CHAPTER 9

How does the way we use the Internet make a difference?

M. I. Franklin

THE QUESTION
THE INTERNET AND US

Internet-dependent media and networked, mobile communications are now embedded in many facets of human endeavour, at least in those parts of the world with access ~~to the Internet~~. Internet media and communications make a difference to the conduct of politics precisely because they can interconnect individuals and communities, governmental agencies, media organisations, businesses, and other sorts of non-state actors, simultaneously at a *supraterritorial* level (Scholte 2000). However many regions, in both the Global North and Global South, are still poorly served in terms of physical access, and quality of transmission, such as speed and capacity (also known as 'bandwidth'). These limitations affect the sorts of goods and services that those on the wrong side of the *global digital divide* between but also within the Global North and Global South – rural communities in sub-Saharan Africa or south Asia, sparsely populated regions such as Alaska, the Australian Outback, or poorer city neighbourhoods in the world's global cities – can use once online. Intergovernmental organisations and the private sector are on record in their ‘shared commitment’ to ‘connecting the next billion’ (Internet Governance Forum 2008; ITU/WSIS 2005; UN 2015).

State and corporate actors differ markedly in key areas of internet policy-making: e.g. over the role that national regulators should play in defining the terms of internet access and use for citizens, or the social responsibilities of internet businesses (Council of Europe 2014; Ruggie 2014). They also differ in their respective positions on how they track, collect, and then handle the massive amount of personal – digital – data we generate when online; measured now in *petabytes*. Contentions about who owns, but also who – or what – controls the world’s data centres that store these stacks of ‘big data’, are part of struggles over agendas for internet–design, access, use, data–collection, and content-management. More recently the role that automated computer programs (based on algorithms) play in managing, even manipulating these streams of ‘big data’ – to influence ~~as~~ online news sources, if not election outcomes – have become headlines news in themselves.

These issues are not just legal or technical questions for computer experts, civil servants, or politicians. They go to the heart of debates about who governs, how, and on whose terms as competing understandings of sociocultural, political economic, and environmental well-being have become inseparable from how polities, and communities are increasingly ‘logging on’ to digital devices and networks, becoming ‘linked in’ to various online spaces and services on a daily basis.

There have been concerns that such interference might have affected outcomes of electoral processes, perhaps triggered by the unanticipated outcomes of the UK’s referendum on leaving the European Union and the US election in 2016.

One version of the story of how internet media and communications became intrinsic to global politics goes like this: the Internet emerged out of military-funded R&D (Research and Development) into computerised communication network design in academic research institutions, not only in the US but also in Europe. Software that made it much easier to find information on this ‘network of networks’ made the Internet a global, popular success. For instance, in the 1990s these *World Wide Web* protocols, developed by Tim Berners-Lee’s team at CERN in Switzerland, which pioneered user-friendly applications enabled the Zapatista Movement in Mexico to communicate their arguments against neoliberal globalisation agendas, such as the North American Free Trade Area (NAFTA) to the world. Websites, blogs and alternative news-wires heralding the arrival of *citizen journalism* were instrumental in publicising later waves of anti-globalisation protests ~~since then~~. Whilst all these civic activities were taking place, specialised innovations enhanced the speed and volume of trans-border transactions underpinning deregulated – globalising – financial markets. Early, start-up companies, some of which are now global brands, took off at this time.

How we find out about the world is the subject of **Chapter 8**, which also discusses citizen journalism; of course, today many of us get much of our information about what goes on around us, and abroad from online sources.

In the last two decades attention has turned from the World Wide Web innovations to the role that commercial applications, known as ‘Web 2.0’ or ‘social media’, have been playing in large-scale mobilisations (from student demonstrations in Athens 2008, to popular riots in London 2011, to anti-government demonstrations in Teheran, Rangoon, or Bangkok), in political transformations (in the Middle East and North Africa), and in waves of trans-border mobilisations of popular protest around the world (linking the *Occupy* protests in downtown Manhattan and inner-city London, to the *Podemos* sit-ins in Madrid and the demonstrations around Gezi Park in Istanbul). Internet communications, now accessed through mobile phones, have been a primary means for ordinary people to organise, make their voices heard around the world online, and on the streets.

The Occupy movement is discussed in **Chapter 18** and **26**.

This makes how people use live-video apps, instant-messaging, and micro-blogging services very interesting for not only law enforcement and intelligence services but also for commercial operators. Government agencies are particularly keen on accessing our communications data, containing personal information about us (where we are, who we are messaging, and when). These measures are justified in order to fight crime, defend national security, or to catch potential terrorists. Companies, those that own and control the most popular online services, and institutions like schools and universities are keen to gather data for, what they claim, is market research, service 'optimisation', or improved 'student experience'. Human rights organisations and civil liberties watchdogs have been joining forces with 'digital rights' activists to argue that without informed consent, or at least a search warrant, excessive data-tracking and collection practices amount to mass online surveillance (Necessary and Proportionate 2014). Even if we believe we have 'nothing to hide' the lack of legal or political accountability undermine our fundamental rights and freedoms, online as well as offline (the right to express ourselves freely, to associate with whom we please, academic and other freedoms such as religion, and the right to privacy).

BOX 9.1 ONLINE PIONEERS: THE ZAPATISTAS

The Zapatistas, or, in full, the Zapatista Army of National Liberation (*Ejército Zapatista de Liberación Nacional*, EZLN), are based in Chiapas, a state in southern Mexico. Their anti-neoliberal globalisation ideas and mobilisation strategies, available on the web in the writings of their former leader, known as Subcommandante Marcos (an early internet celebrity), have influenced resistance groups elsewhere. This is, in part, due to their pioneering internet-based communications strategy and creative use of visual imagery.

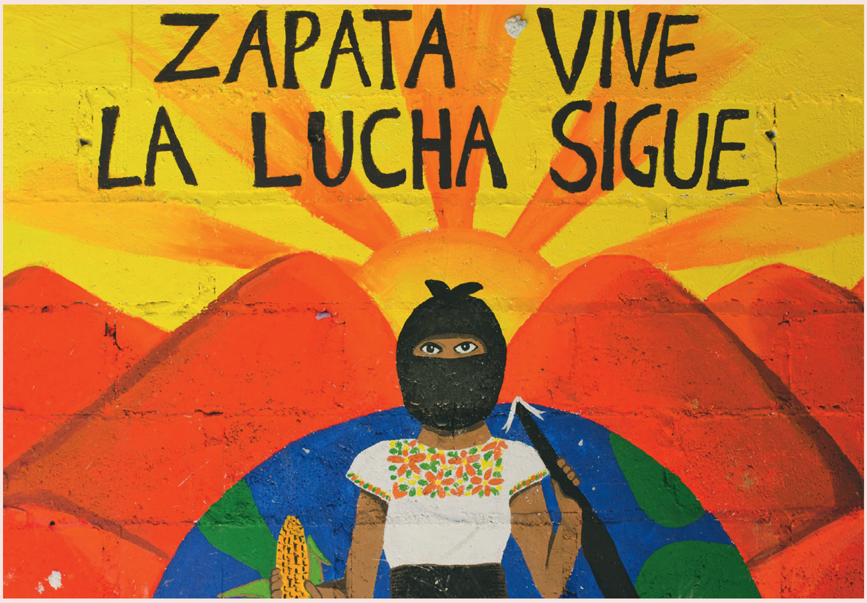


FIGURE 9.1 Mural, Oventic, August 2013: http://chiapas.mobilities.ca

This position was strengthened considerably when, in 2013, a young computer programmer working for the US National Security Agency (the NSA) called Edward Snowden blew the whistle on how a US-led international consortium (US, UK, Canada, Australia, and New Zealand) were collecting and monitoring millions of people's everyday lives online, not only Americans but also citizens of other countries. The techno-economic and political repercussions of these revelations, which came 2 years after the *Wikileaks* organisation leaked documents, and footage implicating US military in human rights abuses in Iraq and Afghanistan, are still emerging.

At this point we need to pause to return to just what people mean when talking of the *Internet*, for this is a term that encompasses more than your latest mobile-phone app. It refers to an architecture of computerised infrastructures and software programs that interconnects local computer networks, submarine, and aerial telecommunications systems so that they can communicate with one another. Overlapping layers of computer protocols and internationally agreed to technical standards are the software codes governing how this 'network of networks' functions. Some legal theorists consider this a shift towards a situation in which 'code is law' (Lessig 2006). Recall that the early, world-wide-web applications that still provide ways for us to navigate around the Internet and the latest generation of commercial social media tools all operate through this infrastructure. It augments imperial and post-world war telecommunications pathways. These digitalised submarine and satellite transmissions are relayed through tubes, cables, wires, and radio signals. This is one reason why the physical geography of internet-based communications, like those of pre-digital telegraph and telephony, cluster around historically dominant powers; the North Atlantic, and now the Asian region.

In the second decade of this century Russia and China developed their own, competitive, albeit criticised, models for their citizens to access online goods and services, social media platforms, and mobile phone apps. *Yandex* is the search engine of choice in Russia, *Alibaba* is the Chinese equivalent of Amazon whilst *Tencent's Weibo* and *WeChat* are popular applications with a global reach for Chinese users, at

BOX 9.2 WEB 2.0 OR SOCIAL MEDIA?

