(4), p. 112. doi: 10.1186/gb-2011-12-4-112.

Pierce, J. (2014) 'On the presentation and production of design research artifacts in

HCI', pp. 735–744. doi: 10.1145/2598510.2598525.

Pierce, J. (2016) 'Design Proposal for a Wireless Derouter: Speculatively Engaging Digitally Disconnected Space', *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*, pp. 388–402. doi: 10.1145/2901790.2901908.

Pierce, J. and DiSalvo, C. (2018) 'Addressing Network Anxieties with Alternative Design Metaphors', in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 1–13. doi: 10.1145/3173574.3174123.

Pierce, J. and Paulos, E. (2014) 'Counterfunctional things: exploring possibilities in designing digital limitations', *Proceedings of the Designing Interactive Systems Conference on - DIS '14*, 1, pp. 375–384. doi: 10.1145/2598510.2598522.

Plotnick, R. (2018) *Power Button: A History of Pleasure, Panic, and the Politics of Pushing*. The MIT Press. doi: 10.7551/mitpress/10934.001.0001.

Porter, J. (2019) *Netflix records all of your Bandersnatch choices , GDPR request reveals*. Available at: https://www.theverge.com/2019/2/13/18223071/netflix-bandersnatch-gdpr-request-choice-data.

Powell, W. (1971) *The Anarchist Cookbook*.

Railton, A. (1950) 'Push-Button Manor', *Popular Mechanics*, pp. 84–87, 252.

Randall, D. (2003) 'Living Inside a Smart Home: A Case Study', in *Inside the Smart Home*. London: Springer-Verlag, pp. 227–246. doi: 10.1007/1-85233-854-7_12.

Ratto, M. (2011) 'Critical making: Conceptual and material studies in technology and social life', *Information Society*, 27(4), pp. 252–260. doi: 10.1080/01972243.2011.583819.

Reichardt, J. (1978) *Robots: Fact, Fiction, and Prediction*. Thames and Hudson.

Reinert, A. (2011) 'The Blue Marble Shot: Our First Complete Photograph of Earth', *The Atlantic*. Available at: https://www.theatlantic.com/technology/archive/2011/04/the-blue-marble-shot-our-first-complete-photograph-of-earth/237167/.

Reinhardt, P. (2015) *Replacing Middle Management with APIs*. Available at: https://rein.pk/replacing-middle-management-with-apis.

Rodden, T. and Benford, S. (2003) 'The evolution of buildings and implications for the design of ubiquitous domestic environments', *Proceedings of the conference on Human factors in computing systems - CHI '03*, (5), p. 9. doi: 10.1145/642611.642615.

Rogers, Y. (2006) ‘Moving on from Weiser’s vision of calm computing: Engaging UbiComp experiences’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 4206 LNCS, pp. 404–421. doi: 10.1007/11853565_24.

Rogers, Y. (2014) ‘Mindless or mindful technology?’, in *Proceedings of the 2014 ACM SIGCHI symposium on Engineering interactive computing systems - EICS ’14*. New York, New York, USA: ACM Press, pp. 241–241. doi: 10.1145/2607023.2611428.

Rohwedder, C. (2019) ‘A Home Smart System That Helps With Religious Observances’, *Wall Street Journal*, 19 October. Available at: https://www.wsj.com/articles/a-home-smart-system-that-helps-with-religious-observances-11570026331.

Rojas, P. (2004) *The WiFi Lamp*, *Engadget*. Available at: https://www.engadget.com/2004-05-21-the-wifi-lamp.html.

Rose, D. (2014) *Enchanted Objects: Design, Human Desire, and the Internet of Things*. Scribner.

Rosenbaum, R. (1971) ‘Secrets of the Little Blue Box’, *Esquire Magazine*. Available at: http://www.historyofphonephreaking.org/docs/rosenbaum1971.pdf.

Rowling, J. K. (1999) *Harry Potter and the Chamber of Secrets*. London: Bloomsbury.

Russell, B. (1935) *In praise of idleness and other essays*. Simon and Schuster. doi: 10.1016/j.cardfail.2011.01.001.

Rutter, T. (2015) ‘The rise of nudge – the unit helping politicians to fathom human behaviour’, *The Guardian*, pp. 1–5. Available at: http://www.theguardian.com/public-leaders-network/2015/jul/23/rise-nudge-unit-politicians-human-behaviour.

Said, C. (2019) ‘Kiwibots win fans at UC Berkeley as they deliver fast food at slow speeds’, *San Francisco Chronicle*. Available at: https://www.sfchronicle.com/business/article/Kiwibots-win-fans-at-UC-Berkeley-as-they-deliver-13895867.php.

Salmela, J. (2014) *Pi-hole*. Available at: https://pi-hole.net/.

Sanders, E. B. N. and Stappers, P. J. (2014) ‘Probes, toolkits and prototypes: Three approaches to making in codesigning’, *CoDesign*. Taylor & Francis, pp. 5–14. doi: 10.1080/15710882.2014.888183.

Saponas, T. S. *et al.* (2006) ‘The impact of pre-patterns on the design of digital home applications’, *Proceedings of the Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques, DIS*, 2006, pp. 189–198. doi: 10.1145/1142405.1142436.

Schep, T. (2019) *Candle - privacy friendly smart home*. Available at: https://www.

candlesmarthome.com/.

Schmidt, P. and Eno, B. (1975) *Oblique Strategies*.

Schrock, A. R. (2016a) ‘Civic hacking as data activism and advocacy: A history from publicity to open government data’, *New Media and Society*, 18(4), pp. 581–599. doi: 10.1177/1461444816629469.

Schrock, A. R. (2016b) ‘“Hackathons with no hacking”: civic hackathons and the performance of innovation’, *Rethinking the Innovation Economy: Exploring the Future of Technology, Social Inequality, and Creative Labor*.

Schulz, M., Wegemer, D. and Hollick, M. (2017) ‘Nexmon: The C-based Firmware Patching Framework’. Available at: https://nexmon.org.

Schwartz Cowan, R. (1983) *More work for mother: the ironies of household technology from the open hearth to the microwave*. Basic Books.

Scott, J. (2005) ‘UbiComp : Becoming Superhuman’, in *In Proceedings of the UbiComp 2005 Workshop on UbiPhysics*, pp. 2–4.

Serra, R. and Schoolman, C. F. (1973) *Television Delivers People*.

Severance, C. (2013) ‘Bob metcalfe: Ethernet at forty’, *Computer*. IEEE, 46(5), pp. 6–9. doi: 10.1109/MC.2013.159.

Shafer, S. *et al*. (1998) ‘The New EasyLiving Project at Microsoft Research’, *Proceedings of the 1998 DARPA/NIST smart spaces workshop*, pp. 127–130.

Shaw, T. and Bowers, J. (2016) ‘Public Making : Artistic Strategies for Working with Museum Collections , Technologies and Publics . In : International Symposium on Electronic Art . 2015 , Vancouver , Canada : ISEA . Date deposited : Public Making : Artistic Strategies for Working with’.

Shepard, M. (2011) *pwnazon*. Available at: https://github.com/mflint/pwnazon.

Shorter, M. (2019) *Scout*. Available at: https://www.mrshorter.co.uk/work/scout-making-home-data-visible.

Silverstone, R., Hirsch, E. and Morley, D. (1992) ‘Information and Communication Technologies and the Moral Economy of the Household’, *Consuming Technologies: Media and Information in Domestic Spaces*. Edited by Roger Silverstone and Eric Hirsch. Routledge, pp. 15–31.

Simanowski, R. (2011) *Digital Art and Meaning: Reading Kinetic Poetry, Text Machines, Mapping Art, and Interactive Installations*. University of Minnesota Press (Electronic mediations).

Simon, H. (1969) *The Sciences of the Artificial*, *The Sciences of the Artificial*.

Singh, A. (2005) ‘Amstracker’.

Smith, A. (1759) *The theory of moral sentiments*. Penguin.

Smith, G. C. and Tabor, P. (1996) ‘The role of the artist-designer’, in *Bringing design to software*. New York, NY, USA: ACM, pp. 37–61. doi: 10.1145/229868.230031.

Smith, R. L. (1988) *Smart house: the coming revolution in housing*. GP Pub.

Snowden, E. (2014) *Live Q & A with Edward Live Q & A with Edward Snowden*. Available at: https://edwardsnowden.com/asksnowden/.

Sorensen, H. A. (2002) ‘Adblock’.

Space Caviar (ed.) (2014) *SQM, the Quantified Home*.

Speight, A. (2021) ‘The UK’s right to repair law already needs repairing’, *Wired UK*. Available at: https://www.wired.co.uk/article/right-to-repair-uk.

Stafford, T. and Webb, M. (2004) *Mind Hacks: Tips &amp; Tools for Using Your Brain (Hacks)*. O’Reilly Media, Inc.

Standage, T. (2002) *The Mechanical Turk*. Penguin.

Standing, G. (2014) *The Precariat - The new dangerous class*. Amalgam.

Stanford-Clark, A. (1999) *MQ Integrator Pervasive Device Protocol*. Available at: http://stanford-clark.com/MQIpdp/.

Stanford, C. (2017) ‘ikea-tradfri’.

Steenson, M. W. (2009) ‘Problems before patterns: A different look at Christopher Alexander and pattern languages’, *Interactions*, 16(2), pp. 20–23. doi: 10.1145/1487632.1487637.

Sterling, B. (2013) *The Epic Struggle of the Internet of Things*. Strelka Press.

Stolterman, E. (2008) ‘The nature of design practice and implications for interaction design research’, *International Journal of Design*, 2(1), pp. 55–65. doi: 10.1016/j.phymed.2007.09.005.

Stroustrup, B. (1985) *The C++ Programming Language*. Addison–Wesley.

Suchman, L. (1995) ‘Making Work Visible’, *Commun. ACM*. New York, NY, USA: Association for Computing Machinery, 38(9), pp. 56–64. doi: 10.1145/223248.223263.

Suchman, L. A. (2007) *Human-machine reconfigurations: Plans and situated actions*, *Human–Machine Reconfigurations*. Cambridge University Press.

Superflux (2015) *Uninvited Guests*. Available at: https://superflux.in/index.php/work/uninvited-guests/.

Sussberg, J. and Alvarado, D. (2020) *We Are As Gods*.

Tansley, A. G. (1935) ‘The use and abuse of vegetational concepts and terms’, *Ecology*, 16(3), pp. 284–307.

Taylor, A. S. *et al.* (2007) ‘Homes that make us smart’, *Personal and Ubiquitous Computing*, 11(5), pp. 383–393. doi: 10.1007/s00779-006-0076-5.

Taylor, A. S. and Swan, L. (2005) ‘Artful systems in the home’, *CHI ’05 - Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 641–650. doi: 10.1145/1054972.1055060.

Taylor, C. W. (1990) ‘Creating Strategic Visions’. Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a231618.pdf.

Taylor, F. W. (1911) *The Principles of Scientific Management*. Harper (Engineering special collection).

Taylor, N. *et al.* (2021) ‘Prototyping Things: Reflecting on Unreported Objects of Design Research for IoT’, in *Designing Interactive Systems Conference 2021*. New York, NY, USA: ACM, pp. 1807–1816. doi: 10.1145/3461778.3462037.

Taylor, N. and Clarke, L. (2018) ‘Everybody’s Hacking: Participation and the Mainstreaming of Hackathons’, *Proc. of CHI*, pp. 1–12. doi: 10.1145/3173574.3173746.

Thaler, R. H. and Sunstein, C. R. (2008) *Nudge: Improving decisions about health, wealth, and happiness*. Springer.

Tidwell, J. (2005) *Designing Interfaces: Patterns for Effective Interaction Design*. O’Reilly Media.

Tim Harford (2019) *Does pornography still drive the internet?*, *BBC News*. Available at: https://www.bbc.co.uk/news/business-48283409.

Toffanin, P. (2011) *k4freeserver*.

Tolmie, P. *et al.* (2002) ‘Unremarkable computing’, *Conference on Human Factors in Computing Systems - Proceedings*, 4(1), pp. 399–406. doi: 10.1145/503447.503448.

Tolmie, P. *et al.* (2007) ‘Making the Home Network at Home : Digital Housekeeping’, *Proceedings of the Tenth European Conference on Computer Supported Cooperative Work*, (September), pp. 331–350. doi: 10.1007/978-1-84800-031-

5_18.

Torvalds, L. (2005) ‘git’.

Turi, J. (2014) *Popular on Engadget*, *Engadget*. Available at: https://www.engadget.com/2014-07-06-gadget-rewind-2005-nabaztag.html.

Tzapu (2015) ‘WiFiManager’. Available at: https://github.com/tzapu/WiFiManager.

Underkoffler, J. and Ishii, H. (1999) ‘Urp: A luminous-tangible workbench for urban planning and design’, *Conference on Human Factors in Computing Systems - Proceedings*, pp. 386–393. doi: 10.1145/302979.303114.

UNESCO (2019) ‘I’d blush if I could: closing gender divides in digital skills through education’. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000367416.locale=en.

Vallgårda, A. and Redström, J. (2007) ‘Computational Composites’, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery (CHI ’07), pp. 513–522. doi: 10.1145/1240624.1240706.

Vermeren, P. (2005) ‘If you can’t open it, you don’t own it’, *Make Magazine*, 4, pp. 154–157.

Violet Dal, the first “emotional lamp” (2004) *LinuxDevices*. Available at: https://linuxdevices.org/device-profile-violet-dal-the-first-emotional-lamp/.

Voros, J. (2017) *The Futures Cone, use and history*. Available at: https://thevoroscope.com/2017/02/24/the-futures-cone-use-and-history/.

Wakkary, R. *et al.* (2015) ‘Material Speculation: Actual Artifacts for Critical Inquiry’, *Aarhus Series on Human Centered Computing*, 1(1), p. 12. doi: 10.7146/aahcc.v1i1.21299.

Wakkary, R. *et al.* (2017) ‘Morse Things’, pp. 503–514. doi: 10.1145/3064663.3064734.

Wall, C. (1993) ‘Gendering Rooms: domestic architecture and literary acts’, *Eighteenth-Century Fiction*. University of Toronto Press, 5(4), pp. 349–372.

Wallman, J. (2014) *Stuffocation: Living More with Less*. Penguin Books Limited.

Want, R. *et al.* (1992) ‘The Active Badge Location System’, *ACM Transactions on Information Systems (TOIS)*, 10(1), pp. 91–102. doi: 10.1145/128756.128759.

Want, R. *et al.* (1995) ‘An overview of the PARCTAB ubiquitous computing experiment’, *IEEE Personal Communications*, 2(6), pp. 28–43. doi: 10.1109/98.475986.

Weil, D. (1981) ‘Radio in a Bag’.

Weiser, M. (1991) ‘The Computer for the 21st Century’, *Scientific American (International Edition)*, 265(3), pp. 66–75. doi: 10.1038/scientificamerican0991-94.

Weiser, M. (1994a) ‘Creating the Invisible Interface: (Invited Talk)’, in *Proceedings of the 7th Annual ACM Symposium on User Interface Software and Technology*. New York, NY, USA: Association for Computing Machinery (UIST ’94), p. 1. doi: 10.1145/192426.192428.