When we speak of 'social media' we are referring to both a redesign of pre-existing web services and a business model of social networking sites – 'platforms' – that emerged after the 1990s wave of global financial crises and the 'dot.com' crash at the turn of this century (Mandiberg 2012; Van Dijck 2013). The current market-leader is Facebook, who also owns Whatsapp and Instagram. For millions of people, particularly in the Global South, these services *are* the Internet. Recent figures show that ~~over a~~ billion people, about ~~one~~ in seven people on the planet have a Facebook account – a 'community' larger than the population of many major nation-states (www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/). Companies like Facebook and Google (who owns YouTube) know more about us than we might care to think. This business model means that they have an investment in developing automated tools that can track us, but also govern who, and what content we see when online (Carmi 2016).

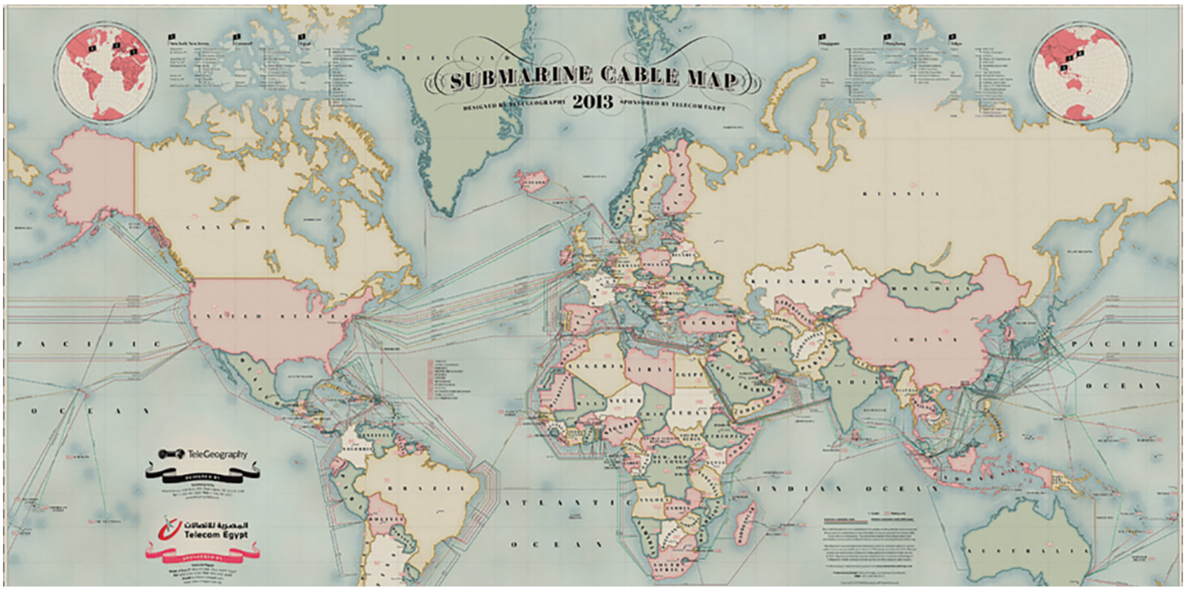


FIGURE 9.2 TeleGeography: Submarine Cable Map (2013)

What is meant by modernisation, and the various changes linked with this term, is discussed in many places in this book. See **Chapters 6 and 17**, for example.

For more on the nation-state see **Chapter 12** and for a discussion of imperial expansion see **Chapter 16**.

home and abroad. The powerful US corporations that control the lion's share of the world services have limited access to these huge markets, prompting some commentators to argue that these restrictions are contributing to the 'fragmentation of the global Internet' (Goldsmith and Wu 2006: 184). But there are good reasons for considering this term in the plural, rather than the singular. The *Internet* is a term that covers a complex, multi-layered system, services, hardware, and software. As a 'network of networks' we need to beware of reducing it to one sort of tool, a unified engineering artefact, or our favourite service. Like precursor inventions in media and communications that have become indispensable to politics, culture, and society, internet technologies are socio-historically constructed. What they are seen to promise and what they deliver are bound up in discourses of international development – progress and modernisation. The role played by science and technology in these grand narratives undergirds the rise of nation-states, the age of empire and, as some argue, the emergence of a post-Westphalian world-order (Fraser 2007; Haraway 1990).

ILLUSTRATIVE EXAMPLE
POLITICAL UPRISINGS AND INTERNET GEOPOLITICS

This section illustrates how internet-dependent media and communications operate as sociocultural artefacts, historically situated designs, and expressions of political economic power that have material and symbolic dimensions, civic and military ramifications. By regarding the Internet, a shorthand for these techno-economic and sociocultural technologies, as historically constructed, we can start seeing where and why civil society organisations, corporate powers, and state actors converge but also diverge in their respective versions of past 'internets' and visions for the future.

First we look at power struggles *through* the Internet: struggles taking place on the web and, nowadays, through social media. Then we turn to power struggles *over* internet-policy agendas: contestations over ownership and control of strategic aspects of internet design, terms of access, cultures of use, along with emerging contestations around content-management and the handling of our personal data.

The revolution has not been tweeted

The ever-growing applications that link our mobile phones to all sorts of internet-based services became prominent in mass protests in 2011 that led to the overturning of some authoritarian governments in North Africa and the Middle East. In Tunisia and Egypt mass demonstrations on the streets and online mobilisation led to the toppling of the Ben Ali and Mubarak regimes respectively. The subsequent wave of protests around the region is now referred to as the *Arab Uprisings*. As protesters using their mobile phones sent a stream of messages and images around the world, mainstream news media-outlets picked up and re-circulated this content. ~~Global media coverage, the outcomes and aftermath of these uprisings went hand in hand even though there were differences from place to place.~~ These events and their precursors in Mexico, Iran, and Myanmar – the Zapatistas, Green and Saffron movements respectively – represent how the ways people make use of contemporary media and communications and sociopolitical transformations are interrelated. Whatever the global brand may be (and these are constantly changing), these events underscore the many ways in which citizens deploy everyday online services to expose injustice, challenge powerful social and political institutions, and overthrow repressive rulers.

Dubbed 'citizen journalists' these participants, and established bloggers in the region, then circulated (re-tweeted or posted) these images and slogans around the world through personal and community social networking sites, in English but also in Arabic (El Dahshan 2012). This worldwide, persistent coverage of events through unofficial channels beat the professionals in getting the news scoop. They were also able to bypass attempts to restrict or censor content before going on air in this way.

Methods of controlling the media in wartime are discussed in **Chapter 8**.

The unremitting flow of tweets and mobile-phone footage conveyed a more immediate, more compelling sense of what was going on as images and analyses from these citizen journalists overwhelmed the usual editorial practices of mainstream print and TV news-desks. Almost immediately journalists resorted to using this unedited content in order to meet their production schedules, often without verifying or cross checking the source and, initially, without clear guidelines about how to convey this material to their audiences. Debates continue today about the impact of non-professional (social) media content on the production and consumption of news around the world. Meanwhile journalists maintain blogs and social media accounts, and news corporations like the BBC develop their Facebook and web-based outlets in turn.

During but also since these uprisings led to regime change in the region, blogger-journalists and human rights activists continue to be imprisoned, tortured, and persecuted by the authorities: Egypt's current military ruler, President Abdel Fattah el-Sisi, is one case in point. This is one approach to stifling civic unrest online and on the ground: punish those who report on events. Another tactic became apparent as events unfolded: cut transmission. In 2011 during the height of the Egyptian uprisings and

BOX 9.3 THE ARAB UPRISINGS

In December 2010 a market-seller set himself on fire in Tunisia in protest at ongoing police violence. This event sparked a series of protests that spread across the whole region. In Tunisia, Egypt, and Libya they led to the ousting of authoritarian regimes, despite violent repression on the ground, and persecution of dissidents who were active online. In Bahrain, Syria, and in Saudi Arabia the authorities crushed protests there. These mass movements were notable for their occupation of public spaces, such as Tahrir Square in Cairo, and for the way protesters, linking across the region and abroad, used commercial social media to publicise events that were being repressed, and censored by their governments. These tactics – online and on the ground – inspired the Occupy movement around the US, Europe, and other parts of the western world against global inequalities and poverty.

They also inspired protesters in Turkey during the 2015 occupation of Gezi Park in Istanbul.