Weiser, M. (1994b) ‘The World is Not a Desktop’, *Interactions*. New York, NY, USA: Association for Computing Machinery, 1(1), pp. 7–8. doi: 10.1145/174800.174801.

Weiser, M. (1996a) ‘{ Open House }*’, *Interactive Telecommunications Program Review*, 39(March 1996), pp. 1–4.

Weiser, M. (1996b) *Ubiquitous Computing*. Available at: https://web.archive.org/web/19970114044913/http://www.ubiq.com/hypertext/weiser/UbiHome.html.

Weiser, M. and Brown, J. S. (1995) ‘Designing Calm Technology’, *PowerGrid Journal*, pp. 1–5. Available at: https://web.archive.org/web/19970624041814/http://www.powergrid.com/1.01/calmtech.html.

Weiser, M., Gold, R. and Brown, J. S. (1999) ‘The origins of ubiquitous computing research at PARC’, *IBM Systems Journal*, 38(4), pp. 693–696. doi: 10.1147/sj.384.0693.

Which (2020) *Later Life Care*. Available at: https://www.which.co.uk/later-life-care/home-care/technology-to-keep-you-safe/telecare-an4ul6z1bvnl.

Wikipedia contributors (2019) ‘List of Google products’. Available at: https://en.wikipedia.org/w/index.php?title=List_of_Google_products&oldid=924140702.

Willard, N. (2002) ‘Filtering Software: The Religious Connection’, pp. 1–26. Available at: http://www.embracecivility.org/wp-content/uploadsnew/2011/10/FSRCreport.pdf.

Wisneski, C. *et al.* (1998) ‘Ambient displays: Turning architectural space into an interface between people and digital information’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 1370, pp. 22–32. doi: 10.1007/3-540-69706-3_4.

Wisneski, C. A. (1999) ‘The Design of Personal Ambient Displays’, pp. 1–60.

Woodruff, A., Augustin, S. and Foucault, B. (2007) ‘Sabbath day home automation: “it’s like mixing technology and religion”’, *Conference on Human Factors in Computing Systems - Proceedings*, pp. 527–536. doi: 10.1145/1240624.1240710.

Woolf, V. (1929) *A Room of One’ s Own*. London: Hogarth Press. Available at: http://

gutenberg.net.au/ebooks02/0200791.txt.

Wright, J. (2016) ‘Nosedive (Black Mirror: Season 3, Episode 1)’. Netflix.

Yap, J. (2006) *ikeahackers.net*.

Zang, N., Rosson, M. B. and Nasser, V. (2008) ‘Mashups: Who? What? Why?’, in *CHI ’08 Extended Abstracts on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery (CHI EA ’08), pp. 3171–3176. doi: 10.1145/1358628.1358826.

Zenith Radio Corporation (1972) *Zenith Space Command*. Available at: https://www.youtube.com/watch?v=PlgSuaIHYsY.

Zimmerman, J., Forlizzi, J. and Evenson, S. (2007) ‘Research through design as a method for interaction design research in HCI’, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI ’07*. New York, New York, USA: ACM Press (CHI ’07), pp. 493–502. doi: 10.1145/1240624.1240704.

Zimmerman, J., Stolterman, E. and Forlizzi, J. (2010) ‘An analysis and critique of Research through Design: towards a formalization of a research approach.’, *Proceedings of the 8th ACM Conference on Designing Interactive Systems (DIS ’10)*, pp. 310–319. doi: 10.1145/1858171.1858228.

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile.

Appendix

Ethics Application

DEPARTMENT OF DESIGN

RESEARCH ETHICS APPROVAL FORM (Students)

(NOTE: Staff applications are submitted on a different form to the College Research Ethics and Integrity Sub-Committee. See: https://goldmine.gold.ac.uk/PoliciesForms/Documents/Advice and information/Academic Resources/Research and enterprise/ethical-approval-form.doc *)*

This form should be completed for any research project that involves human participants or if the research involves animals or if it may involve environmental harm. The principal investigator or, where the principal investigator is a student, the supervisor, is responsible for exercising appropriate professional overview of the research.

You should:

- first, read and understand the Goldsmiths Code of Practice on Research Ethics: http://www.gold.ac.uk/media/research-ethics.pdf
- then complete and submit this form (if it's incomplete or there are errors, there'll be delays)
- then, wait for approval before contacting any potential participants in any research.

Section One Applicant Details

1.1 Name of researcher	David Chatting
1.2 Status (undergraduate student, postgraduate student)	Postgraduate student (PhD)
1.3 Goldsmiths email address	david.chatting@gold.ac.uk
1.4 Contact address	Interaction Research Studio, 6th Floor, Ben Pimlott Building, Goldsmiths, New Cross, London, SE14 6NW.
1.5 Contact phone number	07747 602974

Section Two Programme information

2.1 Programme & Programme leader	Fulltime PhD in Design. Supervised by Bill Gaver and Andy Boucher.
2.2 Module & Module leader	
2.3 Name of the Design Department member of staff supervising your research project	

Section Three Project Details

3.1 Project title:

A Design Led Exploration of Home Networks

3.2 *Brief* outline of the project, including its purpose:

My PhD research is a design-led exploration of the Smart Home and the Internet of Things (IoT) devices that increasingly constitute it; questioning how these systems impact the agency of those who live precariously there – typically those who rent their homes. There are two primary activities for which I am seeking ethical approval:

i) A small workshop hosted at my house engage professional designers to explore the technical possibilities that exist in the home network. This preliminary study will inspire my future design work. Proposed for Autumn 2018.

ii) A short "Cultural Probes" study and interview with up to a dozen households who privately rent their homes. A probe pack will be delivered to the household, containing exercises and instruments to record both their experiences of renting and their understanding of their home network, a week prior to an audio recorded interview with the researcher (typically one hour in duration). This will provide an ethnographic account of current practice and will inspire my future design work. It is hoped that relationships built with participants at this stage of the work will allow further collaboration in a later design phase. This study is proposed for Autumn 2018.

The workshop should present few ethical concerns. However, it is unusual in a number of respects that warrant some reflection. Firstly, being in a private space – a rented flat – it has an up-to-date set of safely certificates, evacuation procedures and insurances. The participants will be made aware of these. Secondly, being my own home there is a risk to my own safety or privacy. All the participants will already be known to me professionally and socially, so that we have a trusting relationship. Thirdly, elements of hacking practice are illegal when exercised against a third-party's property – here the focus is my private home network. Fourthly, in catering for my participants I will mitigate any allergies or intolerances they might have.

The protocol for a Cultural Probes study is well established by the Interaction Research Studio and personally through my previous work at Newcastle University (the Family Rituals project). By its nature it will produce a set of responses that are personal to the participants and adequate security and anonymousation will be required. Some of the probe materials will be electronic devices and participants will need instruction on their use. For home visits the researcher will operate with their personal safety in mind.

3.3 *Brief* description of methods of data collection/activity:

The purpose of the workshop is to create a series of prototypes and speculations using the devices to be found on my home network (televisions, Wi-Fi lights, etc.). These will be documented through shared computer code, photography and video. We will also make notes and sketches.

Participants of the probes study will receive a probe pack to complete a week in advance of an interview. The probe pack will containing exercises and instruments to record both their experiences of renting and their understanding of their home network – this will be a mixture of writing, drawing and photography that relate to their relationship to their rented property and their WiFi network. The instruments will allow them to measure features of their network: signal strength, the busyness of the network at different time and the actions of IoT devices. The interview will between the researcher and as many members of the household as practicable, it will focused on reviewing the probe returns and the instrument findings. It is anticipated that the interview will last for one hour. This will provide an ethnographic account of current practice and will inspire my future design work (beyond this initial study).

3.4 Where will the data collection be undertaken?

One-day Design Workshop at the researcher's home.

The probes study will take place at the participants' homes.

Section Four Human participants

4.1 How many and what type of participants are involved in the research? Workshop: Six professional designers. Probe study: Six to twelve households who are privately renting their homes. These will be selected to represent an interesting diversity of arrangements from family units to home-mates, across a range of ages.
4.2 How will the participant(s) be recruited? *(Attach copies of any recruiting materials if used).* Workshop: Participants will be recruited by word of mouth. Given the private nature of my home, they will be all known to me and be people I have an existing professional and social relationship with. Probe study: Participants will be recruited by word of mouth and advertisement – using the attached flyer (probes-recruitment.pdf). To protect myself I will only disclose my email address at this stage of the process; no telephone numbers or physical addresses.
4.3 How will the participant(s) consent be obtained? *(Include a copy of any proposed consent materials).* All participant in both activities will need to give informed written consent – using the attached forms.

Insert ✓	Y	N
4.4 Will it be necessary for participants to take part in the study without their knowledge and consent at the time? (e.g. covert observation of people in non-public places)		✓
4.5 Is there any deception involved?		✓
4.6 Will the participant(s) be paid or rewarded?		✓
4.7 Will the participant(s) be fully informed about the nature of the project and of what they will be required to do? *(Attach any associated materials.)*	✓	
4.8 Will the participant(s) be told they can, if they wish, withdraw from participation at any time and that they do not need to give a reason for doing so? (*Attach any associated materials.)*	✓	
4.9 If you have ticked a box marked * please give the question number/s and fuller information here:		

Section Five Persons who are young, vulnerable or in legal custody

Insert ✓	Y	N
5.1 Will any persons who are: young (under the age of 18 years); vulnerable (e.g. with learning difficulties or with severe cognitive disability); or, in legal custody be involved in the research? ***If NO, go to Section Six. If YES please complete this section*.**	✓	
5.2 How will consent be given (i.e. from the participant themselves or from a third party such as a parent or guardian) and how will agreement to the research be asked for? (*Attach any associated materials.)* Please see attached information sheets and contest forms for both activities (probes-participants-sheets.pdf and workshop-participants-sheets.pdf)		
Insert ✓	Y	N
5.3 If you are conducting research with young persons under the age of 18 years or 'vulnerable persons' do you have Disclosure and Barring Service (DSB) clearance? Please see attached DBS certificate (dbs-chatting.pdf)	✓	
5.4 Will face-to-face interviews or observations or experiments be overseen by a third party (such as a	✓*	

teacher, care worker or prison officer)? Parent or guardian		
5.5 Is it possible that the research might disclose information regarding child sexual abuse or neglect? *(If yes, indicate how such information will be passed to the relevant authorities (e.g. social workers, police), but also indicate how participants will be informed about the handling of such information were disclosure of this kind to occur. A warning to this effect must be included in the consent form if such disclosure is likely to occur.)*	*	✓
5.6 If you have ticked a box marked * please give the question number/s and fuller information here: The probes study may include children under the age of 18, they will not be the primary respondents or be interviewed individually, however they may have some participation in both – accompanied at all times by their parents or guardians. Although highly unlikely, should evidence of child sexual abuse or neglect become evident I would immediately contact the police/social services as appropriate. The workshop is only with adults.		

Section Six Participants' personal data

Insert ✓	Y	N
6.1 Will personal data of any kind (including digital and images) be gathered on participants? ***If NO go to Section Seven. If YES, complete this Section.***	✓	
6.2 Will the data be anonymous?	✓	
6.3 Will the data be treated confidentially?	✓	
6.4 Will the study involve discussion of topics sensitive to the participants (e.g. religious or culturally sensitive issues, sexual activity, drug use)?		✓

6.5 Where will the data be stored and what security be applied to it?

The data (audio recording, digital photographs/video that include images of the participants) will be stored on an encrypted hard drive, kept securely at Goldsmiths. Physical materials (such as probe returns) and Consent Forms the will also be kept securely (in a locked filing cabinet) on campus at Goldsmiths. Data shall be kept for the shortest possible time on any personal device (always encrypted) and transferred to a Goldsmiths secure hard drive as soon as possible.

6.6 How long will the data be stored and how will it be eventually destroyed?

The data will be stored for 10 years before the hard disk is re-formatted. Physical materials will be shredded and destroyed after this time period.

6.7 If you have ticked a box marked * please give the question number/s and fuller information here:

The identity of participants be anonymous by default in subsequent reports of either study, their name will be replaced by a pseudonym and their likeness disguised in any photographs or video.

For the workshop, the design work produced by the participants is not considered to be personal data. However, participants can also elect to be anonymous in this regard. There may be concerns about Intellectual Property. Participants will aware that the Intellectual Property of what they produce remains their own. Anything they choose to document (by sharing computer code, images or video) and uploading it to the workshop repository might then be use in my subsequent design work, for which they can be credited in a manner of their choosing.

For the probe study the instruments have been designed such that they do not retain any of the data they collect from the network. Rather the instruments present data in ways that allows the participants to reflect on it and recount this through their notes and their recall of these experiences in the interview.

The data will be stored for at most 10 years.

Section Seven Risk and Duty of Care issues

Insert ✓	Y	N
7.1 Will the research involve the investigation of illegal conduct?		✓
7.2 Are there any potential adverse consequences to the participant(s), or any other person?		✓
7.3 Are there any procedures which may cause discomfort, distress or harm to the participant(s), or any other person?		✓
7.4 Will the research place you in situations of harm, injury or criminality?		✓
7.5 Have you any special personal considerations or vulnerabilities that might influence your safety while carrying out fieldwork (injuries, disabilities, allergies, asthma, personal conflicts with informants/community etc.).	✓	

For visits to participants' homes, I will inform a colleague where I am going, for how long, and that I have returned safely.		
7.6 Might the research cause harm to those represented in it?		✓
7.7 Will the research involve any animal subjects?		✓
7.8 Will the research cause any environmental harm?		✓
7.9 Are drugs, placebos or other substances (e.g. food substances, vitamins) to be administered to the study participants or will the study involve invasive, intrusive or potentially harmful procedures of any kind?		✓
7.10 Will blood or tissue samples be obtained from participants?		✓
7.11 Is pain or more than mild discomfort likely to result from the study?		✓
7.12 Could the study induce psychological stress or anxiety or cause harm or negative consequences beyond the risks encountered in normal life?		✓
7.13 Will the study involve prolonged or repetitive testing?		✓
7.14 Do you know of any other potential developments arising from this research that may lead to ethical, health, safety, risk, harm, or duty of care concerns?		✓
7.15 If you have ticked a box marked * please give the question number/s and fuller information here: For the workshop, elements of hacking practices are illegal, but here the focus is on the investigator's private home network and participants will be instructed to work only with these devices. For catering participants will be asked to declare any allergies or intolerances prior to the event.		

Section Eight **Other matters**

Insert ✓	Y	N
8.1 Are there any conflicts of interest regarding the investigation and dissemination of the research (e.g. with regard to compromising independence or objectivity due to financial gain)?		✓
8.2 Is the research likely to have any negative impact on the academic status or reputation of the College?		✓
8.3 Is data to be collected from an institutional location (such as a school, prison, hospital)? *If so, attach evidence of agreement obtained from the relevant authority (e.g. Head Teacher, Local Education Authority, Home Office)?*		✓
8.4 If you have ticked a box marked * please give the question number/s and fuller information here:		

Section Nine **Attachments, signatures and submission**

Wherever possible, applications will be dealt with within two weeks of receipt. Delays will occur if the application has not been carefully completed. The decision regarding your application for ethical approval will be communicated to you and your supervisor (if applicable) directly.

You should now complete the following checklist, supply any necessary signatures and submit the full application/documentation to the Department Ethics Contact (Steve Keirl s.keirl@gold.ac.uk).

9.1 Attachment checklist:

Have you attached copies of all supporting materials? Please indicate which and insert ✓ in the appropriate column

Document	Not applicable	Attached
Recruitment document/s		✓
Informed consent materials		✓
Other information for participants		✓
Consent agreements for young, vulnerable or ‘in custody’ persons		✓
Disclosure and Barring Service (formerly Criminal Records Bureau) Check		✓
Institutional location agreement	✓	
Other *(please specify)...*	✓	

9.2 To be completed by student applicants…

Please note that your Supervisor and the Department Ethics Contact should be notified of any adverse or unforeseen circumstances arising out of this study. They should also be notified of any significant changes to the research design regarding research ethics.

Signature of Applicant

Date

24th October 2018

9.3 To be completed by Principal Supervisor…

Please note that the Department Ethics Contact should be notified of any adverse or unforeseen circumstances arising out of this study or of any emerging ethical concerns that the Supervisor may have about the research once it has commenced.

Insert ✓	Y	N
Has the student read and understood the Goldsmiths Code of Practice on Research Ethics?	✓	
Has there been appropriate discussion of the ethical implications of the research with you as Supervisor?	✓	
Are the ethical implications of the proposed research adequately described in this application?	✓	
Please add any other comments you wish to make here: Dave is an experienced researcher with a strong commitment to ethical research. This is reflected by his disclosure of the potential illegality of some of the hacking practices that might be used in his workshop: As he writes, using these on his own personal home network is not a problem, but it is commendable that he exposes the issue for review.		

Signature of Principal Supervisor

Date

24 October 2018

10 Ethical Approval

This project has been considered using agreed Departmental procedures and is now approved. This approval is valid for a maximum period of three year/s.

Signed S. Keirl

Date 25th October 2018

Print Name Steve Keirl

Department Ethics Contact

Design: R&E Ethics v8 2016-17

Patterns for a Network of One’s Own

This appendix describes 30 patterns for a *network of one’s own*, or rather 30 patterns that relate to a *network of one’s own*, where some are in fact counter patterns. The intention is to allow a reader with a design purpose to navigate these linked patterns, rather than being read in a linear undirected way. Some patterns are implied and only named, as yet unresolved, they are highlighted to offer starting points for further work.

The ordering and numbering does not imply a hierarchical containment but does indicate a scale and degree of abstractness that allows the patterns to be grouped into broad thematic sets. Patterns that are derived from Alexander’s *A Pattern Language* (Alexander *et al.*, 1977) retain their relative order and his original numbering is shown in brackets.

The Internet
1. The Internet
2. The Cloud

The Home
3. Tenancy
4. Your Own Home (79)

Ways of Being Seen
5. Incremental Intimacy Gradient (127)
6. Invisible Work
7. Visible Work
8. Panoptical Surveillance Capitalism

Computing Paradigms
9. Ubiquitous Computing
10. Virtual Reality
11. Mindful Computing
12. Goldberg Machines

Networked Homes
13. A Network of One’s Own (141)
14. The Home WiFi Router
15. Reception Welcomes You (149)
16. Wide Area Network

Boundaries
17. The Shape of Space (191)
18. Pliable Walls (197)
19. Front Door Bench (242)
20. Positioning, Ranging and Boundary Making

Stuff
21. Nomadic Furniture
22. Stuff from Your Life (253)

Designs
23. Voice Assistant
24. Amazon Dash Button
25. Dolmio Pepper Hacker
26. Pi-hole
27. The Approximate Library

Technical Acts
28. Rogue Access Point
29. DNS Redirect
30. WiFi Deauthentication

1. The Internet

Worldwide Networks of Networks

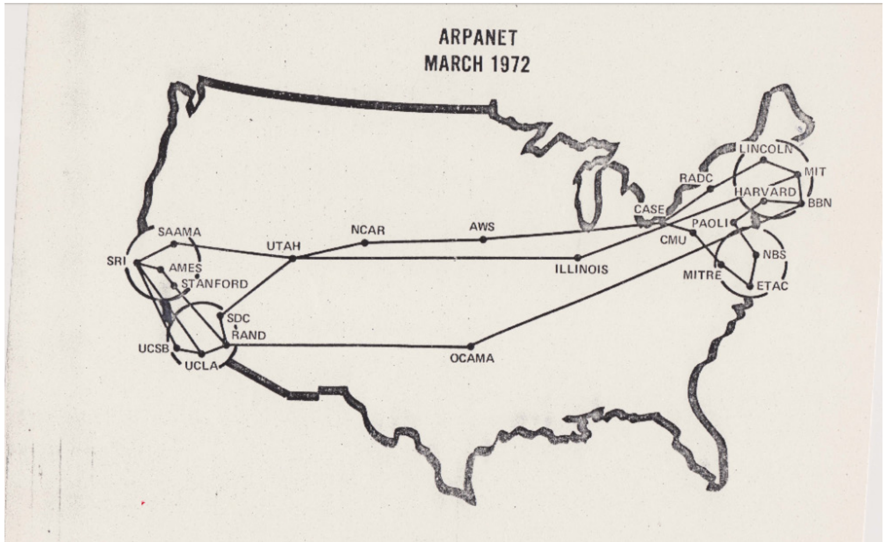


Figure 87. ARPANET March 1972.
© UCLA Library Digital Collections. Used under license, CC-BY-4.0.

The Internet is a worldwide network of interoperating networks, dependant on a set of open standardised technologies, that include packet-switched TCP/IP for routing and addressing, DNS for lookup and HTTP for delivery. These technologies were designed for resilience and with a spirit of optimism. Strictly HTTP is a technology of the World Wide Web, but this pattern knowingly conflates the Internet and World Wide Web (at least what might be considered Web 1.0). As such it encodes the intentions of engineers who considered that information should be free and might identify with Levy's hackers (Levy, 1984). At its technological core this pattern of the Internet persists – despite the counter logics of *The Cloud*.

While the Internet allows the connection of arbitrary devices across distance and political boundaries, the constituent networks have their own properties (for instance, speed and latency), ownership and policies (for instance, the *Great Firewall* of China). In this respect the Internet easily accommodates *A Network of One's Own.* Each network was built and is maintained in a piecemeal fashion, often with the foundation of a previous network (for instance, wired telephone networks).

The Internet is not the only architectural pattern for large data networks, consider dial-up bulletin boards like the WELL and the French Minitel system.

Related Patterns

2. The Cloud
13. A Network of One's Own (141)

Implied Patterns

The Telephone Network
Bulletin Boards

References

Levy, S. (1984) *Hackers: Heroes of the Computer Revolution*.

2. The Cloud

The Internet as a Service

Figure 88. The Cloud. © Shutterstock. Used under license.

The Cloud is the conceptualisation of the Internet as a service, broadly the social and commercial web, that might be characterised as Web 2.0. Some services (like Netflix) are subscription-based, others are apparently free (like Facebook) and rely on advertising models. This Internet is often mis-conceptualised as a pipe from which we simply consume.

Central to the notion of the Cloud is the client–server network architecture, where the client requests content from the server. Unlike the consumption of traditional broadcast television and radio, information flows in both directions. Furthermore, a set of authentication, tracking and payment technologies identify the actions of individual clients; these include HTTPS, web cookies and databases. These reciprocal transactions leave a trace at the server – which *Panoptical Surveillance Capitalism* can then exploit.

The Cloud assumes an asymmetry of consumption and production in which a powerful server owns and controls valuable content and services; and in which clients download more data than they uploaded. Peer-to-peer networking suggests a more symmetric pattern.

Metaphorically, the Cloud diverts attention away from the material reality of networks and servers; it suggests the Internet is but one ubiquitous entity – experienced only from the periphery. Technically, the Cloud is reliant on well-defined web-APIs (Application Programming Interfaces) of which clients make requests for resources using technologies like HTTP and HTTPS. This defines an interface of what is seen and unseen – and implies the doing of *Invisible Work.*

In many respects the Cloud is a counter pattern to the Internet, despite their shared technical foundations.

Related Patterns

1. *The Internet*
6. *Invisible Work: Hidden Servants*
8. *Panoptical Surveillance Capitalism*
9. *Ubiquitous Computing*

Implied Patterns

Broadcast Media
Client-Server Architecture
Peer-to-Peer Architecture

3. Tenancy

Using but not Owning

Figure 89. Tenancy. © Shutterstock. Used under license.

Tenancy is a counter pattern to *Your Own Home* which describes occupancy through contractual payments to a landlord, where one does not own the property. While it evidently describes housing, it also defines more general short-term arrangements of services and users, with forms of rental and subscription payment.

Tenancy implies an ownership only of one's own *stuff*, that inhibits change or maintenance of the slower infrastructural layers by the tenant (Brand, 1995) – see *Pliable Walls*. Coupled with short-term tenancy agreements and temporary employment, this experience can be one of a good deal of precarity (Standing, 2014).

With respect to the domesticated Internet, rental models extend to the consumption of services, regardless of housing arrangements. Netflix is a clear example with a monthly subscription model. Less obviously, some of the stuff one might expect to own, like photograph albums and music collections, have also been transformed into rented services in *The Cloud*. When one's remaining physical stuff becomes entangled in the Internet of Things, their ownership and operation also becomes contested and precarious. In sum, especially for a renter, *The Stuff from Your Life*, of which you have direct ownership and control, becomes diminished. The *Nomadic Furniture* pattern suggests some responses.

While housing tenancy is defined by legal documents and clear exchanges, many cloud services are apparently free or innocuously supported by advertising. The *Panoptical Surveillance Capitalism* pattern suggests this can be far more insidious.

Nonetheless, while you may not own your home, it is possible you can still assert *A Network of One's Own*.

Related Patterns

2. The Cloud
4. Your Own Home (79)
8. Panoptical Surveillance Capitalism
13. A Network of One's Own (141)
18. Pliable Walls (197)
21. Nomadic Furniture
22. The Stuff from Your Life (253)

Implied Patterns

Internet of Things

References

Brand, S. (1995) 'How Buildings Learn: what happens after they're built', *Penguin Books*, p. 720. doi: 10.2307/990971.

Standing, G. (2014) *The Precariat - The new dangerous class*. Amalgam.

4. Your Own Home (79)

A Home You Own

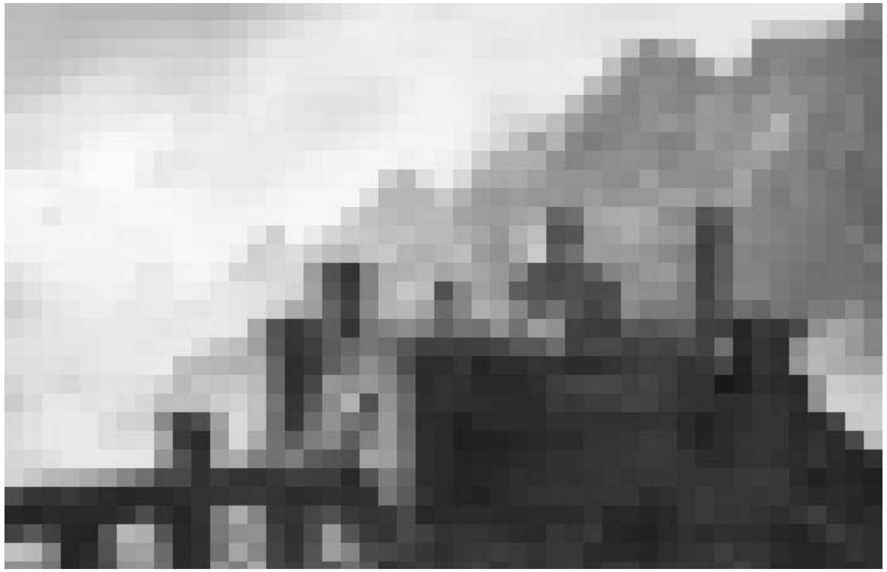


Figure 90. "Fortify your home" advertisement. © BT, 2018. Redacted.

Your Own Home is an appropriation of Alexander's unequivocal pattern of the same name:

> *People cannot be genuinely comfortable and healthy in a house which is not theirs. All forms of rental — whether from private landlords or public housing agencies — work against the natural processes which allow people to form stable, self-healing communities.*
>
> *(Alexander et al., 1977, pp. 392–397)*

Your Own Home clearly resonances with the castle doctrine (Coke, 1644), an Englishman's Home is his castle, Bey's Pirate Utopia (Bey, 1991) and Chesterton's wildness of domesticity (Chesterton, 1912). It implies both an ownership and the ability to enact change, independently from the outside world. To live privately as one chooses, be that motivated by values, politics, or religious practice – beyond the gaze of others, behind closed doors (*Incremental Intimacy Gradient*). However, for those inside the home, this might imply struggles of individual expression, parental authority, assumed gender roles or even domestic abuse.

The *Network of One's Own* pattern expresses Your Own Home with respect to the network.

Your Own Home suggests *Tenancy*, a counter-pattern that captures the reality of renting and degrees of precarity in a home you don't own.

Related Patterns

1. The Internet
3. Tenancy
5. Incremental Intimacy Gradient (127)
13. A Network of One's Own (141)

Implied Patterns

Pirate Utopia

References

Bey, H. (1991) *T.A.Z.: The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism*. Autonomedia (New autonomy series).

Chesterton, G. K. (1912) *What's Wrong with the World?*

Coke, E. (1644) *The Third Part of the Institutes of the Laws of England: Concerning High Treason, and Other Pleas of the Crown, and Criminal Causes*.

5. Incremental Intimacy Gradient (127)

Degrees of Privateness

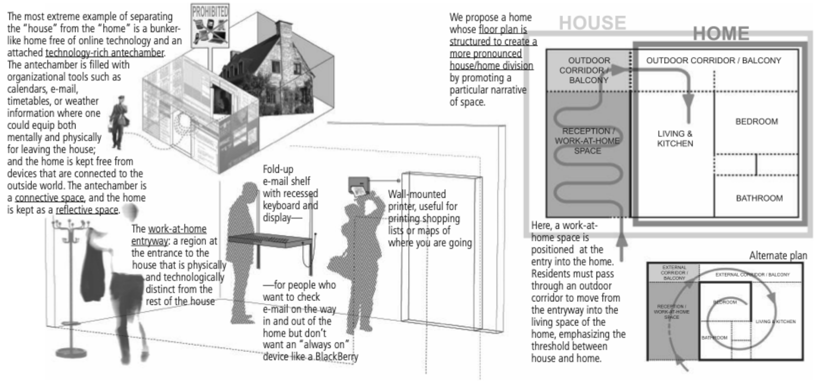

The most extreme example of separating the "house" from the "home" is a bunker-like home free of online technology and an attached technology-rich antechamber. The antechamber is filled with organizational tools such as calendars, e-mail, timetables, or weather information where one could equip both mentally and physically for leaving the house; and the home is kept free from devices that are connected to the outside world. The antechamber is a connective space, and the home is kept as a reflective space.
PROHIBITED
The work-at-home entryway: a region at the entrance to the house that is physically and technologically distinct from the rest of the house
Fold-up e-mail shelf with recessed keyboard and display—
—for people who want to check e-mail on the way in and out of the home but don't want an "always on" device like a BlackBerry
Wall-mounted printer, useful for printing shopping lists or maps of where you are going
We propose a home whose floor plan is structured to create a more pronounced house/home division by promoting a particular narrative of space.
HOUSE
HOME
OUTDOOR CORRIDOR / BALCONY
OUTDOOR CORRIDOR / BALCONY
RECEPTION / WORK-AT-HOME SPACE
LIVING & KITCHEN
BEDROOM
BATHROOM
Here, a work-at-home space is positioned at the entry into the home. Residents must pass through an outdoor corridor to move from the entryway into the living space of the home, emphasizing the threshold between house and home.
Alternate plan
EXTERNAL CORRIDOR / BALCONY
EXTERNAL CORRIDOR / BALCONY
RECEPTION / WORK-AT-HOME SPACE
BEDROOM
LIVING & KITCHEN
BATHROOM

Figure 91. Heterogeneous Home. © Ben Hooker, 2008. Used with permission.