For an interactive timeline of events, see www.theguardian.com/world/interactive/2011/mar/22/middle-east-protest-interactive-timeline

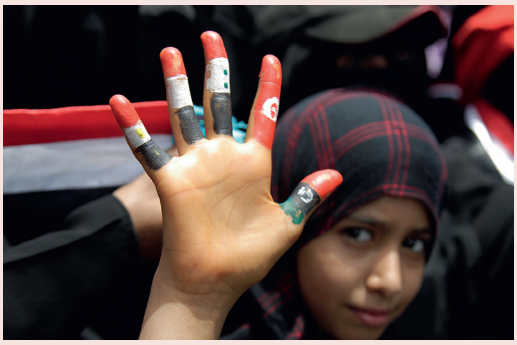


FIGURE 9.3
Arab Spring – Yemen: a girl raises her hand with her fingers painted with flags of Yemen, Egypt, Syria, Tunisia, and Libya as she marches during a demonstration to demand the ousting of Yemen's President Ali Abdullah Saleh in the southern city of Taiz, 22 June 2011.
Photograph: Khaled Abdullah/Reuters

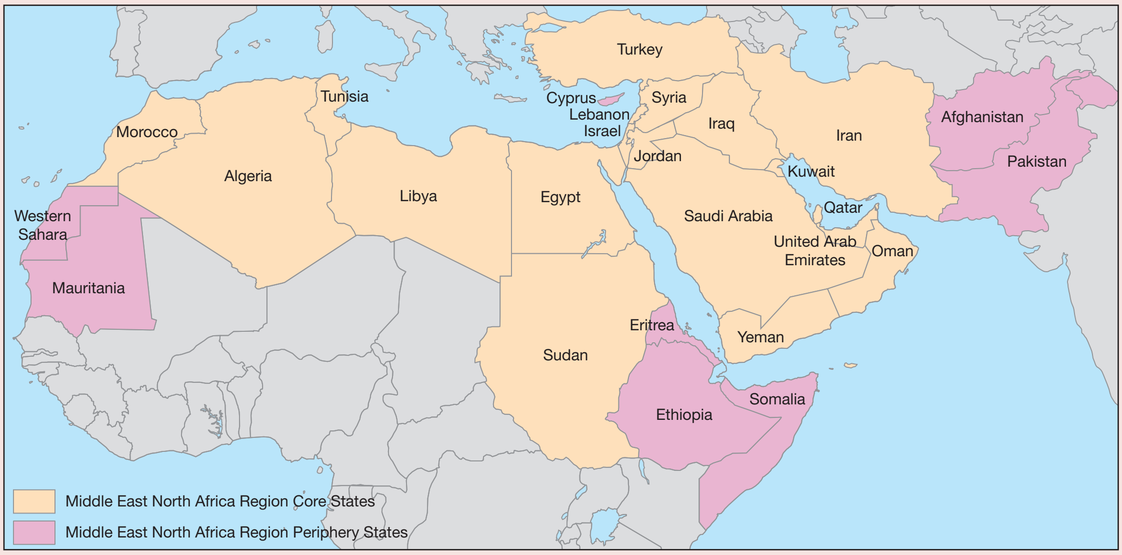


FIGURE 9.4
Map of Middle East and North Africa

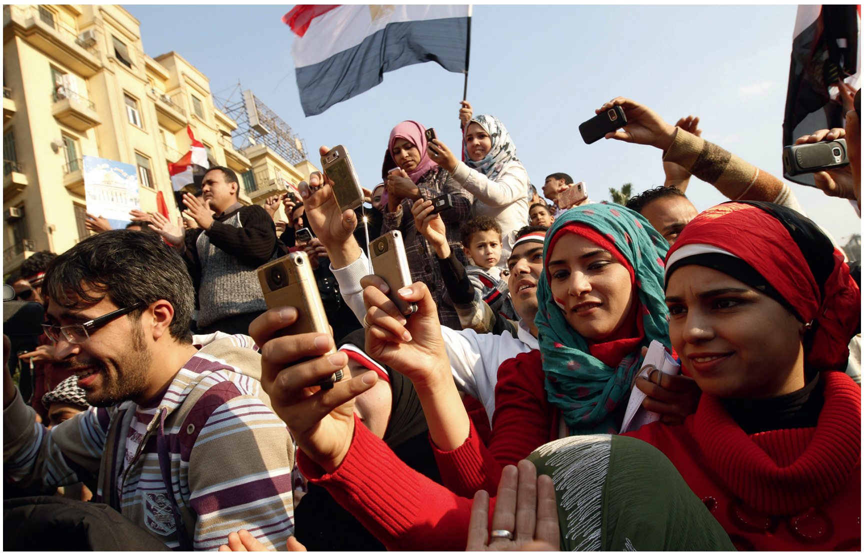


FIGURE 9.5
Protestors use mobile phones. Photograph: AFP/Getty Images

occupation of central Cairo, the beleaguered Mubarak government, in partnership with Vodafone, cut telecommunications access, depriving demonstrators in Tahrir Square from using their mobile phones to send messages. Overnight this revolution could no longer be tweeted. The response from media and civil rights activists in the West was swift. Vodafone was widely condemned for its collusion with the Mubarak regime.

This incident encapsulates the ways in which the same technology can be used for competing ends; here the former authoritarian regime and a transnational corporation joined forces to obstruct the right to freedom of expression, and freedom of the press. Attempts to control both transmission and the message are not new, just harder to do successfully as the speed and variety of communications outlets increase and the entry-threshold for ordinary users becomes easier to cross. The stakes have been raised though as government agencies (law enforcement and intelligence services) have started to develop their own internet-policy agendas. In a previous case from the Middle East and North Africa, evidence of violence during clashes between protesters and Iranian government forces after the elections in 2009 had also been widely disseminated by mobile phones – on YouTube, via Twitter, and on Iranian-based and Western blogs. The government moved swiftly by deploying an array of technical tools to filter, redirect and so censor dissident content (Sreberny and Khiabany 2010).

Governments in the Internet's heartlands are also becoming more proactive in this regard for reasons of national security, law and order, cultural integration, or the protection of minors. Examples include the strict regulation of internet access and use by the Chinese government, EU measures against online pornography, the UK government's attempt to control mobile phone-access during the 2011 London riots, and the 2016 *Investigatory Powers Act* that enables intelligence services to collect all communications data from UK citizens and residents. Control of access to the media and the message in periods of civil unrest and war has been the concern of governments throughout history, intensifying with the arrival of television, and now internet-media and communications.

The use of media in war, and how it has developed over time, is the subject of **Chapter 8**.

But it is not just governments who track and collect information about us when we are online, or who are able to control the terms of internet access and use. Major internet service providers (ISPs for short), global corporations, also collect vast amounts of data for what they argue is market research or customer service. But they also cooperate, voluntarily or under duress, with governments in ways that recall the example of Vodafone in Egypt mentioned above. In 2010, Yahoo! and Google came under fire for complying with the Chinese authorities' request for personal data and preventing access to offending websites respectively. In early 2012, Twitter announced that it was now company policy to remove tweets from users on the instructions of any host countries, albeit on a case-by-case basis ~~and with full transparency~~. The company, along with other Tech Giants, ~~have~~ been coming under increasing pressure to take measures against forms of online abuse such as Hate Speech, or Revenge Porn (Datta 2017). But these measures run up against constitutional and international law, and norms protecting free speech and freedom of expression.

Many politicians and celebrities have Twitter accounts. The current US President, Donald Trump, with over 42 million followers, is very vocal on Twitter. Former president Barack Obama has over 96 million.

These global players are aware of the fine line they walk between compliance and defiance of national regulations, international law and norms, or in the area of ~~content versus service provisions~~. Their responses range from agreeing to 'take-down orders' of a host country, in the case of China, Pakistan, or France for example (Deibert 2008), to being active in civil society-led campaigns against any sort of internet censorship. For example, when sued in France for hosting a sale of Nazi memorabilia, Yahoo! blocked the sale even though as a US-based company they are not liable under French law. Google bans content in China but it also filters searches in Germany and France according to their respective regulations. Facebook can restrict access to content, based on who is viewing and whether the content is legal in a particular country. These decisions have consequences for regulators and company policy, and for the world's *netizens* (McKinnon 2014). For every service that is blocked, an alternative route can be found; anonymising and privacy-enhancing applications such as Virtual Private Networks (VPN), The Onion Router (TOR), and other encryption services for Email uses, such as Pretty Good Privacy (PGP), are popular ways to thwart online snooping or data-tracking by third parties to protect your privacy, and that of your sources if you are a journalist. These actions and responses all challenge a number of international norms such as national sovereignty – state control over territories in 'meatspace'. They are putting national and international judiciaries under pressure to take into account that what people and power-holders do in 'cyberspace' (Franklin 2013: 2014–15, note 5) matters as well.

Who controls the Internet?

It appears that states and private actors stand on opposite sides of the fence on questions of who should decide how the Internet, in part or as a whole, *should* be run. These questions have become more prominent in the wake of the above events and in gradual recognition that how we use the Internet is formative, not simply a side issue in national and global politics. In successive UN consultations at least we can see a range of overlapping and competing discussions about the role that internet-access can play in combating global poverty and other socio-economic inequalities (around race, gender, and class), as a motor for promoting development twenty-first century-style (UN 2000, 2015; UNHRC 2014).

'No single actor controls every single hub of cyberspace' (Giacomello *et al.* 2009: 206).

To this end, the UN General Assembly undertook to hold a new series of 'high-level summits' in 2003 in order to 'build a global consensus' on the best way to govern the Internet (United Nations General Assembly 2000). The Internet Governance Forum is the latest in these UN-brokered initiatives to address the *global* policy implications of today's media and communications. UNESCO hosted the first meetings of what is known as the New World Information and Communications Order (NWICO) in the 1970s (Frau-Meigs *et al.* 2014). The second set of meetings, the World Summit on the Information Society, or WSIS (2003–5), was hosted by the International Telecommunications Union. The WSIS began with great hopes on the part of civil society participants in Geneva in 2003, enthusiasm that was tempered by the last summit in 2005 in Tunis, a meeting marked by waves of women's rights and human rights protests against the Ben Ali government's crack-down on access and use of the country's limited internet services (WSIS Civil Society Caucus 2003, 2005).

The Internet Governance Forum (IGF) followed up these summits with its first meeting in 2006, renewed for another 10 years in 2015. What sets the WSIS and IGF consultations apart is the way they are premised on a more inclusive form of participation. This 'multistakeholder participatory model' allows all-comers, including representatives from non-accredited organisations, or individuals (academics and students for instance) to sit at the table with civil society organisations, corporate representatives, and governments in settings usually reserved for diplomats and official delegations. Whilst to its critics largely a talk-shop, and to its supporters an indispensable space for advocacy and networking with a more diverse range of participants, IGF meetings are but one venue in which these various 'stakeholders' mingle. The outcomes of these consultations and accompanying preparations are part of a burgeoning annual calendar of meetings around the world that is increasingly accessible online, as a public record. This makes these processes, personalities, records of events, and decisions objects of academic inquiry.