Incremental Intimacy Gradient is a recontextualisation of Alexander's pattern Intimacy Gradients.

> *Unless the spaces in a building are arranged in a sequence which corresponds to their degrees of privateness, the visits made by strangers, friends, guests, clients, family, will always be a little awkward.*
>
> *(Alexander et al., 1977, pp. 610–613)*

An Incremental Intimacy Gradient as an architectural pattern is very relatable to privacy in *Your Own Home.* The notion of a private room or *Network of One's Own*, implies some situation with degrees of communal space and a more public world beyond. The architectural or technical structures that define this gradient, limit the gaze of others, creating intimate private spaces behind closed doors.

An Incremental Intimacy Gradient can be easily read into the Heterogeneous Home proposals (Aipperspach, Hooker and Woodruff, 2008) which suggests ways to design with the architecture and the network – see Figure 94. This references Alexander's later work (Alexander, 2002).

This pattern allows a range of other intimacy gradients to be considered in network terms; *Panoptical Surveillance Capitalism* with a gradient of zero, as well as cliff face gradients – like Bey's Pirate Utopia.

Related Patterns

3. Your Own Home (79)
6. Panoptical Surveillance Capitalism
13. A Network of One's Own (141)

Implied Patterns

Pirate Utopia
Heterogeneous Home
Homogeneous Home

References

Aipperspach, R., Hooker, B. and Woodruff, A. (2008) 'The Heterogeneous Home', in *UbiComp 2008: Ubiquitous Computing*, pp. 222–231. doi: 10.1145/1409635.1409666.

Alexander, C. (2002) *The Nature of Order: The process of creating life*. Center for Environmental Structure (Center for Environmental Structure series).

Bey, H. (1991) *T.A.Z.: The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism*. Autonomedia (New autonomy series).

6. Invisible Work

Hidden Servants

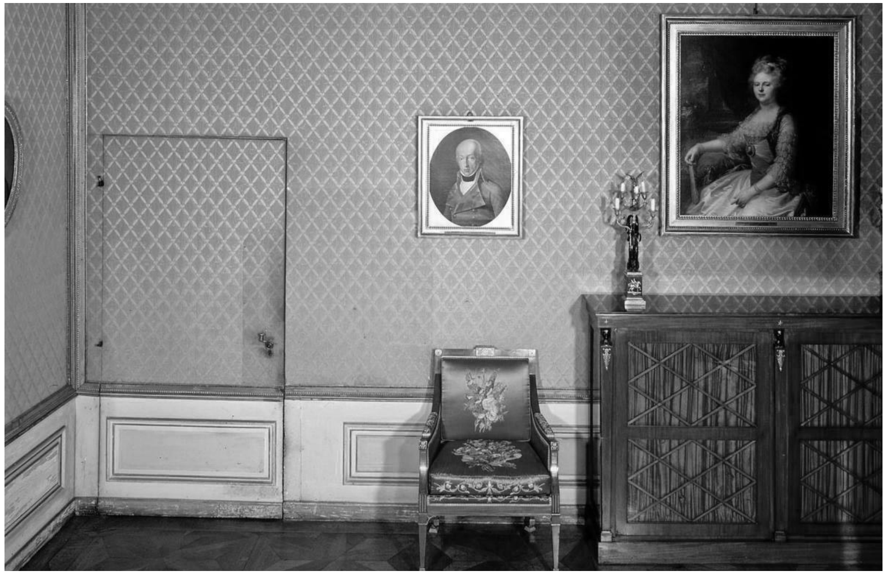


Figure 92. Hidden Servants.
© Landesmedienzentrum Baden-Württemberg / Dieter Jaeger, c1980. Used under license.

Invisible Work seeks to hide all but the products of work for those who initiate and consume it – the complex network of people and resources implicated is unseen. The rendering of work to be invisible is motivated by ideas of convenience and simplicity for the master, where servants are hidden *below stairs* – see Mr Mathias' *Push-Button Manor* (Railton, 1950). However, this very invisibility of consequence may instead diminish a sense of mastery. This is explicitly a counter pattern to *Visible Work*.

The Invisible Work pattern is encoded in much of the practice and teaching of engineering and HCI, where well-specified but complex functions are enclosed inside uninspected black boxes. Indeed, for software engineering, this is echoed by the Gang of Four's facade pattern (Gamma *et al.*, 1994, pp. 185–193). For distance spanning networks like the Internet or the electricity grid, this approach can seamlessly implicate global work and resources – that become considered as services or utilities. From the point of consumption it may be unclear if the work has been remotely accomplished by a machine or a person engaged in Ghost Work (Gray and Suri, 2019).

Invisible Work is well suited to work that can be contractualised. Consider the action of pressing an Amazon's Dash Button and having washing powder delivered by a driver within a few hours. For the cloud such contracts are defined by APIs (Application Programming Interface) putting global human and machine resources under the command of the programmer.

Related Patterns

2. The Cloud
7. Visible Work
24. Amazon's Dash Button

References

Daniels, A. K. (1987) 'Invisible Work', *Social Problems*, 34(5), pp. 403–415.

Gamma, E. *et al.* (1994) *Design Patterns: Elements of Reusable Object-Oriented Software*. Pearson Education (Addison-Wesley Professional Computing Series).

Gray, M. L. and Suri, S. (2019) *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass*. HMH Books.

Railton, A. (1950) 'Push-Button Manor', *Popular Mechanics*, pp. 84–87, 252.

7. Visible Work

Seeing Complexity

Figure 93. Road Works. © Shutterstock. Used under license.

Visible Work seeks to make work and the use of resources legible and consequential of action. It is explicitly a counter pattern to *Invisible Work*, so rather than enclosing work inside well-specified, black-boxed services, visible work is more disruptive, less contractual, and more accountable. This pattern is counter to much of the practice and teaching of engineering and HCI – it is a fundamentally different approach, where complexity must be addressed and not ignored.

Visible Work can be straightforwardly read in the terms of DiSalvo's Adversarial Design, that one must *reveal the hegemony* (DiSalvo, 2012) which practical suggest forms of visualisation that show how the network and its ecology is worked. However, as Haraway might warn, one can only construct a partial knowledge (Haraway, 1988) rather than truly reveal the hegemony and show the work in every black box. The question is then what work can you choose to make visible and what is purposefully or necessarily made invisible?

Relatedly, Matthew Chalmers' advocation of *seamful design* (Chalmers and MacColl, 2003) seeks to design with the technical limitations of the system, making its seams visible. This builds on Mark Weiser's *Ubiquitous Computing* concept of *beautiful seams* (Weiser, 1994a). Visible Work goes beyond this, suggesting that some work should be visible not for simple pragmatic interactional reasons, but rather to practice a politics and engage in a struggle. This has some resonance with James Auger's Reconstrained Design, which seeks to "*encourage more inclusive, holistic, and environmentally responsible futures.*" (Auger, Hanna and Encinas, 2017, p. 2).

The *Mindful Computing* pattern suggests some calm ways to see complexity and the *Goldberg Machines* pattern offers practical ways to approach Visible Work.

Related Patterns

8. Invisible Work
9. Ubiquitous Computing
11. Mindful Computing
12. Goldberg Machines

References

Auger, J., Hanna, J. and Encinas, E. (2017) 'Reconstrained Design: Confronting Oblique Design Constraints', *Nordes*, 7(June).

Chalmers, M. and MacColl, I. (2003) 'Seamful and Seamless Design in Ubiquitous Computing', Workshop At the Crossroads: The Interaction of HCI and Systems Issues in UbiComp., (January), p. 8. doi: 10.1.1.104.9538.

DiSalvo, C. (2012) *Adversarial Design*. The MIT Press.

Haraway, D. (1988) 'Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective', *Feminist Studies*, 14(3), p. 575. doi: 10.2307/3178066.

Weiser, M. (1994) 'Creating the Invisible Interface: (Invited Talk)', in *Proceedings of the 7th Annual ACM Symposium on User Interface Software and Technology*. New York, NY, USA: Association for Computing Machinery (UIST '94), p. 1. doi: 10.1145/192426.192428.

8. Panoptical Surveillance Capitalism

All Watched Over by Machines of Loving Grace

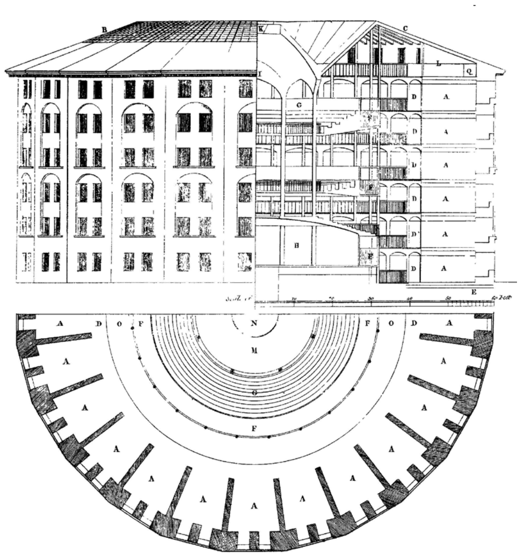


Figure 94. Bentham's panopticon prison. © Willey Reveley, 1791. In public domain.

The Panoptical Surveillance Capitalism pattern is suggested by Shoshana Zuboff's explanation of the bewildering activities of the largest *cloud* companies – namely: Facebook, Amazon, Netflix and Google (Zuboff, 2019). Zuboff suggests this is nothing less than a restructuring of Capitalism – where instead of the *free market* operating to set a price by the complex unknown forces of supply and demand, these companies can instead know, predict and manipulate the motivations of each individual actor in the market – to set the maximum price and so profit. This is dependent on multifactored real-time surveillance of large populations using homogeneous services, producing *big data* and driving machine learning algorithms, through which individuals are laid bare. The domesticated Internet infused into everyday things becomes an intimate source of data. Such panoptical surveillance would be familiar to Jeremy Bentham, as would its consequent limits on private forms of expression (Bentham, 1791). This pattern does not represent a *Network of One's Own*, but as Zuboff puts it, "*an assault on human autonomy*" (Kavenna, 2019).

Panoptical Surveillance Capitalism is not the utter dissolution of privacy, where there is no *intimacy gradient* whatsoever and everything is cast into the public gaze. It is also not politically motivated as state surveillance. Instead, it is the privatisation and the consequent exploitation of homelife, by whatever means the algorithm determines – "*all watched over by machines of Loving Grace*" (Brautigan, 1967). Whether or not Zuboff's analysis is correct, this is a plausible pattern, where corporate interests gaze directly into the home.

Related Patterns

2. The Cloud
5. Incremental Intimacy Gradient (127)
13. A Network of One's Own (141)
23. Voice Assistants

Implied Patterns

Free Market
Surveillance State

References

Bentham, J. (1791) *Panopticon Or the Inspection House*. T. Payne (Panopticon Or the Inspection House).

Brautigan, R. (1967) *All Watched Over by Machines of Loving Grace*. Communication Company.

Kavenna, J. (2019) ‘Shoshana Zuboff: “Surveillance capitalism is an assault on human autonomy”’, *The Guardian*, 12, pp. 1–8. Available at: https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile.

9. Ubiquitous Computing

Computers in the World

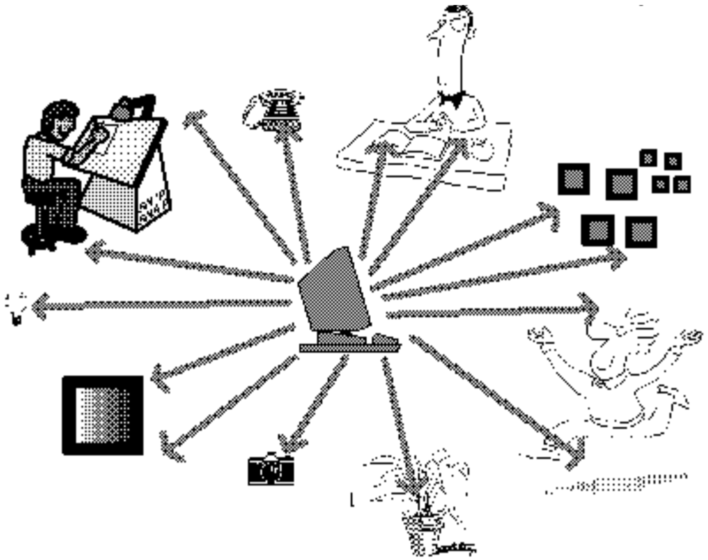


Figure 95. Ubiquitous Computing [original quality].
© Mark Weiser, 1996. Used with permission of Victoria Reich.

Ubiquitous Computing (Ubicomp) is a pattern where networked computing is embedded in the world – into the *stuff* of everyday life. Mark Weiser first defined the concept in his Scientific America article *The Computer for the 21st Century* (Weiser, 1991), where he explicitly framed Ubicomp in opposition to Virtual Reality. *Virtual Reality* is offered here as a counter pattern, where the world is instead made inside the computer.

Ubicomp is today commonly understood by the ubiquity and so apparent invisibility of resources, this opposes more ecological understandings of complex resources and sustainability. Likewise, the network is generalised as a simple omnipresent resource that is recognisable as the *Cloud* pattern.

Ubiquitous Computing creates different kinds of *Invisible Work*. Weiser says, "*A good tool is an invisible tool. By invisible, I mean that the tool does not intrude on your consciousness; you focus on the task, not the tool.*" (Weiser, 1994). Norman characterises this as the *invisible computer* (Norman, 1998). This kind of invisibility renders interactions with the computer incidental and implies the doing of the work (and resources it consumes) is also largely invisible. Ubicomp attempts to provide such seamless interaction through an understanding of the user's current context (the physical state of the world), their likely desires and opaque interfaces. Ubicomp then requires a surveillance infrastructure that makes people and their stuff visible to the machine's gaze. The invisible work of the computer implies a visible user.

Depending on the design of this surveillance infrastructure, and specifically the ways employed for *Positioning, Ranging and Boundary Making* will determine the degree to which Ubiquitous Computing will nurture a *Network of One's Own*, rather than *Panoptical Surveillance Capitalism.*

Related Patterns

2. The Cloud
6. Panoptical Surveillance Capitalism
8. Invisible Work
9. Virtual Reality
13. A Network of One's Own (141)
20. Positioning, Ranging and Boundary Making
22. Stuff from Your Life (253)

References

Norman, D. A. (1998) *The Invisible Computer*. Cambridge, MA, USA: MIT Press.

Weiser, M. (1991) 'The Computer for the 21st Century', *Scientific American (International Edition)*, 265(3), pp. 66–75. doi: 10.1038/scientificamerican0991-94.

Weiser, M. (1994) 'The World is Not a Desktop', *Interactions*. New York, NY, USA: Association for Computing Machinery, 1(1), pp. 7–8. doi: 10.1145/174800.174801.

Weiser, M. (1996) *Ubiquitous Computing*. Available at: https://web.archive.org/web/19970114044913/http://www.ubiq.com/hypertext/weiser/UbiHome.html

10. Virtual Reality

A world inside the computer

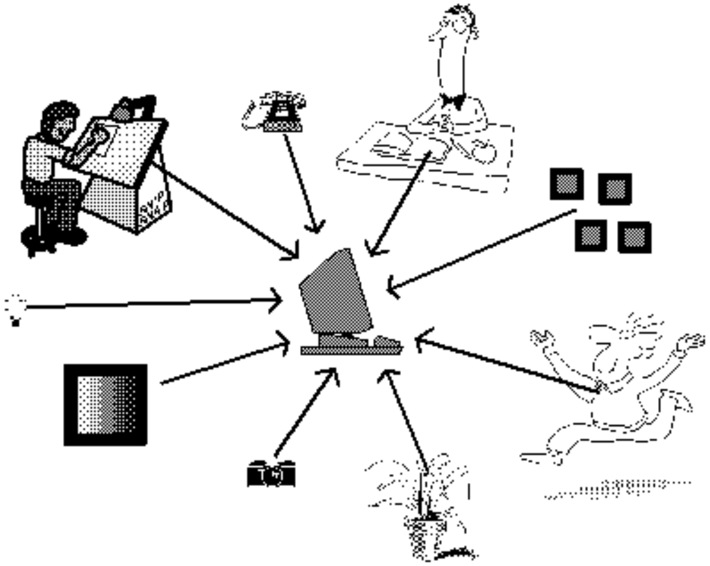


Figure 96. Virtual Reality [original quality].
© Mark Weiser, 1996. Used with permission of Victoria Reich.

Virtual Reality (VR) is a pattern for mediated experience, where the world is made inside the computer. Mark Weiser explicitly framed *Ubiquitous Computing* (Weiser, 1991) in opposition to VR, which at the time was a popular concept through the fantastical vision of Jaron Lanier (Lanier and Biocca, 1992) and others. In VR the world is modelled and rendered inside the machine as multimedia and experienced through devices that enclose our senses. *Ubiquitous Computing* is offered here as a counter pattern, where the computer is in the world.

With respect to the clutter of everyday homelife and the ideals of minimalism, Virtual Reality (and the related pattern of Augmented Reality) seems to offer a way to experience stuff without incurring its physical footprint. This is consistent with James Wallman's *stuffocation* agenda, in which our experiences become valued over our stuff (Wallman, 2014).

The conception of VR in the 1990s was that the world was produced by the computer without a network, a self-contained island with no reference to the world outside. However, the dominant present conception of VR is that of a world inside the cloud with the interconnectivity that implies. In this VR, experience and interactions with stuff become transactions inside Zuckerberg's Metaverse (Milmo, 2021).

The Virtual Reality pattern suggests a mediated homelife with less *Stuff from Your Life* – for tenants, this stuff was potentially the last thing that was owned.

Related Patterns

2. The Cloud
3. Tenancy
9. Ubiquitous Computing
22. Stuff from Your Life

Implied Patterns

Augmented Reality

References

Lanier, J. and Biocca, F. (1992) ‘An Insider’s View of the Future of Virtual Reality’, *Journal of Communication*, 42(4), pp. 150–172. doi: 10.1111/j.1460-2466.1992.tb00816.x.

Milmo, D. (2021) ‘Enter the metaverse: the digital future Mark Zuckerberg is steering us toward’, *The Guardian*. Available at: https://www.theguardian.com/technology/2021/oct/28/facebook-mark-zuckerberg-meta-metaverse.

Wallman, J. (2014) *Stuffocation: Living More with Less*. Penguin Books Limited.

Weiser, M. (1991) ‘The Computer for the 21st Century’, *Scientific American (International Edition)*, 265(3), pp. 66–75. doi: 10.1038/scientificamerican0991-94.

Weiser, M. (1996) *Ubiquitous Computing*. Available at: https://web.archive.org/web/19970114044913/http://www.ubiq.com/hypertext/weiser/UbiHome.html

11. Mindful Computing

Calm ways to see complexity

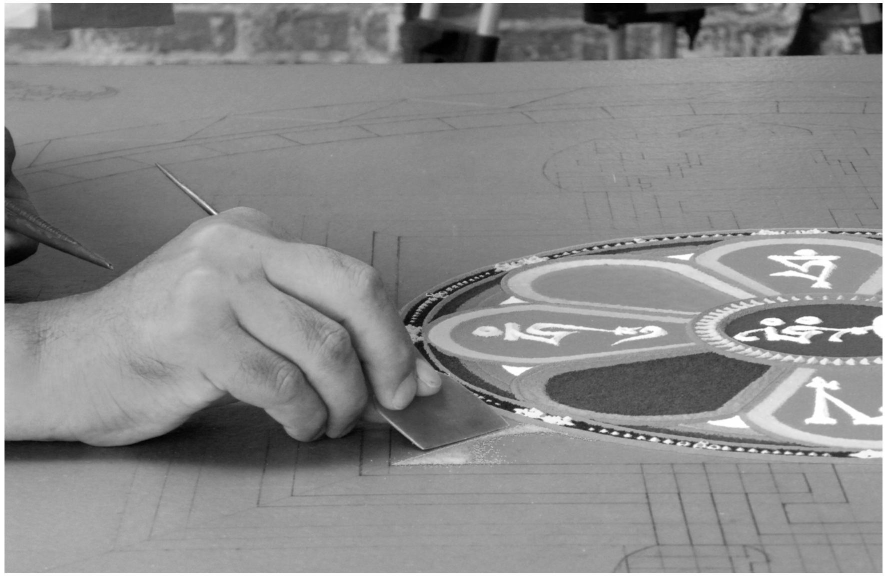


Figure 97. Sand Mandala. © S. C. Hargis, 2010. Used under license, CC BY-ND 2.0.

In recent years mindfulness has gained popularity as a positive mental health practice, in which one is fully present in the moment, knowing one's thoughts, feelings and sensations, but not being unduly reactive or overwhelmed by them. The concept of mindfulness was developed in the late 1970s and has its roots in ancient Buddhist meditation techniques (Henley, 2014).

Mindful Computing then becomes a strategy for dealing with technical complexity, not by hiding or ignoring it, but by making it calmly visible. The grains of sand in the mandala are individually at rest and not contained – see Figure 100. While Mark Weiser's *Ubiquitous Computing* has a somewhat ambiguous relation to *invisibility*, his proposal of Calm Technology frames calmness is a matter of attention rather than of absence (Weiser and Brown, 1995). Mindful Computing by this conception is then not about tools for mindful practice, as such, but a commitment to disclose complexity in calm ways.

Related Patterns

6. Invisible Work
7. Visible Work
9. Ubiquitous Computing

References

Henley, J. (2014) 'Mindfulness: a beginner's guide', *The Guardian*. Available at: https://www.theguardian.com/lifeandstyle/shortcuts/2014/jan/07/mindfulness-beginners-guide-meditation-technique-treatment-depression.

Weiser, M. and Brown, J. S. (1996) 'Designing Calm Technology', *PowerGrid Journal*. Available at: https://web.archive.org/web/19970624041814/http://www.powergrid.com/1.01/calmtech.html.

12. Goldberg Machines

Legible ecologies of Stuff

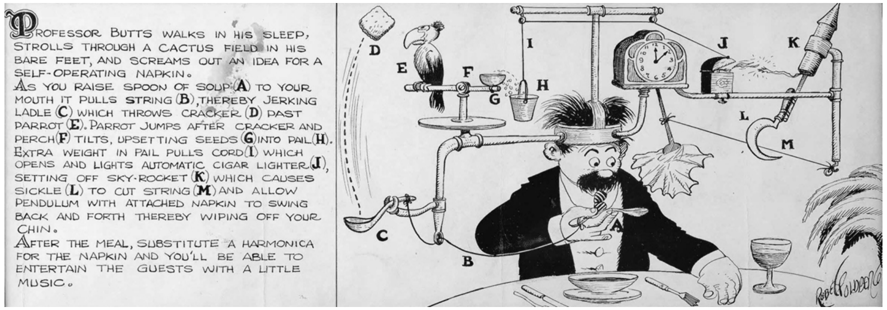

PROFESSOR BUTTS WALKS IN HIS SLEEP, STROLLS THROUGH A CACTUS FIELD IN HIS BARE FEET, AND SCREAMS OUT AN IDEA FOR A SELF-OPERATING NAPKIN.
AS YOU RAISE SPOON OF SOUP (A) TO YOUR MOUTH IT PULLS STRING (B), THEREBY JERKING LADLE (C) WHICH THROWS CRACKER (D) PAST PARROT (E). PARROT JUMPS AFTER CRACKER AND PERCH (F) TILTS, UPSETTING SEEDS (G) INTO PAIL (H). EXTRA WEIGHT IN PAIL PULLS CORD (I) WHICH OPENS AND LIGHTS AUTOMATIC CIGAR LIGHTER (J), SETTING OFF SKY-ROCKET (K) WHICH CAUSES SICKLE (L) TO CUT STRING (M) AND ALLOW PENDULUM WITH ATTACHED NAPKIN TO SWING BACK AND FORTH THEREBY WIPING OFF YOUR CHIN.
AFTER THE MEAL, SUBSTITUTE A HARMONICA FOR THE NAPKIN AND YOU'LL BE ABLE TO ENTERTAIN THE GUESTS WITH A LITTLE MUSIC.
D
E
F
G
I
H
J
K
L
M
C
B
A

Figure 98. Self-operating napkin. © Rube Goldberg Institute, 1931. Used under license.

Goldberg Machines is a pattern for legible ecologies of *Stuff from Your Life* and represents a way to consider *Visible Work* in the home. These are inspectable systems of chain-reaction networks of well-understood elements, that visibly accomplish work when set in motion by some simple action. While Goldberg's cartoons are reliant on imagined physical laws, these articulated ecosystems can inspire realised designs. Mr Mathias' *Push-Button Manor* is an early DIY example (Railton, 1950). With DiSalvo's reconception of Ubicomp, Goldberg Machines can be seen as articulated networks of objects; tangles of humans, stuff and other non-humans (DiSalvo, 2012).

Goldberg Machines are a pattern for whimsical DIY contraptions that are a joyful bespoke alternative for what might be characterised as the *smart home* – beyond that offered by the corporate mass-produced homogeneous home. This pattern suggests visible networks of simple elements coupled together to create some desirable outcome, rather than inscrutable monolithic systems embedded with sophisticated levels of reasoning. Such components have well-defined functions that need no contextual reasoning and so no surveilled users; simple buttons, rather than voice assistants.

The popular *If This Then That (IFTTT)* cloud service allows bespoke chains of action to be created for home automation and can be easily read with some of the intention of the Goldberg Machine pattern. However, with respect to networking, if visible work is prioritised then this dictates a preference for the local rather than remote operation; that it runs on your *own network* rather than *the Internet* or *the Cloud*.

Related Patterns

1. The Internet
2. The Cloud
7. Visible Work
13. A Network of One's Own (141)
22. Stuff from Your Life (253)
23. Voice Assistants

Implied Patterns

Do It Yourself (DIY)
Smart Homes
Push Buttons
If This Then That (IFTTT)

References

DiSalvo, C. (2012) *Adversarial Design*. The MIT Press.

Goldberg, R. (1931) 'The Self-operating napkin: The Inventions of Professor Lucifer G. Butts, A.K.', *Collier's*.

Railton, A. (1950) 'Push-Button Manor', *Popular Mechanics*, pp. 84–87, 252.

13. A Network of One's Own (141)

A Network you Own

Figure 99. Sun Rays. © Alfred Stieglitz, 1889. In public domain.

A Network of One's Own is evidently a recontextualisation of Alexander's *A Room of One's Own*, which in turn draws on Woolf's seminal feminist text (Woolf, 1928). The intention of this pattern is to suggest ways to own the home network*,* allowing homelife to unfold privately in creative and fulfilling, indeed ludic (Gaver, 2006), ways; whether or not this is *Your Own Home*.

Alexander's retelling of Woolf's essay loses some of its political and intellectual charge. A Network of One's Own intends a reengagement with a wider feminist discourse concerning the home: broadly suggesting a critical perspective on domestic technologies (Schwartz Cowan, 1983) and in particular promoting designs that render forms of work visible (Daniels, 1987). This suggests the *Visible Work* pattern and its counterpart *Invisible Work: Hidden Servants*.

A Network of One's Own implies a degree of privacy, distinct from public realms and suggests an *Incremental Intimacy Gradient* exists between the home and *The Internet*. While the model of Bey's pirate island utopias is appealing (Bey, 1991), operating unseen beyond the horizon, networks are defined by connectivity and a solitary network node is evidently absurd. Bey's related concept of Temporary Autonomous Zones is altogether more pragmatic (Bey, 1991) and recognises forms of struggle necessary for its maintenance.

A Network of One's Own technically implies that one has the visuality and control over the network, to determine which devices connect, what data is consumed and produced, and what connections are made to *The Internet* and *The Cloud*. This can be conveniently achieved through an authorised intervention at *The Home WiFi Router*, like the *Pi-hole* ad-blocker. The *Dolmio Pepper Hacker* demonstrates an alternative approach as a unilateral hacker. A critical question in the communal home is then who gets to assert their own network?

Related Patterns

1. *The Internet*
2. *The Cloud*
3. *Tenancy*
4. *Your Own Home (79)*
5. *Incremental Intimacy Gradient (127)*
6. *Invisible Work: Hidden Servants*
7. *Visible Work*
13. *The Home WiFi Router*
25. *Dolmio Pepper Hacker*
26. *Pi-hole*

Implied Patterns

Pirate Utopia
Temporary Autonomous Zones

References

Bey, H. (1991) *T.A.Z.: The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism*. Autonomedia (New autonomy series).

Daniels, A. K. (1987) 'Invisible Work', *Social Problems*, 34(5), pp. 403–415.

Gaver, W. W. (2006) 'The video window: My life with a ludic system', *Personal and Ubiquitous Computing*, 10(2–3), pp. 60–65. doi: 10.1007/s00779-005-0002-2.

Schwartz Cowan, R. (1983) *More work for mother: the ironies of household technology from the open hearth to the microwave*. Basic Books.

Woolf, V. (1928) *A Room of One's Own*. Available at: http://gutenberg.net.au/ebooks02/0200791.txt.

14. The Home WiFi Router

An Internet access point you own, that defines your home network.

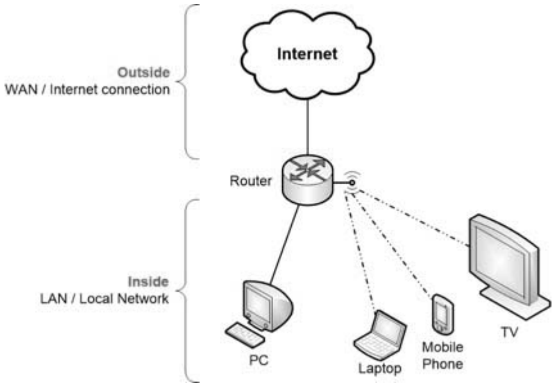


Figure 100. The Home WiFi Router.
© homenethowto.com, 2016. Used under license, CC BY 4.0.