This raises the question, regularly asked by attendees, practitioners, and scholars, about whether these sorts of events are where the real decisions take place, not in national legislatures, international treaty-making organisations, by the so-called technical community, or in company boardrooms. The slow grinding of well-oiled diplomatic and institutional cultures in multilateral institutions that play a role in 'framing the world' (Bøås and McNeill 2004) appears at odds with the rapidly changing global market in internet-based goods and services, or in popular uptake of both non-profit and commercial tools.

GENERAL RESPONSES
REGULATION, CENSORSHIP, AND RIGHTS

The above examples illustrate the intimate, multi-layered relationship between major technological advances in world communications, societal and political economic transformations, and modes of analysis. Responses to these challenges range from the highly specialised (technical operating standards within the 'technical community' for instance), to the legal (tussles between national and international authorities about jurisdiction over data-flows), to the normative and sociocultural concerns (articulating

For another discussion of the implication of regulation and its absence see **Chapter 17** on the 'informal' economy.

human rights online, addressing digital divides based on geographical, gender, or race inequalities). This section looks at three interconnected responses to the growth in internet-access and use at the intersection of global business and politics: (i) attempts to upgrade intellectual property and copyright in the face of stiff opposition from free and open software (F/OSS) communities, and 'free downloading' advocates; (ii) tracking, monitoring, and censoring access and online content; and (iii) the development of human rights and principles frameworks for decision-making on design, access, use, content, and data-management.

Regulating the digital

In late 2011 and early 2012, an internationally orchestrated mobilisation united grassroots groups, peer-to-peer platforms such as Wikipedia, and major companies against two bills before the US Congress: the Protect IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, or PIPA) and the Stop Online Piracy Act or SOPA. These widely publicised protests benefitted from earlier mobilisation against an international trade agreement being negotiated at the intergovernmental level, the Anti-Counterfeiting Trade Agreement, ACTA. Currently signed by many members of the Organization for Economic Co-operation and Development (OECD) yet opposed vehemently by grassroots groups and NGOs within signatory countries, this agreement was a precursor to the Protect IP Act and the Stop Online Piracy Act. All three initiatives targeted practices, communities, and non-proprietary applications that emerge from how individuals and dedicated networks (such as fan-bases) make use of the Internet to create and disseminate art and culture, alternative forms of knowledge (e.g. Wikipedia), DIY cultures, and forms of support and community (e.g. for sexual or ethnic minorities) that are not adequately accounted for in neither the jurisprudence nor the business model of individual property rights. Online campaigning (petitions, official blackouts from leading service providers) and offline (demonstrations around the world and intense lobbying on Capitol Hill in Washington) contributed to the withdrawal of all three initiatives.

This was heralded as a victory for 'internet freedom' even as these consumer-centred protests did not settle thorny questions around whether proprietary forms of copyright are good or bad for national economies, or for the arts and culture. For instance, is downloading films or music, without paying for it, a crime – 'online piracy' – or does litigation from powerful copyright-holders stifle freedom of expression, and cultures of online sharing? These protests highlighted how existing intellectual property rights regimes were struggling to cope with a surfeit of 'free' content circulating beyond their control. Their opponents argue that this emerging domain, a creative – digital – commons needs defending against the vested interests of the US-dominated *culture industries*, represented by the Motion Picture Association of America (MPAA), and U.S. Chamber of Commerce for instance.

A CBS News article by Stephanie Condon outlines the main issues, www.cbsnews.com/news/sopa-pipa-what-you-need-to-know/, January 18, 2012.

The issues here are legally but also sociologically complex. Opponents of these moves to 'digitally manage' content available online, are embedded in the not-for-profit, DIY cultures of internet-facilitated communities that characterised the 1980s and 1990s. But the challenge to commercial interests and market power, when people share movies and music files without buying these products, predates internet-enabled networks; videotapes and audiocassettes are still popular forms of 'piracy' in many parts of the world. They also characterise the alternative worldview of many who came of age during the world-wide-web generation of online services, such as Napster (the pioneering app for music downloading), gaming, open discussion forums, and early examples of 'sharing economies' such as Couch Surfing (for free accommodation). The main bone of contention is that these moves, made in the name of protecting copyright, make online spaces a legitimate target for government and corporate tracking. On the one hand, critics see these regulatory moves producing a situation whereby fundamental rights and freedoms are eroded: freedom of information, education, and expression for instance. On the other hand, the tools and enforcement procedures that enable companies and police officers to track and prosecute so-called pirates (many of whom are children, or minors) do not have sufficient judicial oversight or democratic accountability. Moreover, comparable sorts of digital tracking could be used, indeed have been used, to persecute political dissidents.

Popular uses of internet-facilitated media and communications have always been a haven for alternative expressions of community and exchange based on non-commercial, non-proprietary relationships (that is, where access and use are not restricted by trademark, patent or copyright laws). These practices, and software applications developed for them, still constitute a formidable counter-cultural understanding of the sorts of community, knowledge, and communicative practices that networked communications enable. Longstanding peer-to-peer (P2P) networks and free/open-source (F/OSS) software advocates are now emerging as political players in Europe, and elsewhere under the Pirate Party banner. For economies in the Global South that generate much foreign exchange by providing cheaper versions of western (mostly US-owned) software applications and services, these sorts of regulatory moves also point to how the 'implementation of these blunt policy instruments will require more and more public-funded surveillance and censorship' of the Internet and its corollary media and communications devices and networks (Abraham 2012).

For discussions of the global economy and its impact in the Global South, see **Chapters 15, 17, and 20**.

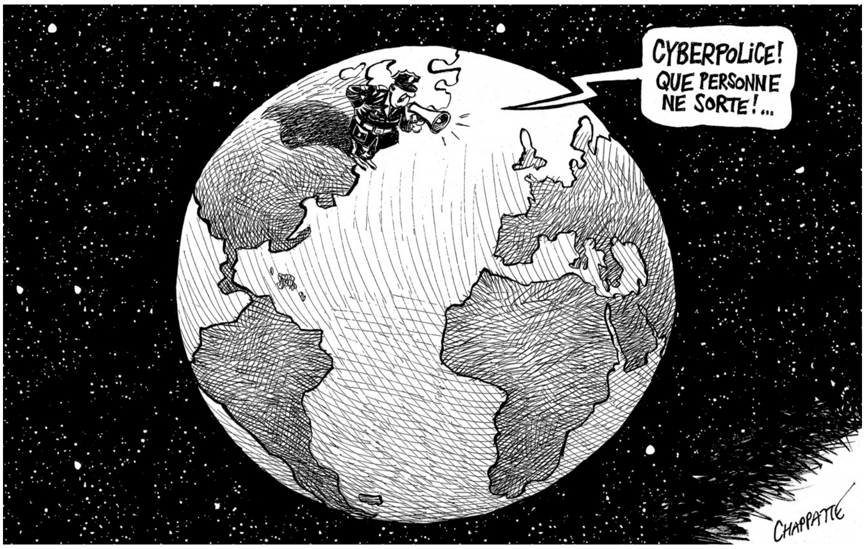


FIGURE 9.6
'Cyberpolice!'
By Chappatte, www.globalcartoons.com

Tracking, Filtering, or Censorship?

Has the media always involved censorship or bias? See **Chapter 8**.

Navigating the web in a relatively unencumbered way is possible because the Internet's transmission infrastructure and accompanying protocols are 'open', meaning that they have not been encrypted. We can traverse the web with relative impunity on an everyday level. Yet the digital footprint we leave behind makes it very easy for others to track us (Latour 2007). At the same time, public institutions such as schools, libraries and universities, and parents for that matter, have an interest in keeping track of where we are, and what we are doing. This includes taking measures to block content that is considered harmful or inappropriate for younger or vulnerable users. Since the 1990s, governments have been concerned about whether it is up to regulators or individuals, such as parents or educational institutions, to decide who can access online content. Yet at the same time, all these activities have become the object of increasingly pervasive forms of monitoring by such authorities but also for market research. All major service providers (also known as internet intermediaries) have increasingly sophisticated tools to track, collect, and then make sense of our personal data in order to 'optimise' the product, and maximise advertising revenue. Our private lives online, indeed we ourselves, are now the product as our behaviour, personal settings and 'user preferences' become the core business for service providers and advertisers.

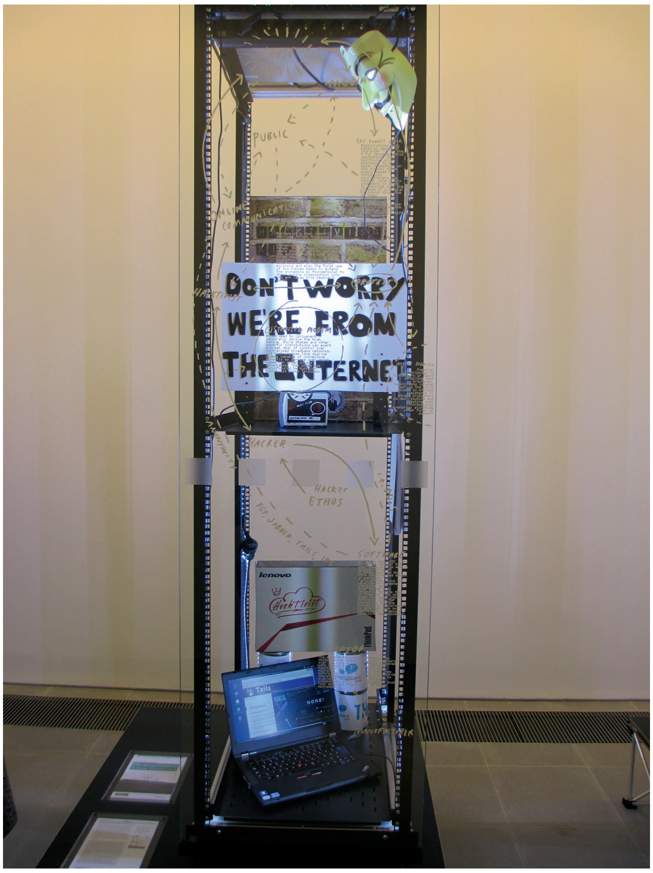


FIGURE 9.7
'Don't Worry, We're from the Internet', Artist, Simon Denny, Still from *Products for Organising*, 2015 (Photo, M.I. Franklin)

This shift has changed the rules of the game for governments, businesses, and ordinary people. R&D and consumer goods that can link to the Internet are now big business, from the 'Internet of Things' ('smart' refrigerators or electricity meters that digitally track our use, and upload these data on to company databases) to the 'Internet of Toys' (where safety standards and suitable privacy controls remain under-developed). Through our mobile phones, large-scale urban development projects are now based on connecting us to computer networks that link our consumer electronics to our bodies, in the home and on the road. We also provide data through the latest in networked 'wearables', such as wristwatches or fitness monitors: an 'Internet of Brands'.

These innovations are being developed at a faster pace than many governments and international standards-making bodies can keep up with. This disconnect between what is technically possible and what is legally or morally appropriate also opens the way for more malevolent uses of digital technologies: both to commit crimes and to persecute individuals or minorities without due process or full accountability.

One innovation, called *Deep Packet Inspection*, illustrates this paradox, as data-tracking and online surveillance become standard operating procedures in internet-connected societies. Deep Packet Inspection works from within the transmission infrastructure so ordinary people are not aware that it is affecting what they access and what they eventually see. This application basically performs a form of triage on the substantive content being transmitted through the network at the point a service provider or other agent controls access. Along with their usefulness for both censoring content and allowing a commercial edge for competing services these sorts of automated filtering and sorting technologies behind our screens undermine the operating principle of 'network neutrality' (Belli and Marsden 2017). They are also integral to a growing global market in cyber-weapons. For example, the Boeing-owned tool, Echelon, was deployed by the Mubarak regime to track protester messages; other Deep Packet Inspection tools were used in Ben Ali's Tunisia, and by the military junta in Myanmar.

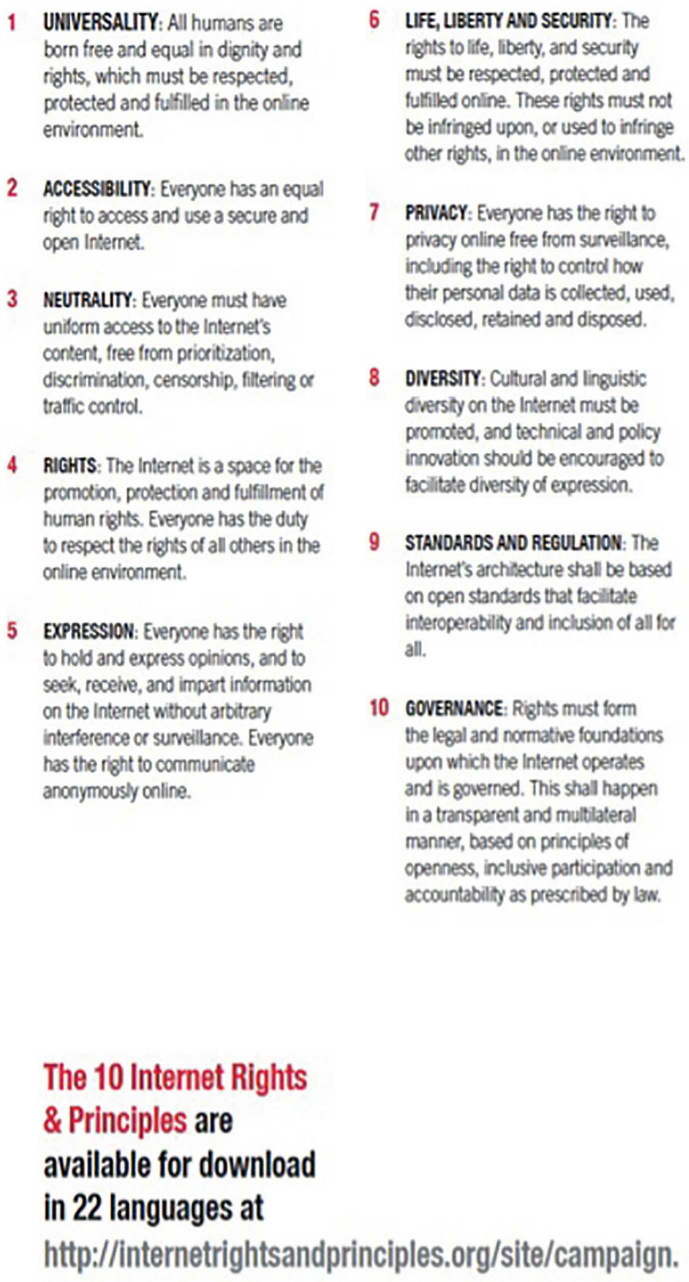
Human Rights for the Internet?

At the third UN Internet Governance Forum meeting in Hyderabad in 2008, a coalition of NGOs, grassroots groups, representatives from intergovernmental organisations, and the private sector, along with academics, set up the Internet Rights and Principles Coalition (IRPC). The aim was to develop precursor campaigns linking media, and now internet-policymaking to human rights norms (Hamelink 1998; Jørgensen 2006), and do so in a legally rigorous but also technically correct and accessible format for all sectors: judiciaries, legislatures, civil society organisations. The outcome of these efforts was the *Charter of Human Rights and Principles for the Internet* (IRP Coalition 2011 [2014]). Based on the 1949 Universal Declaration of Human Rights and subsequent treaties, the charter was a crowd-sourced effort that used 'collabowriting' tools online, discussions based on an email list along with face-to-face meetings, and web conferencing tools. The main objective was to make explicit how the Internet is more than a technological edifice or business. It is also a 'people-centred medium' with environmental, legal, and sociocultural implications.

Note that the three–four generations of treaties and covenants comprising the UN Bill of Rights have not all been ratified by all member-states. They remain the object of much political and cultural debate as **Chapter 25** points out.

Launched in 2011 the IRPC Charter, comprising the full charter of 21 Articles (IRP Coalition ~~2014~~; 12–27) and the *Ten Internet Rights and Principles* (IRP Coalition

201~~4~~: 7), has established itself as an authoritative framework for making explicit the human rights implications of how we use the Internet, and for how others may use the Internet against us. The IRPC Charter developed alongside, and inspired, a number of intergovernmental, national, and 'multistakeholder' declarations articulating rights and principles for a range of internet-inflected issues from privacy through to cybersecurity,



1 **UNIVERSALITY**: All humans are born free and equal in dignity and rights, which must be respected, protected and fulfilled in the online environment.

2 **ACCESSIBILITY**: Everyone has an equal right to access and use a secure and open Internet.

3 **NEUTRALITY**: Everyone must have uniform access to the Internet's content, free from prioritization, discrimination, censorship, filtering or traffic control.

4 **RIGHTS**: The Internet is a space for the promotion, protection and fulfillment of human rights. Everyone has the duty to respect the rights of all others in the online environment.

5 **EXPRESSION**: Everyone has the right to hold and express opinions, and to seek, receive, and impart information on the Internet without arbitrary interference or surveillance. Everyone has the right to communicate anonymously online.

6 **LIFE, LIBERTY AND SECURITY**: The rights to life, liberty, and security must be respected, protected and fulfilled online. These rights must not be infringed upon, or used to infringe other rights, in the online environment.

7 **PRIVACY**: Everyone has the right to privacy online free from surveillance, including the right to control how their personal data is collected, used, disclosed, retained and disposed.

8 **DIVERSITY**: Cultural and linguistic diversity on the Internet must be promoted, and technical and policy innovation should be encouraged to facilitate diversity of expression.

9 **STANDARDS AND REGULATION**: The Internet's architecture shall be based on open standards that facilitate interoperability and inclusion of all for all.

10 **GOVERNANCE**: Rights must form the legal and normative foundations upon which the Internet operates and is governed. This shall happen in a transparent and multilateral manner, based on principles of openness, inclusive participation and accountability as prescribed by law.

The 10 Internet Rights & Principles are available for download in 22 languages at http://internetrightsandprinciples.org/site/campaign.

FIGURE 9.8
TEN INTERNET RIGHTS AND PRINCIPLES. From the Charter of Internet Rights and Principles for the Internet (IRP Coalition 2~~01~~4: 7)

corporate social responsibility to forms of online espionage (Franklin 2013: 138 passim, 2015; Kulesza and Balleste 2015).