The Home WiFi Router is perhaps the most common pattern for the home network, at least in the UK. By virtue of its telephone network legacy, the router is typically owned and managed by the occupier, regardless of their ownership of the house. This presents the possibility of *A Network of One's Own* in ways alternative networking topologies, such as the *Wide Area Network*, do not. Furthermore, the default use of WiFi to connect devices allows one to create a private network through walls you don't need to own, unliked *Wired Home Networks*.

The private WiFi network managed by the Home Router creates a simple *Intimacy Gradient* in which devices are either connected or not, that know the WiFi credentials or do not. Furthermore, the relatively low power of the router's signal shapes a physical space around the router that defines limited access to the home network. For devices physically cabled to the router by ethernet, this is even more exclusionary.

The Home WiFi Router presents a single point of intervention at which one can define fundamental behaviours of the home network. Some of these are accessible via admin configuration interfaces, otherwise require the router or its software to be replaced. A simple, typically accessible and powerful example, is the ability to define local DNS (Domain Name Server) records, specifying how server names are transformed into IP addresses, for every device on the network. The possibility of such *DNS Redirection* is used by *Pi-hole* ad-blocker to block content from servers known to advertisers. However, the home router also represents a potential point of *surveillance at* which to learn all about the home network and its use of the Internet. As an example, if Google's DNS server (8.8.8.8) is specified by the router as a default, the activity of each device on the network is visible to Google.

The design of the *Router of all Evil* opens the technical possibilities of the Home WiFi Router for private configuration.

Where the devices in the home connect directly to *Wide Area Network* (perhaps a 4G, 5G or *LoRaWAN* network) then *a Network of One's Own* is impossible to assert by this pattern. However, where a smartphone is used as a WiFi hotspot to share a data connection, the Home Router pattern is still relevant.

Related Patterns

6. Incremental Intimacy Gradient (127)
8. Panoptical Surveillance Capitalism
13. A Network of One's Own (141)
16. Wide Area Network
17. The Shape of Space (191)
20. Positioning, Ranging and Boundary Making
26. Pi-hole
27. DNS Redirect

Implied Patterns

Wired Home Networks
Smartphone WiFi hotspots
The Router of all Evil

15. Reception Welcomes You (149)

Visitors are acknowledged as they join the network

Figure 101. Fawlty Towers. © Michael Sanders, 1979. Used under licence.

Reception Welcomes You is a recontextualisation of Alexander's pattern of the same name. This pattern simply suggests an interesting moment for which one could design – as a visitor is welcomed into the home and is potentially granted access to participate with the home network. Yet being a *Network of One's Own* there will likely be house rules and expectations. With the simple exchange of WiFi credentials comes the risk that devices once on the inside will compromise the network.

Christine Geeng's *Privacy Notice in IoT Homes* is centred around a physical pressure-sensitive welcome mat and screen at the front door that goes some way to illustrate the reception of a guest to the home network (Geeng, 2017). The intention of this proposal is to communicate the surveillant practices operated by the home network, "*Making guests aware that data is being collected from them is a small step towards balancing the power dynamics between the host and other users in a domestic space that surveils audio and visual data.*" (Geeng, 2017, p. 3).

The notion of the reception, like the *Front Door Bench*, is of an intermediate boundary space between inside and outside the network where policies are negotiated. As such this too represents an *Incremental Intimacy Gradient* and suggests that only limited access may ultimately be granted – perhaps by way of a separate guest network.

Related Patterns

5. Incremental Intimacy Gradient (127)
13. A Network of One's Own (141)
19. Front Door Bench (242)
20. Positioning, Ranging and Boundary Making

References

Geeng, C. (2017) 'Privacy Notice in IoT Homes', *CHI 2017 Making Home workshop*.

16. Wide Area Network

No One's Network

Figure 102. Wide Area Network. © Shutterstock. Used under license.

Wide Area Network is a counter pattern to the *Home WiFi Router* for the domesticated Internet. Rather than connecting to a local WiFi network, devices access the Internet through a Wide Area Network (WAN) that serves multiple homes or even whole metropolitan areas. These WAN technologies include mobile data (for instance 4G and 5G), municipal WiFi and *LoRaWAN*. The access speed of 5G, in particular, challenge and often exceed those of the established home router model. However, with these WAN technologies there is no *Network of One's Own* – there is only *being on the network* and plugged into the Cloud. Change can only be enacted at the edge, on individual devices, if at all.

Mesh networking technologies create ad hoc networks between nearby devices and frustrate attempts to create a static view of the network. Amazon Sidewalk (*Amazon Sidewalk: a new way to stay connected*, 2020), enabled by default on the Ring doorbell and Amazon Echo, creates a backup mesh network between neighbours, such that if any of the home WiFi networks are disconnected, an encrypted connection is maintained to the Amazon *Cloud* via peers. In this model there is no single point of access and no single point of intervention. Amazon's domestic devices persistently enact their logics and resist being turned off – as devices of surveillance this can be problematic.

Some domestic WAN networks are simply large shared semi-public WiFi networks, such that might be found in student accommodation. Here there is no administrative access to the router, there is also likely no isolation of the devices between apartments and so no *intimacy gradient* between neighbours.

The Smart City is predicated on Wide Area Networks to enact its metropolitan scale logics, logics which discount a *network of one's own.*

Related Patterns

2. The Cloud
5. Incremental Intimacy Gradient (127)
8. Panoptical Surveillance Capitalism
13. A Network of One's Own
14. The Home WiFi Router

Implied Patterns

Smart City

References

Amazon Sidewalk: a new way to stay connected (2020). Available at: https://www.aboutamazon.com/news/devices/amazon-sidewalk-a-new-way-to-stay-connected.

17. The Shape of Space (191)

Material and Immaterial Spaces

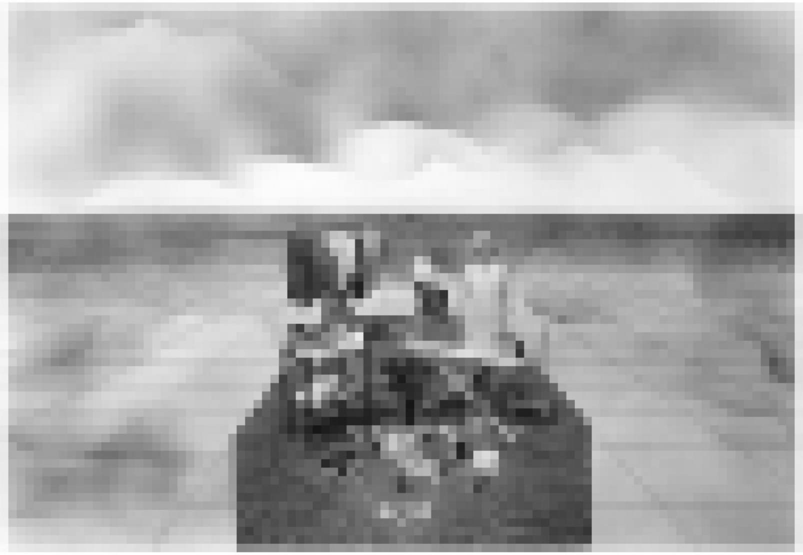


Figure 103. The Happy Island project. © Superstudio, 1971. Redacted.

The Shape of Space pattern is a recontextualisation of Alexander's pattern *The Shape of Indoor Space*, that allows one to consider the material and immaterial spaces of the home.

> *The perfectly crystalline squares and rectangles of ultra-modern architecture make no special sense in human or in structural terms. They only express the rigid desires and fantasies which people have when they get too preoccupied with systems and the means of their production.*

(Alexander et al., 1977, pp. 883–888)

Even in Alexander's materially crystalline square homes, the immaterial shape of the Hertzian space of the home WiFi network will be specific and situated, resulting from complex dynamic interplays of the material ecology. This pattern is then a caution about assumed homogeneity or *ubiquity* – in which technological seams are necessarily *visible* and confrontable.

A *Home WiFi Router* creates an immaterial space that more or less fills the walls of the home and some way beyond. The router's relatively low power determines that devices are in quite close physical proximity to join the network, creating a delineating immaterial *boundary*. The nature of this boundary depends on how the network is secured, by technologies like WPA-2, or whether it is left open. However, with any density of housing these spaces overlap, interfere and present opportunities to those how would break into the network without breaking into the home.

Beyond WiFi, other technologies create immaterial spaces in the home; namely: infrared for remote control, low power domestic radio (notably 433 and 868 MHz) and the receptive fields of microphones on speech assistants. The interplay of these spaces creates further heterogeneous potential.

Related Patterns

5. *Incremental Intimacy Gradient (127)*
7. *Visible Work*
9. *Ubiquitous Computing*
14. *The Home WiFi Router*
20. *Positioning, Ranging and Boundary Making*

References

Superstudio (1971) 'Supersurface, The Happy Island, project'.

18. Pliable Walls (197)

Walls that allow modification

Figure 104. Plasterboard walls. © Shutterstock. Used under license.

Pliable Walls is a recontextualisation of Alexander's *Thick Walls* pattern:

> *Houses with smooth hard walls made of prefabricated panels, concrete, gypsum, steel, aluminum, or glass always stay impersonal and dead.*
>
> *(Alexander et al., 1977, pp. 908–912)*

Alexander's Thick Walls pattern can be carelessly (but usefully) read as means to achieve acoustic privacy and by extension suggests ways to constrain the radiation of wireless technologies – defining the *Shape of Space*. However, on closer inspection it speaks about the possibility of adaption, to make a home personal and alive; thick walls are intended to allow modification, such that material can be removed, and the integrity of the wall withstands – this might be a drilled hole or a carved niche. However, for many tenants this is adaptation is explicitly prohibited, some prevented from making even Blu Tacked additions to their walls.

The Pliable Walls pattern suggests there are ways to create thick adaptable walls, even in spaces where one is a tenant. There is a resonance here with Brand's Shearing Layers (Brand, 1995), which suggests there are material ways to design and co-opt the affordances of walls for change. A simple example would be the installation of a picture rail or bracketing for a shelving system. The *Nomadic Furniture* pattern suggests both material and immaterial changes to rented spaces, by way of indoor tents and light projectors. Lighting can create an ambience and edit visibility, with minimal physical intervention in the room.

The Stuff of Home model (Chapter Seven) offers the related concept of *surfaces* that are adaptable through display and lighting technologies, addressable via the networked home.

Related Patterns

3. Tenancy
17. The Shape of Space (191)
21. Nomadic Furniture

Implied Patterns

Light Projectors

References

Brand, S. (1995) 'How Buildings Learn: what happens after they're built', *Penguin Books*, p. 720. doi: 10.2307/990971.

19. Front Door Bench (242)

Yellow Chair Stories

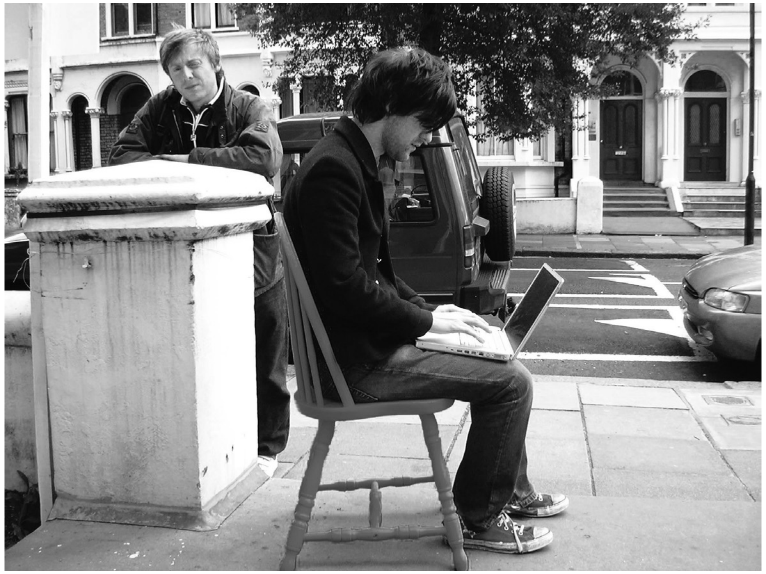


Figure 105. Yellow Chair Stories. © Anab Jain, 2005. Used with permission.

Front Door Bench is a recontextualisation of Alexander's pattern of the same name. It is reminiscent of Anab Jain's *Yellow Chair Stories* (Jain, 2005), an attempt to create a *community-of-presence* around Jain's open home WiFi. Neighbours were invited to publicly sit on a chair outside Jain's house and use the network, rather than consume it unseen and anonymously, as they had previously. In 2005 WiFi networks without security were commonplace.

Front Door Bench speaks of the ill-fitting WiFi *shape of spaces* created by the *Home WiFi Router* that extend into the street and public spaces. Like the *Reception,* the Yellow Chair suggests a way to negotiate the immaterial *Intimacy Gradient* of the home and make *boundaries*.

Related Patterns

5. Incremental Intimacy Gradient (127)
14. The Home WiFi Router
15. Reception Welcomes You (149)
17. The Shape of Space (191)
20. Positioning, Ranging and Boundary Making

References

Jain, A. (2005) *Yellow Chair Stories*. Available at: https://superflux.in/index.php/work/yellow-chair-stories/

20. Positioning, Ranging and Boundary Making

Locative technologies

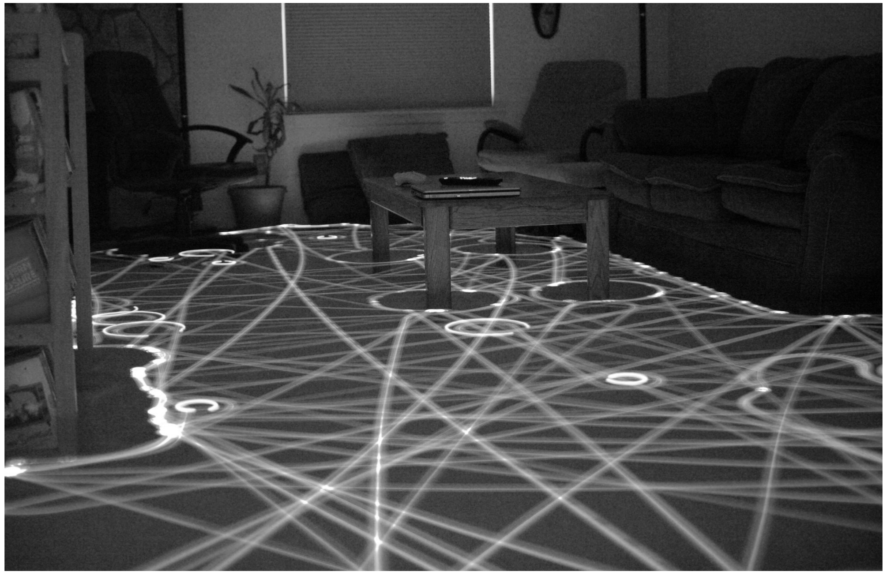


Figure 106. Roomba paths, long exposure light painting.
© Chris Bartle, 2009. Used under license, CC BY 2.0.