In these early years it was not widely recognised that international human rights standards and advocacy, the online environment (some call this cyberspace), and our lives offline – which is now less and less of our days according to some reports – are interconnected in law, theory, and policy practice. That these interconnections are now officially recognised is partly due to leadership from, and advocacy within, intergovernmental bodies (Council of Europe 2014; La Rue 2011; Pillay 2014; UNHRC 2014).

The IRPC Charter has managed to bring a fuller spectrum of international human rights treaties and covenants into the same frame as techno-economic discussions about how best to run the Internet. In this respect, the Internet as a technological system was not only the object of this early exercise in cross-sector cooperation to articulate what human rights have to do with internet-policy agendas or R&D. It was also the means by which the Charter emerged and was circulated.

This interconnection between the present and future decisions became clearer for onlookers after Edward Snowden made public the extent to which major western powers were abusing existing human rights norms by tracking innocent people online without due cause. Expressing these ongoing and new connections between uses of internet-technologies and existing human rights frameworks calls power-holders, public and private, to account.

BROADER ISSUES
GLOBAL FUTURES

Being online, enjoying hanging out with friends or calling home, purchasing – or downloading – ~~free~~ apps for news and entertainment generates forms of trans-border interconnectedness, in real-time, in ways that are distinct from telephone conversations or live TV. These are communicative cultures, experiences and relationships that are no longer defined by face-to-face forms of physical proximity, or the sorts of 'communities' that national broadcasting and news media outlets provide. We are all using the Internet to connect with others in non-embodied, supraterritorial, instantaneous, and multi-sited ways. These practices bring human society, individuals, and communities into closer and closer intimacy with the 'thinking machines' (Quintas 1996) that now govern our daily lives, open windows on to our world, and allow others to access what we do, think, and feel.

For a discussion of 'imagined communities' see **Chapter 12** and for a discussion of the news media see **Chapter 8**.

The jury is still out as to whether all these conveniences, and wider changes that these refinements bring augur well for civic life, national well-being, or even the planet: internet uses are a major factor in debates about causes and solutions for human-induced climate change (Oghia 2017). There are also ongoing debates about the historical if not political significance of these technologies, in light of other inventions such as the wheel, the printing press, the telephone, steam power or electricity. For optimists and pessimists alike the Internet, however defined, has become part of the latest chapter in the grand narrative of progress and development through science and technology.

Several broad themes for the study of global politics emerge from these issues.

Does technology drive such developments, or do politics and social factors drive technology?

Futures and pasts

First there are historical points to remember. As a telecommunications architecture, information resource, and way to communicate, the Internet has been around for about 40 years. It is only in the last 25 years that it took off in popular terms around the world. Since 2004, the rise to dominance, in market and social terms, of the previously discussed Web 2.0 business applications has changed the terms of debate. This global reach impacts on how much autonomy state actors have to assert their authority over the sociopolitical power that these 'commercial sovereigns' wield (McKinnon 2014).

This relatively short chapter in the history of world communications as digital networked systems – the modern printing press dates from the mid-fifteenth century, the telephone from the late nineteenth century – is also one that is still being written. Today's big brands in services, consumer gadgets, or software packages can very quickly become yesterday's news. Some already are. The way ordinary people, communities, and power-brokers now enter and exit cyberspace – the online environment – and architectures that sustain these practices are refashioning levels of analysis, the exercise of power, and resistance to it. How we use the Internet, and how the Internet 'uses' us, plays a role in the emergence of newer power hierarchies around sovereignty, territorial jurisdiction, ownership, and control of the world's media and communications.

Can you think of any examples of ones that have become 'yesterday's news'?

For all these reasons future visions for the Internet has become an advocacy goal for a range of agendas to refine its surveillance and commercial capabilities, or to redesign it with more environmentally sustainable, more socially inclusive operating principles that respect, rather than undermine, our fundamental rights and freedoms. The idea of 'privacy by design' promoted by the Council of Europe is one example. These views argue that it is not the duty nor the role of citizens to make these decisions on their own. Governments have an obligation, under national and international law, to ensure that these technologies sustain rather than deplete human life. This is even more so, activists argue, when these same state actors pass laws that legitimate practices that animate a digital, online incarnation of George Orwell's Big Brother (from his novel, *Nineteen Eighty-Four*); practices that Edward Snowden exposed in 2013 (Nyst 2017).

Various forms of activism are discussed in this book: environmentalism (**Chapter 4**); feminist movements (**Chapter 5**); religious movements (**Chapter 6**); grassroots democracy (**Chapter 14**); anti-capitalist movements (**Chapter 18**); and anti-war movements (**Chapter 26**), for example.

Rethinking world order in a digital, online context

As user-generated content straddles parochial, personal and global domains of action and reflection, jurisdictional struggles over the practices and content of online practitioners, at home and abroad, does too. The Internet, as a constellation of overlapping, computerised processes and services based on the 24/7 operations of supraterritorial layers of transmission networks, permits more than one way of being online, more than one way to express yourself, or to find a like-minded community. Alongside the latest services owned and controlled by private and state-owned corporations (as is the case in China and Russia for instance), there are many older, lo-tech applications still in use. Old-school Email is one example of how successive generations of electronic communications inform and overlap rather than instantly supersede one another.

When considering the broader implications of how we use the Internet we need to beware of reiterating instrumentalist or determinist understandings of the interplay

BOX 9.4 DONNA HARAWAY

In the late 1980s, Donna Haraway published her *Cyborg Manifesto*, an essay in which she presented an alternative vision of future 'fruitful couplings' between humans and machines that can shake entrenched inequalities based on class, gender, and race. Haraway argues, following Foucault, that human life, machines, and technological systems have become increasingly intertwined. The promises of hi-tech solutions, for what may be sociocultural, or political issues need to be critically evaluated. If not we become complicit in how the powerful can use these devices to dehumanise, or perpetuate inequalities along the lines of race, gender, and class. One example is the poor labour conditions in the global electronics and digital assembly lines that workers in the Global South, women particularly, have to endure.

FIGURE 9.9
Donna Haraway with Cayenne, 2006. Photograph: Rusten Hogness

between politics, society, and technology. As Donna Haraway observed, in the early decades of ~~the~~ networked computers: 'We are living through a movement from an organic, industrial society to a polymorphous, information system. from the comfortable old hierarchical dominations to the scary new networks . . . of domination' (1990: 203)

Commercial and foreign-policy led moves to transform core features of internet-design, and the underlying principles for how people access any services, are tech-driven visions of the future that are contestable. As more parts of the world go online, non-Western and less advantaged populations and groups in the Internet's heartlands leave an ever-larger digital and carbon footprint behind, ready to be tracked by public and private agents of networked surveillance and social control.

Who 'we' are influences how we use the Internet

The way different actors use these technologies – spontaneously or more strategically – makes a difference to the sorts of stakes they have in its future. States have always been active in adopting national technological and now digital agendas that serve changes in economic and foreign policy priorities. Despite the international outcry over Edward Snowden's exposure of the *disproportionate* uses of online surveillance tools (Necessary and Proportionate 2014), western governments are now passing laws to allow these forms of mass online surveillance in the name of cyber-security and counter-terrorism measures. Premised on regarding citizens and residents as potential criminals, or terrorist threats, before proven otherwise, these legislative interventions are as much political decisions as they are hi-tech articulations of state power at the online–offline nexus.

From the point of view of consumer rights-advocates, the ability to exercise technical tools that can provide leverage for what people do in cyberspace demands

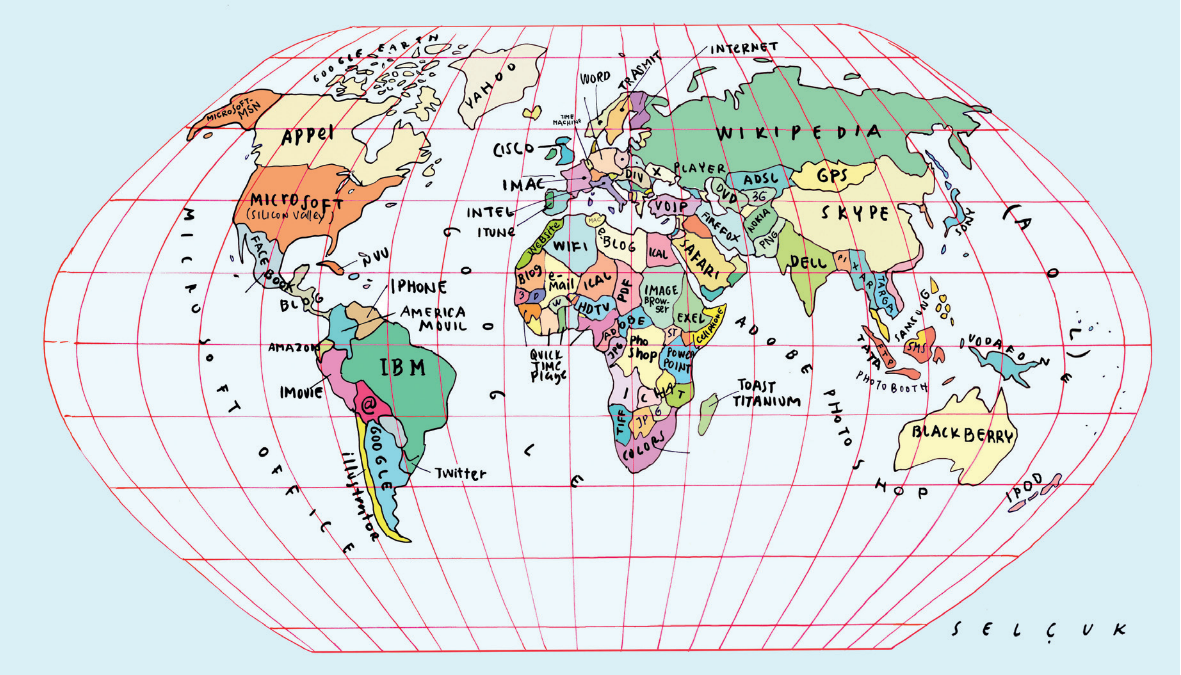


FIGURE 9.10
Selçuk, *Le Monde diplomatique* (2010)

greater accountability from government authorities. But it also requires more transparency from commercial operators about what they, in turn, are doing with all that information they have about our private and public lives online.

The Internet we use is currently owned and controlled by powerful western-based corporations: Google, Apple, Facebook, and Amazon (GAFA), followed closely by other tech giants such as Tencent (Weibo, We Chat), Microsoft (who owns Skype, a popular way to phone home online), Wikipedia, or Twitter.

For more on the role of corporations in the global economy, see **Chapters 15, 16 and 17**, for example.

Civilian (including academic uses and applications in the USA) and government-sponsored programs of public service access (such as the Minitel service in France) have all played a major role in the development of the Internet, as have laissez-faire policies for letting people go online to gather, exchange ideas, and challenge the status quo in what was once relative safety from indiscriminate snooping. Since the turn of this century at least, the ability to go online anonymously or assume another persona has all but disappeared, for all but the most tech-savvy communities. Moreover, the North American–western European axis of the early Internet's geographical dominance is starting to shift eastwards and southwards, in terms of the statistics of mobile phone and social media uptake. This is where global incumbents like Google and Facebook are setting out to compete with state-owned telecommunications operators in offering relatively limited forms of internet-connectivity to the remaining billions.

I will end this section by way of one more example: the changing 'privacy policies' of Internet service providers who set the terms of use and access for the majority of services we use when online.

Privacy and public policy matters

Visible on the right-hand side of millions of screens, the following phrase announced a change in Google's privacy policy effective from 1 March 2012:

> We're changing our privacy policy and terms. This stuff matters.
>
> (Google Banner 2012)

On clicking the 'find out more' link, at the end of the presentation of what was or was not changing to the way this corporation tracks, stacks, and stores data based on millions of people's individual web-searching activities, the reader would come upon the following legal stipulation:

> Notice of change: 1 March 2012 is when the new Privacy Policy and Google Terms of Service will come into effect. If you *choose* to keep using Google once the change occurs, you will be doing so under the new Privacy Policy and Terms of Service.
>
> (Google Banner 2012, emphasis added)

Many media and Internet rights activists and advocacy groups in the Global South as well as Washington DC regard the ability that service providers, in this case one of the world's largest, have to dictate the terms of use like this troubling for accountability and transparency; terms of use (that box you have to click to continue) are notoriously difficult to read for lay-persons. These concerns relate to objections to the linking up of databases that facilitate government security and law enforcement agencies combining forces with each other, and then with service providers in order to access and process even more of our personal data (Council of Europe 2014; Kulesza and Balleste 2015; Pillay 2014).

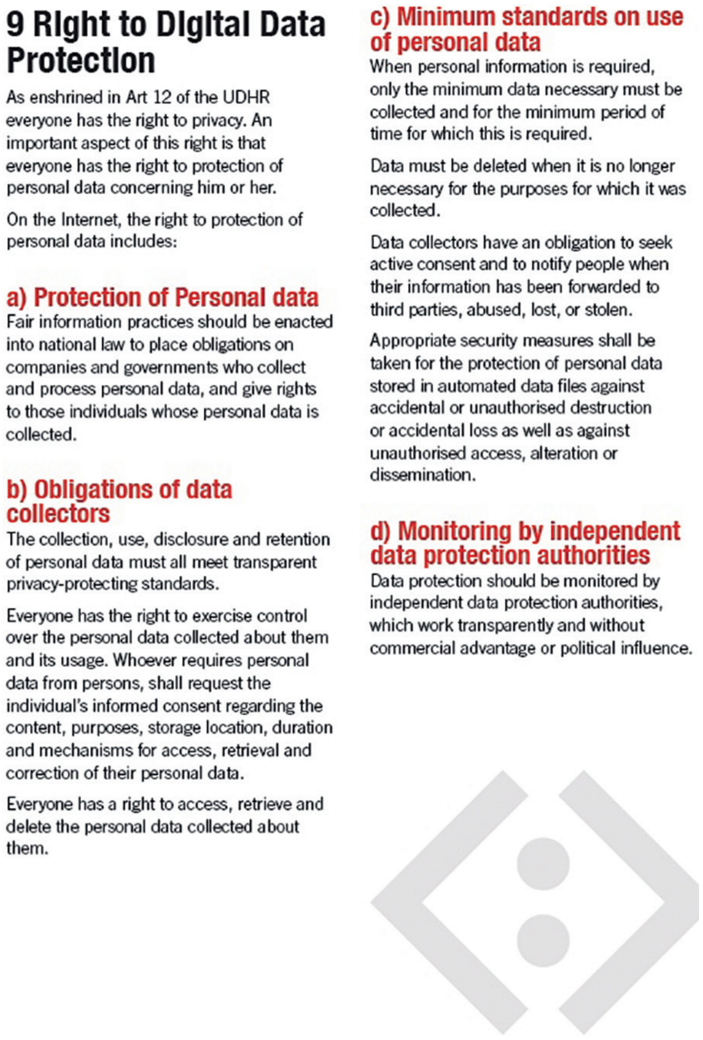
'Beware: your digital imagination leaves traces' (Latour 2007).

CONCLUSION

Public services are now going digital, requiring us to access and upload information online: tax returns, health records, academic records, passport details when travelling and so on. Even with new data protection rules ~~coming into~~ force, in the EU for instance, the question remains: who watches the watchers, and to whom are they accountable for any accidental, or deliberate breaches of our fundamental rights and freedoms under the law?

As access to internet-media and communications becomes integral to the exercise of power – and resistance – simmering struggles over ownership and control of the software and hardware that run the Internet are thrown into relief (Franklin 2013; Giacomello and Ericksson 2009; Mueller 2002). Governments, corporations, and civil society organisations have conflicting priorities in this regard: who foots the bill for ensuring resilient operations on the one hand and, on the other, affordable, socially just and environmentally sustainable services for all. These divergent agendas are putting pressure on traditional decision-making bodies as the everyday realities of how people

'The computer is not only a machine or tool: it is also a medium that determines *how* we perceive just as much as *what* we perceive' (Deuber-Mankowsky 2008: 993).



9 Right to Digital Data Protection

As enshrined in Art 12 of the UDHR everyone has the right to privacy. An important aspect of this right is that everyone has the right to protection of personal data concerning him or her.

On the Internet, the right to protection of personal data includes:

a) Protection of Personal data

Fair information practices should be enacted into national law to place obligations on companies and governments who collect and process personal data, and give rights to those individuals whose personal data is collected.

b) Obligations of data collectors

The collection, use, disclosure and retention of personal data must all meet transparent privacy-protecting standards.

Everyone has the right to exercise control over the personal data collected about them and its usage. Whoever requires personal data from persons, shall request the individual's informed consent regarding the content, purposes, storage location, duration and mechanisms for access, retrieval and correction of their personal data.

Everyone has a right to access, retrieve and delete the personal data collected about them.

c) Minimum standards on use of personal data

When personal information is required, only the minimum data necessary must be collected and for the minimum period of time for which this is required.

Data must be deleted when it is no longer necessary for the purposes for which it was collected.

Data collectors have an obligation to seek active consent and to notify people when their information has been forwarded to third parties, abused, lost, or stolen.

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

d) Monitoring by independent data protection authorities

Data protection should be monitored by independent data protection authorities, which work transparently and without commercial advantage or political influence.

FIGURE 9.11 Charter of Human Rights and Principles for the Internet, Article 9: Right to Digital Data Protection, IRP Coalition ~~2014~~; 19

access and use goods and services online constantly move in and out of national jurisdictions within seconds. Classical notions of territorial sovereignty and its landed borders of political or economic accountability, legality and legitimacy, law and order, no longer suffice for these cyberspatial domains.

The Internet, broadly defined, and as it morphs into the succeeding generation from this generation of mobile apps and social media brands (we cannot live without or try to resist), has already made a difference *because* of the ways we, and others, use these services. The domestic and foreign policy implications of these 'entanglements' affect those who are not (yet) linked in as well, within and between nation-states. The sociopolitical and economic geographies of access matter therefore. A person in the US, whether an activist, lobbyist or congress-person, accesses and uses their Internet in different ways from those doing so from a European, Chinese or Indian vantage point. Ordinary citizens have different perceptions of what is possible, and experiences of what is on offer online, than do digital rights activists, terrorists, journalists, and those *refuseniks* wanting to log-off and unplug. The question to ask ourselves at this point in the internet-timeline is what kind of Internet – or internets – do we envisage for sustaining future generations of 'digital natives', and on whose terms of design, access, and use?