The Positioning, Ranging and Boundary Making pattern captures some of the design decisions in developing and applying locative technologies in the home. Each has different applications and different implications, enabling types of contextual interaction and implying alternative forms of surveillance.

Positioning is meant in the sense that something might be ascribed a position in physical space, likely using some coordinate system and so placed some existing map, from which some inferences can be drawn. GPS (Global Positioning System) is an obvious example – albeit with limited indoor domestic usefulness. The system allows a receiver's position (longitude, latitude and altitude) to be independently calculated on-device by comparing radiofrequency broadcasts from a consolation of satellites; GPS is not inherently surveillant as it implicates no external parties. However, for a service like Google Maps the subsequent acquisition of the map and localised data via the Cloud, requires an external transaction and then renders a visible user.

Positioning technologies (like GPS) tend to seek to be infrastructural and invisible, but there will inevitably be visible seams to be found (Broll and Benford, 2005) which further *shapes space*. In the home, such infrastructures can make considerable demands of the built environment and assume types of ownership. For instance, Weiser's demonstration of an indoor location system, based on Want's Active Badges (Want *et al.*, 1992), required the installation of a network of infrared beacons at known fixed positions. This active badge or pin pattern is the same as later described by Bill Gates for his Lake Washington mansion (Gates and Ottavino, 1995), it makes an explicit declaration that this thing is to be seen by the machine, unlike the implicit observation allowed by cameras. These systems employ some centralised surveillance and reasoning about the location of people and resources to generate desirable experiences, perhaps music that follows an individual from room to room. Curiously, the *Ubiquitous Computing* aspiration to compute in the world can require an internalised *Virtual Reality*. A critical question then, where is this reality kept, by whom and for what purpose?

Ranging is an alternative strategy for location that is meant in the sense that a distance between two points becomes known. Positioning technologies (like GPS) use triangulation, where three or more such ranges are required from known points to compute a position. However, ranging is also a useful locative technique in which there can be contextual reasoning about what is simply close by. The *Approximate Library* uses WiFi signal strength for ranging and simple on-device reasoning based on proxemic volumes. This low-resolution partial data does not have the same surveillant potential as positioning. Ranging might be considered a form of sousveillance, of being watched from beneath (Mann, Nolan and Wellman, 2003).

Finally, Boundary Making is meant in the sense that some spatial boundary is imposed which defines the *Shape of Space* and some consequent set of circumstances. A simple example is the accessibility of the *Home WiFi Router* signal which defines the home network and the rules that exist there. The *Dolmio Pepper Hacker* pattern implies that devices are disconnected whilst within the boundary of the dining room table. Inclusion in bounded space is a yet lower-resolution measure, than ranging – a simple boolean. Again, the *Approximate Library* offers some means to define such boundaries.

Related Patterns

2. The Cloud
8. Panoptical Surveillance Capitalism
9. Ubiquitous Computing
10. Virtual Reality
14. The Home WiFi Router
17. The Shape of Space (191)
25. Dolmio Pepper Hacker
27. The Approximate Library

Implied Patterns

GPS
Sousveillance
Active badges

References

Broll, G. and Benford, S. (2005) ‘Seamful Design for Mobile Games’, *Design*, pp. 1–19. doi: 10.1007/11558651_16.

Gates, B. and Ottavino, J. (1995) *Road Ahead*. HighBridge Company.

Mann, S., Nolan, J. and Wellman, B. (2003) ‘Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments’, *Surveillance and Society*, 1(3), pp. 331–355. doi: 10.24908/ss.v1i3.3344.

Want, R. *et al.* (1992) ‘The Active Badge Location System’, *ACM Transactions on Information Systems (TOIS)*, 10(1), pp. 91–102. doi: 10.1145/128756.128759.

21. Nomadic Furniture

DIY Furniture for spaces you don't own

Figure 107. Nomadic Furniture: Relaxation and Work Cubes.
© James Hennessey and Victor Papanek, 1973. Redacted.

Hennessey and Papanek's Nomadic Furniture (Hennessey and Papanek, 1973) is a catalogue of plans for DIY furniture motivated by the author's experiences of living in rented accommodation in the 1970s wanting to be surrounded by *their stuff*; it serves as a useful pattern for assertive *tenancy* in the networked home.

Hennessey and Papanek's DIY plans are for inexpensive "*lightweight furniture that folds, inflates, knocks down, stacks, or is disposable and can be recycled*" and several of the designs go beyond the construction of new furniture or stuff and offer ways for the renter access and manipulate the home's space plan and scheme. Freestanding shelving can create a layer in front of a wall or a divider, without attachment to the fabric of the room – this can be considered in the terms of the *Pliable Walls* pattern. Similarly, there are several plans for *Living Cubes* (Entertaining, Children's, Relaxation and Work Cubes), which are described as *indoor tents* and create new pliable walls. The *Relaxation Cube* incorporates a slide-projector and projection screen (see Figure 110) the use of electronic stuff to project light, sound or smell allows one to further immaterially change a space whether you own it or not. Where that stuff is also connected to the home network the interactional potentials are increased.

The DIY Nomadic Furniture pattern also contextualises the commercial robotic furniture systems for dwellers (and likely tenants) of *tiny homes*. This large scale furniture transforms mechanically to optimise small spaces. The Studio Suite built by Ori Systems is such an example, where a robotic wall runs on rails to change the division of a room with beds, tables, storage and lighting housed within – inevitably controlled by an app and enabled by the cloud.

Related Patterns

4. Tenancy
16. Pliable Walls (197)
18. Stuff from Your Life (253)

Implied Patterns

Do It Yourself (DIY)
Tiny Homes
Robotic Furniture Systems
Light Projectors

References

Hennessey, J. and Papanek, V. (1973) *Nomadic Furniture*. Knopf Doubleday Publishing Group.

22. Stuff from Your Life (253)

Know it to be useful or believe it to be beautiful

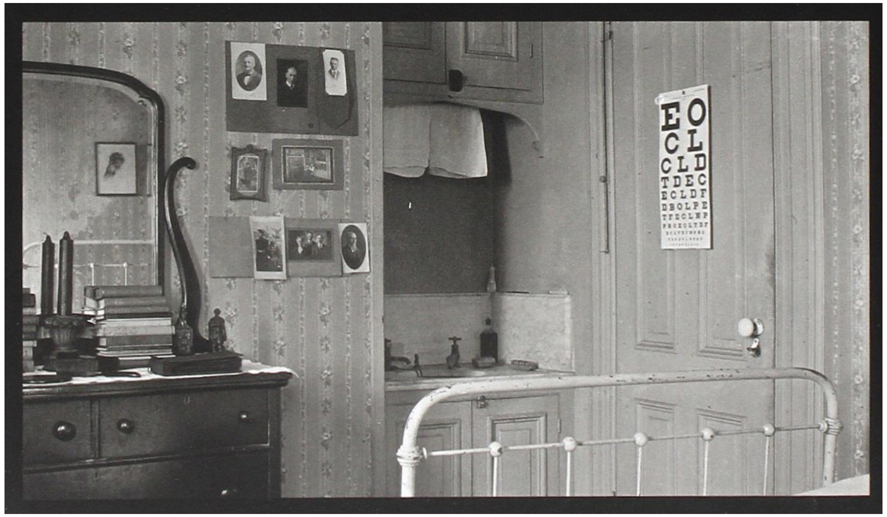


Figure 108. Things from Your Life.
© Unknown photographer, c1910. Used with permission of Wisconsin Historical Society.

Stuff from Your Life is a recontextualisation of Alexander's final pattern, the Things from Your Life. This pattern suggests an instinctual need for people to accommodate "*the things they really want to keep around them" (Alexander et al., 1977, pp. 908–912)*, rather than the publicly constructed demands of good *interior design*. Alexander's pattern somewhat resonates with William Morris', "*Have nothing in your houses that you do not know to be useful, or believe to be beautiful.*" (Morris and Morris, 2012). Both Alexander and Morris suggest that there are things to be excluded from the home; this pattern does not simply advocate for clutter.

The Stuff from Your Life pattern is renamed from Alexander's original to bring to mind Brand's conception of *Stuff* (Brand, 1995), which does account for a degree of clutter. Brand's stuff implies a particular form of ownership and agency expressed through these things regardless of housing tenancy, unlike the slower layers of the home. The Stuff of Home model (Chapter Seven) then allows one to consider how this stuff is changed by the network – specifically where connected stuff has new types of ownership and cloud derived agencies that can update over the air.

Some counter *Interior Design* patterns actively promote the removal stuff, beyond simple decluttering, minimalism being the most aggressive. Similarly, James Wallman's fear of suffocation by stuff, or stuffocation, is further motivated by the environmental cost of manufacturing and disposing of physical things (Wallman, 2014). In reaction Wallman promotes the valuation of immaterial experience over material stuff. However, where these stuff-less experiences are derived from the Cloud they too become externalised somewhat public transactions.

The Stuff from Your Life pattern prioritises physical stuff, over the virtual. In this respect it is compatible with Weiser's original conception of *Ubiquitous Computing* in opposition to *Virtual Reality*.

Related Patterns

2. The Cloud
3. Tenancy
9. Ubiquitous Computing
10. Virtual Reality

Implied Patterns

Interior Design

References

Brand, S. (1995) ‘How Buildings Learn: what happens after they’re built’, *Penguin Books*, p. 720. doi: 10.2307/990971.

Morris, W. and Morris, M. (2012) ‘The Beauty of Life [1880]’, in *The Collected Works of William Morris: With Introductions by his Daughter May Morris*. Cambridge University Press (Cambridge Library Collection - Literary Studies), pp. 51–80. doi: 10.1017/CBO9781139343145.005.

Wallman, J. (2014) *Stuffocation: Living More with Less*. Penguin Books Limited.

23. Voice Assistant

Hey Siri!

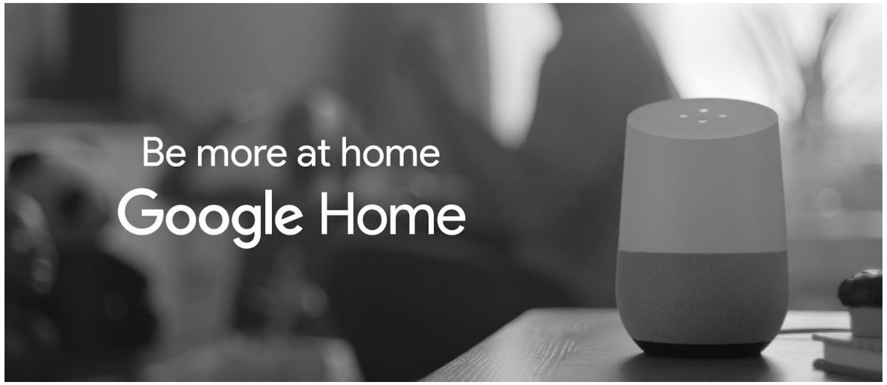


Figure 109. Google Home. © Google, 2017. Author asserts fair use.

The Voice Assistant pattern is instantiated by products such as the Amazon Echo (2014), Google Home (2016) and Apple Homepod (2018) – a speaker and microphone with access to the Cloud. In the domestic context they are able to respond to simple questions (for instance a query about the weather), initiate timers, play music from Cloud services like Spotify and control IoT devices discovered on the home network like lights, thermostats and televisions. These devices are the vessels for the somewhat coherent voices of Amazon's Alexa, Google's unnamed agent and Apple's Siri, who are summoned with a wake word, *Hey Siri!* This initiates a dialog with the assistant with the assurance that until this point the device is not listening (or at least not passing audio recordings to the Cloud).

The Voice Assistant pattern seeks a kind of interactional *ubiquity*, where a dialogue can be initiated from anywhere in the room and somewhat beyond. The sophisticated microphone technology shapes a large receptive space around the assistant. Where more than one assistant occupies a home, they can work in tandem.

The Voice Assistant is perhaps the clearest expression of the *smart home*, that draws on Victorian ideas of domestic servants and *Invisible Work*. Google marketed their voice assistant with the slogan, '*Make Google do it!*' It offers a counter pattern to the Amazon Dash Button.

With millions of devices delivering unimaginable volumes of data to the Cloud services of just few companies, the possibility of improved learning and insight is vast. Over time these devices can be seamlessly improved by over-the-air software updates and improved server technology. However, at the same time the *Panoptical Surveillance Capitalism* pattern is implied, at least for Amazon and Google's products.

Project Alias (Karmann and Knudsen, 2018) is a response to the Amazon Echo and Google Home's inscrutable recordings, that the designers frame as a physical parasite. It is a hardware device that encloses the microphone and produces white noise to prevent their suspected surveillance – clearing the channel only when it verifies the wake word itself. Distributed as DIY plans and self-assembled and self-configured, Project Alias attempts to assert *A Network of One's Own*.

Related Patterns

2. The Cloud
6. Invisible Work
8. Panoptical Surveillance Capitalism
9. Ubiquitous Computing
13. A Network of One's Own (141)
17. The Shape of Space
24. Amazon Dash Button

Implied Patterns

Smart Home
Device Parasites

References

Karmann, B. and Knudsen, T. (2018) *Project Alias*. Available at: https://bjoernkarmann.dk/project_alias.

24. Amazon Dash Button

Place it. Press it. Get it.

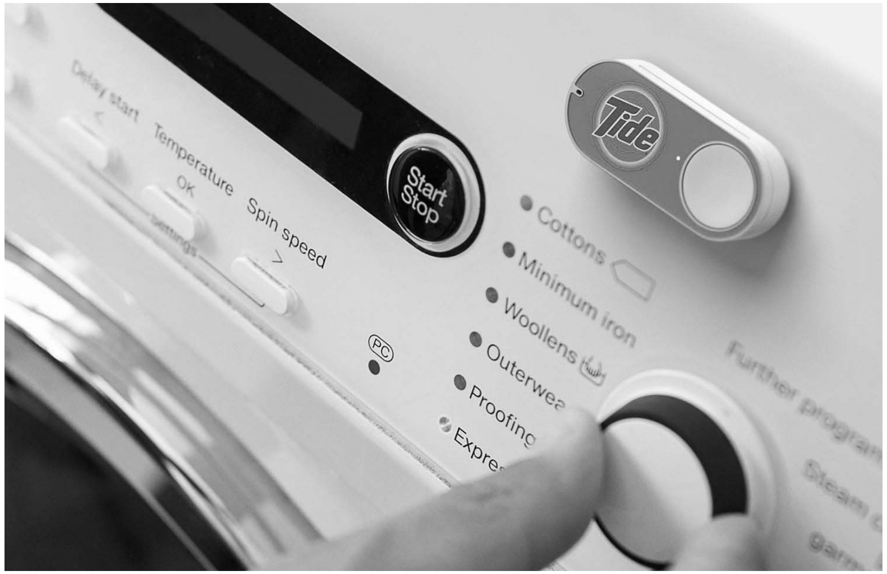


Figure 110. Amazon Dash Button.
© Amazon and Procter & Gamble, 2015. Author asserts fair use.

The Amazon Dash Button (2015 – 2019) is a single button WiFi device which when pressed instantaneously places an Amazon order for the product with which it is associated. Multiple buttons can be positioned around the home to be available at the opportune moment – a detergent button by the washing machine, etc.

The Amazon Dash Button has a familiar interactional pattern, that of the push-button – marketed with the slogan, "*Place it. Press it. Get it*". The push-button is a simple compelling interaction that remains ever-present in modern homes, for instance: doorbells, light switches, and TV remote controls. The consequence of the action is typically very well defined, as it is with the Dash Button. No further context is required to determine the intention of the user and as such there need be no *surveillance* outside the action of the button. As such this is a very different product and design pattern to the *Voice Assistant*.

The Amazon Dash Button implicates a good deal of *Invisible Work* via the *Cloud*, setting in train a series of unseen events and Ghost Work to fulfil the contract of the button press. Indeed Daniel Rausch, an Amazon vice president, said they aspired "*to make shopping disappear*" (Fox Rubin, 2019). However, as a pattern, this is also suggestive of alternative actions that might be simply initiated over the network, perhaps something akin to the *Goldberg Machines*.

It is unclear why Amazon discontinued the Dash Button in 2019, but the Echo series of *voice assistant* devices have since been the company's major domestic line.

Related Patterns

2. The Cloud
6. Invisible Work
8. Panoptical Surveillance Capitalism
12. Goldberg Machines
23. Voice Assistant

Implied Patterns

Push Buttons

References

Plotnick, R. (2018) *Power Button: A History of Pleasure, Panic, and the Politics of Pushing*. The MIT Press. doi: 10.7551/mitpress/10934.001.0001.

Fox Rubin, B. (2019) 'Amazon stops selling Dash buttons, goofy forerunners of the connected home', *cnet.com*. Available at: https://www.cnet.com/news/amazon-stops-selling-dash-buttons-goofy-forerunners-of-connected-home/.

25. Dolmio Pepper Hacker

Turns tech off and family dinnertimes on

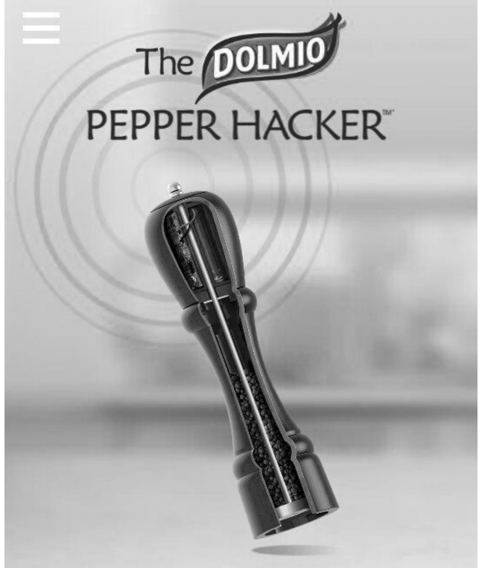


Figure 111. Pepper Hacker. © Mars Incorporated, 2014. Used with permission.

The Dolmio Pepper Hacker was a concept developed in 2014 by Clemenger BBDO, an Australian marketing communications company, for the pasta sauce brand, owned by Mars. "*One twist shuts down TV, WiFi and mobile devices*" and these were given to "*frustrated mums*" as part of an online advertising campaign (Dolmio, 2015). In 2016 thousands of working Pepper Hackers were given away with an on-pack promotion.

"*The Pepper Hacker features hidden custom software that mimics the household WiFi network. This tricks smart devices within the home to disconnect from the WiFi network and connect to the Pepper Hacker's in-built WiFi chip, blocking all outgoing data.*" – Luke Hawkins, Creative Director at Clemenger BBDO (Hawkins, 2015).

While some video sequences shown in the advertisement seem technically dubious, this description and the subsequent promotion suggest that Pepper Hackers do work. This mimicry of the home WiFi network is known as *Rogue Access Point* and if so configured, would block access to the Internet. It would likely need to be coupled with *WiFi Deauthenication* to first cause clients to disconnect from the *Home WiFi Router*. The focus of the Pepper Hacker is the dining room table and if operated at that location would present the strongest WiFi signal for proximate devices, other *Tracking or Ranging* technologies might also be implicated.

The Pepper Hacker responds to a use of the Internet that is primarily about the consumption of rich, attention-holding content from *The Cloud*. It disconnects devices from the Internet not by shutting down the WiFi, but by creating an extreme *Network of One's Own* which has no onwards-connection to the Internet.

The individual yielding the Pepper Hacker is granted a unilateral power, who according to this design is the mother.

Related Patterns

2. The Cloud
13. A Network of One's Own
14. The Home WiFi Router
20. Positioning, Ranging and Boundary Making
28. Rogue Access Point
30. WiFi Deauthenication

References

Dolmio (2015) *Technology has hijacked family dinnertime*. Available at: https://www.youtube.com/watch?v=HUgv5MDF0cQ.

Hawkins, L. (2015) *DOLMIO Pepper Hacker*. Available at: https://www.lukehawkins.com.au/DOLMIO-Pepper-Hacker.

26. Pi-hole

Network-wide ad-blocking

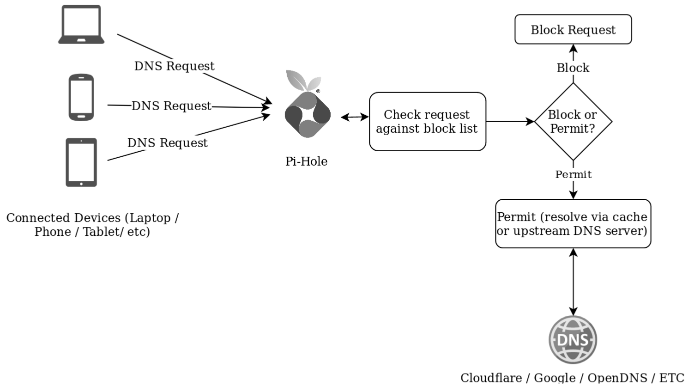

DNS Request
DNS Request
DNS Request
Connected Devices (Laptop / Phone / Tablet/ etc)
Pi-Hole
Check request against block list
Block or Permit?
Block
Block Request
Permit
Permit (resolve via cache or upstream DNS server)
DNS
Cloudflare / Google / OpenDNS / ETC

Figure 112. Pi-hole. © David Holder. Used with permission.

Pi-hole (Salmela, 2014) is a popular network-level ad-blocker that once installed leaves the home network (largely) advertisement free. This uses the *DNS Redirect* pattern to prevent devices on the network from contacting a list of well-known advert-serving websites.

Pi-hole requires an authorised reconfiguration of the *Home WiFi Router*, but no permissions or modifications are needed for the individual network devices. As such it is a unilateral action that can be taken by the network owner. The open-source software is typically hosted on a Raspberry Pi computer that is joined to the home network and must run constantly.

Related Patterns

14. The Home WiFi Router

29. DNS Redirect

Implied Patterns

Content Blocking

References

Salmela, J. (2014) *Pi-hole*. Available at: https://pi-hole.net/.

27. The Approximate Library

Proximate interactions for the Internet of Things

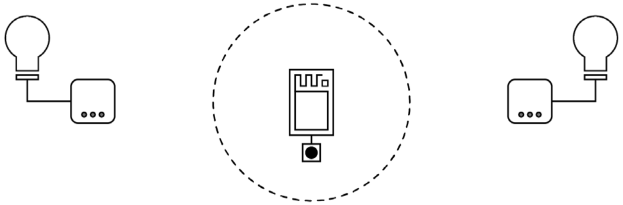


Figure 113. Approximate Library. © David Chatting.

The Approximate Library (Chatting, 2020) is an Arduino C++ library for building proximate IoT interactions for the inexpensive Espressif WiFi modules (ESP8266 and ESP32). With this software installed a device can estimate the physical distance between it and another device on the same network, it offers a means of *ranging* for domestic IoT. This also allows proximate devices to be identified by their network address so contextual interaction can take place – for instance, a remote-control device using the Approximate Library can operate the nearest IoT lamp. This requires no infrastructure, beyond the network itself; devices can make limited (but useful) assertions about their location without transacting with potentially surveillant parties.

The Approximate Library borrows from the language of proxemics (Edward T. Hall, 1963) to describe successively larger spaces as intimate, personal, social and public; this speaks to the *Incremental Intimacy Gradient* pattern.

Technically, the Approximate Library uses packet sniffing to observe messages exchanged by devices over the shared medium of the home WiFi network. Whilst the contents of these messages are typically encrypted, MAC (Media Access Control) addresses and RSSI (Received Signal Strength Indicator) values of participating devices are visible. With this information, the library can identify close-by devices and watch their use of the network. Optionally, the device's IP address can also be obtained by way of an ARP (Address Resolution Protocol) scan.

Packet sniffing over WiFi can observe the traffic of any nearby network, whether or not the security credentials are known. In the domestic context this would include the discovery and observation of the networks of neighbours. The design of the Approximate Library requires the credentials of a specific *Home WiFi Router* to inhibit such illegitimate use.

The Approximate Library offers five documented simple code examples in the C++ language that demonstrate two sub-patterns for use: Proximate Device Handler (when an unknown device is close-by) and the Active Device Handler (when a known device is using the network). Working with Arduino, a multiplicity of possibilities with other software libraries and electronics are opened.

Related Patterns

5. Incremental Intimacy Gradient
8. Panoptical Surveillance Capitalism
14. The Home WiFi Router
20. Positioning, Ranging and Boundary Making

Implied Patterns

Packet Sniffing
ARP Scanning

References

Chatting, D. (2020) *The Approximate Library*. Available at: https://github.com/davidchatting/Approximate/.

Edward T. Hall (1963) ‘A System for the Notation of Proxemic Behavior’, *American Anthropologist*, 65(5), pp. 1003–1026.

28. Rogue Access Point

An access point that has the same characteristics as a legitimate one

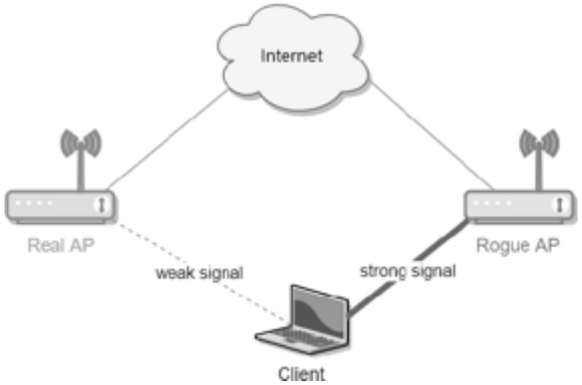


Figure 114. Rogue Access Point. © Ricardo Goncalves. Used with permission.

Rogue Access Points are a well-known method by which hackers can unilaterally force a client device to leave the real WiFi network and join a rogue doppelganger.

This depends on devices attempting to auto-connect to networks with which they are familiar and their preference for joining the network with the strongest signal. Where the client is already connected to the real access point, it is combined with *WiFi Deauthenication* to force a disconnection. If the real network is open and has no security, the Rogue AP can hijack the connection without challenge. If the real network is secured, for instance with WPA-2, then its credentials need to be obtained.

Related Patterns

14. The Home WiFi Router
25. Dolmio Pepper Hacker
30. WiFi Deauthenication

29. DNS Redirect

Redirection of Internet requests

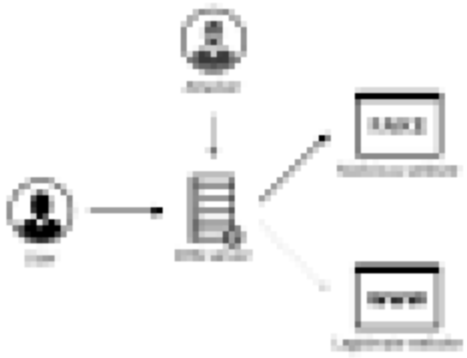


Figure 115. DNS Redirect. © Imperva. Redacted.

DNS Redirect is a pattern by which network requests (like HTTP) can be directed to alternative servers. This manipulates DNS (Domain Name Server) the mechanism by which domain names are mapped to IP (Internet Protocol) addresses – how *www.amazon.com* is resolved to *13.32.69.252*. Network devices will make a DNS request at the start of every exchange, initially with the local router and then if unknown there, with well-known DNS machines on the Internet. Typically, DNS redirection rewrites the local DNS record at the *Home WiFi Router* (and requires administrative access) such that all clients of the home network will experience the redirect.

DNS Redirect is a means by which hackers can redirect users to malicious websites, via a compromised router. However, it can also be used to assert a *Network of One's Own*, to reconfigure the logic of the network without needing to modify the software of individual network devices. The pwnazon script (Shepard, 2011) is an example of this that changes the Amazon Kindle's wallpaper; it redirects requests to the Amazon ad server to the IP address of a local machine serving alternative imagery. For a defunct IoT product, like the Nabaztag, this tactic can allow the withdrawn network servers to be replicated locally and some useful operations to be restored at the network level, without modification to the device. This tactic only works for where there is no subsequent verification of the server, as such it does not work for HTTPS delivery.

DNS Redirect is also the pattern by which network-level content blocking can be achieved; access to specific servers can be effectively blocked by rewriting the local DNS record for a domain as unknown. This creates a *sinkhole* for a list of known servers on this network and is the mechanism by ad-blocking software such as *Pi-hole* operates. Similarly, this tactic can be conceivably employed to block any set of websites that carries content unwanted in the home, be that for parental, political or religious motivations. It might also block access to specific functions unwanted in an IoT device. Content blocking in this way can operate whether or not the delivery is secured.

Related Patterns

13. A Network of One's Own (141)
14. The Home WiFi Router
24. Pi-hole

Implied Patterns

pwnazon
Content Blocking

References

Shepard, M. (2011) *pwnazon*. Available at: https://github.com/mflint/pwnazon

30. WiFi Deauthentication

Forces a Client off an Access Point

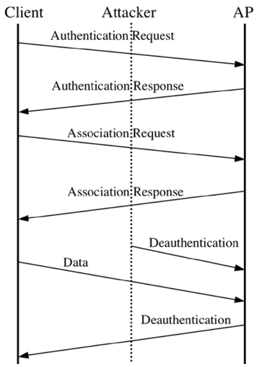


Figure 116. WiFi Deauthentication. © Haitham AL-ani. Used with permission.

WiFi Deauthentication forces a client to be temporarily disconnected from a WiFi access point through the injection of packets on the network. This may be initiated without authentication from either the targeted client or the access point and maybe an ill-intentioned action of a hacker. However, in asserting *A Network of One's Own* it offers some control even when one does not own (or have administrative access to) the router.

Artist Julien Oliver used WiFi Deauthentication in his response to a series of stories in which Airbnb guests had found themselves covertly filmed by hidden WiFi cameras operated by their hosts (Oliver, 2015). Oliver's *dropkick.sh* script identifies and disconnects cameras found on the local WiFi network when run on the guest's laptop. Cameras are identified on the network by their OUI (Organizationally Unique Identifier) which forms part of their MAC address.

It is likely that the *Dolmio Pepper Hacker* uses this pattern to force clients off the home network and on to the one provided by the pepper hacker.

Related Patterns

13. A Network of One's Own (141)
14. The Home WiFi Router
25. Dolmio Pepper Hacker

Implied Patterns

Packet injection

References

Oliver, J. (2015) *Detect and disconnect WiFi cameras in that AirBnB you're staying in*. Available at: https://julianoliver.com/output/log_2015-12-18_14