FURTHER READING

Neil Spiller's *Cyber-Reader* (2002) provides access to landmark texts. Mandiberg (2012) brings us into the Web 2.0 business era. Jørgensen (2006) and Franklin (2013, 2014) look at cases at the intersection of human rights, gender, and internet politics. Freedman *et al.* (2006) cover the intersection of political activism, media reform, and internet policymaking. Lessig (2006) and Mueller (2002) are landmark texts dealing with techno-legal and regulatory issues deep in the system, and behind the screen. Holmes (2007), Dahlberg and Siapiera (2007), and Lovink (2012) provide analyses from critical cultural studies and social theory ~~that inspired~~ Haraway (1990). The Academy award-winning documentary film *Citizen Four* (Dir. Laura Poitras), and biopic, *Snowden* (Dir. Oliver Stone) provide live footage, and re-enactments of the events around Snowden's whistleblowing in 2013. Another documentary film, *A Good American* (Dir. Friedrich Moser), focuses on earlier attempts by cybersecurity experts at the NSA – William Binney, Kirk Wiebe, Diana Roark, and Thomas Drake, to address the civil liberties implications of online surveillance tools. The *Human Rights and the Internet* series on openDemocracy, at www.opendemocracy.net/hri, features analyses and commentaries on emerging issues. In all these sources you can learn more about the spectrum of intergovernmental, activist, and advocacy networks – longstanding and more recent – active in these domains.

REFERENCES

Abraham, Sunil (2012) 'Sense and Censorship', Centre for Internet and Society, January 31. http://cis-india.org/Internet-governance/sense-and-censorship.

Belli, Luca and Christopher T. Marsden (2017) *European Net Neutrality, at Last?* Human Rights and the Internet, openDemocracy, 4 October 2016. www.opendemocracy.net/luca-belli-christopher-t-marsden/european-net-neutrality-at-last.

Bøås, Morten and Desmond McNeill (eds.) (2004) *Global Institutions and Development: Framing the World?* (London and New York: Routledge).

Carmi, Elinor (2016) 'Whose data is it anyway?' Human Rights and the Internet, openDemocracy, 13 June 2016. www.opendemocracy.net/digitaliberties/elinor-carmi/whose-data-is-it-anyway.

Council of Europe (2014) *The Rule of Law on the Internet and in the Wider Digital World*, Issue paper December 2014, Strasbourg: Council of Europe Commissioner for Human Rights. https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper%282014%291&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864.

Dahlberg, Lincoln and Eugenia Siapiera (eds.) (2007) *Radical Democracy and the Internet: Interrogating Theory and Practice* (London and New York: Palgrave Macmillan).

Datta, Bishakha (2017) *Belling the Trolls: Free Expression, Online Abuse and Gender*, Human Rights and the Internet, openDemocracy, 30 August 2016. www.opendemocracy.net/bishakha-datta/belling-trolls-free-expression-online-abuse-and-gender.

Deibert, Ronald J. (2008) 'Black Code Redux: Censorship, Surveillance, and the Militarization of Cyberspace', in Megan Boler (ed.) *Digital Media and Democracy. Tactics in Hard Times*, Cambridge, MA and London: MIT Press.

Deuber-Mankowsky, Astrid (2008) 'The Phenomenon of Lara Croft', in Michael Ryan (ed.) *Cultural Studies. An Anthology*, Malden, MA and Oxford: Blackwell Publishers.

El Dahshan, Mohamed (2012) 'Quit Twitter? No. Let's Trust It', *Guardian*, 28 January: 18.

Franklin, Marianne I. (2013) *Digital Dilemmas: Power, Resistance and the Internet* (New York and London: Oxford University Press).

——(2014) 'Sex, Gender, and Cyberspace', in Laura J. Shepherd (ed.) *Gender Matters in Global Politics: A Feminist Introduction to International Relations*, 2nd edn, London and New York: Routledge, pp 375–88.

Fraser, Nancy (2007) 'Transnationalizing the Public Sphere: On the Legitimacy and Efficacy of Public Opinion in a Post-Westphalian World' *Theory, Culture, and Society* 24, 4: 7–30.

Frau-Meigs, Divina, Nicey Jérémie, Palmer Michael, Pohle Julia and Tupper Patricio (Eds.) (2012) *From NWICO to WSIS: 30 Years of Communication Geopolitics* (Bristol and Chicago: Intellect).

Freedman, Des, Cheryl Martens, McChesney Robert and Jonathan Obar (Eds.) (2016) *Strategies for Media Reform: Communication Research in Action* (New York: Fordham University Press).

Giacomello, Giampiero and Johan Ericksson (Eds.) (2009) 'Who Controls the Internet? Beyond the Obstinacy or Obsoleteness of the State', *International Studies Review* 11, 1: 205–26.

Goldsmith, Jack and Tim Wu (2006) *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press).

Google Banner (2012) www.google.co.uk/, 9 February.

Hamelink, Cees J. (1998) 'The People's Communication Charter', *Development in Practice* 8, 1: 68–74.

Haraway, Donna J. (1990) 'A Cyborg Manifesto: Science, Technology, and Socialist Feminism in the 1980s', in Linda Nicholson (ed.) *Feminism/Postmodernism*, New York and London: Routledge.

Holmes, Brian (2007) 'Future Map or How the Cyborgs Learned to Stop Worrying and Learned to Love Surveillance'. http://brianholmes.wordpress.com/2007/09/09/future-map/

Internet Governance Forum (IGF) (2008) *Workshop #52. ICTs and an Environmentally Sustainable Internet. Another Challenge of Connecting the Next Billion Internet Users.* www.intgovforum.org/cms/2008-igf-hyderabad.

Internet Rights and Principles Coalition (IRP Coalition) (2011 [~~2014~~]) *Charter of Human Rights and Principles Booklet*. http://internetrightsandprinciples.org/site/

ITU/WSIS (2005) *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6 (Rev. 1)-E, November 18, 2005. www.itu.int/wsis/docs2/tunis/off/6rev1.html.

Jørgensen, Rikke F. (ed.) (2006) *Human Rights in the Global Information Society* (Cambridge, MA: MIT Press).

Kulesza, Joanna and Ray Balleste (Eds.) (2015) *Cybersecurity: Human Rights in the Age of Cyberveillance* (Lanham, MD: Rowman and Littlefield/Scarecrow Press).

La Rue, Frank (2011) *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. Human Rights Council, UN General Assembly, A/HRC/17/27, 16 May.

Latour, Bruno (2007) 'Beware, your imagination leaves digital traces', *Times Higher Literary Supplement*, 6 April. http://docs.google.com/View?docid=ad6vvc428w8_103gzv2fdgf.

Lessig, Lawrence (2006) *Code Version 2.0* (New York: Basic Books).

Lovink, Geert (2012) *Networks without a Cause: A Critique of Social Media* (Oxford UK: Polity Press).

Mandiberg, Michael (2012) *The Social Media Reader* (New York and London: New York University Press).

McKinnon, Rebecca (2014) *'Playing Favourites' in Guernica: A Magazine of Art and Politics*, February 3, 2014. www.guernicamag.com/features/playing-favorites/.

Mueller, Milton (2002) *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge, MA: MIT Press).

Necessary and Proportionate.Org (2013) *International Principles on the Application of Human Rights to Communications Surveillance*, July 2013. https://en.necessaryandproportionate.org/text.

Nyst, Carly (2017) *The End of Anonymity? Trump and the Tyranny of the Majority*, Human Rights and the Internet, openDemocracy, 14 September 2017. www.opendemocracy.net/digitaliberties/carly-nyst/end-of-anonymity-trump-and-tyranny-of-majority.

Oghia, Michael J. (2017) *Internet Access, Sustainability, and Citizen Participation: Electricity as a Prerequisite for Democracy?* Human Rights and the Internet, openDemocracy, 11 August 2017. www.opendemocracy.net/hri/michael-j-oghia/internet-access-sustainability-and-citizen-participation-electricity-as-prerequisite.

Pillay, Navi (2014) *The Right to Privacy in the Digital Age*, Office of the United Nations High Commissioner for Human Rights, Human Rights Council, A/HRC/27/37, 30 June 2014. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

Ruggie, John (2011) *United Nations Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, Report to the UN Human Rights Council, A/HRC/17/31, 21 March 2011. https://business-humanrights.org/sites/default/files/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf.

Scholte, Jan Aart (2000) *Globalization: A Critical Introduction* (New York: St. Martin's Press).

Spiller, N. (2002) *Cyber-Reader: Critical Writings for the Digital Era* (London and New York: Phaidon Press).

Sreberny, Annabelle and Gholam Khiabany (2010) *Blogistan: The Internet and Politics in Iran* (London and New York: I. B. Tauris).

UN General Assembly (2015) *Sustainable Development Goals*. www.un.org/sustainabledevelopment/sustainable-development-goals/.

UN Human Rights Council (2014) *Resolution A/HRC/26/L.24: Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development*, Twenty-sixth session, Agenda item 3, UN General Assembly, 20 June 2014. http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/26/L.24.

United Nations General Assembly (2000) *Millennium Development Goals*. www.un.org/millenniumgoals/.

Van Dijck, José (2013) *The Culture of Connectivity: A Critical History of Social Media* (London and New York: Oxford University Press).

WSIS Civil Society Caucus (2003) *Shaping Information Societies for Human Needs: Civil Society Declaration to the World Summit on the Information Society*, 8 December. www.itu.int/net/wsis/docs/geneva/civil-society-declaration.pdf.

——(2005) *Civil Society Declaration: Much More Could Have Been Achieved*, document WSIS-05/TUNIS/CONTR/13-E, 23 December. www.worldsummit2003.de/download_en/WSIS-CS-summit-statement-rev1–23–12–2005-en.pdf.

For a range of further resources supporting this chapter, please visit the companion website for *Global Politics, 3rd Edition* at www.routledge.com/cw/edkins/