INTERNET POLICY REVIEW
Journal on internet regulation

Volume 5 | Issue 3

The politics of surveillance policy: UK regulatory dynamics after Snowden

Arne Hintz
Cardiff School of Journalism, Media and Cultural Studies, Cardiff University, United Kingdom, hintza@cardiff.ac.uk

Lina Dencik
Cardiff School of Journalism, Media and Cultural Studies, Cardiff University, United Kingdom, dencikl@cardiff.ac.uk

Published on 26 Sep 2016 | DOI: 10.14763/2016.3.424

Abstract: The revelations by NSA whistleblower Edward Snowden have illustrated the scale and extent of digital surveillance carried out by different security and intelligence agencies. The publications have led to a variety of concerns, public debate, and some diplomatic fallout regarding the legality of the surveillance, the extent of state interference in civic life, and the protection of civil rights in the context of security. Debates about the policy environment of surveillance emerged quickly after the leaks began, but actual policy change is only starting. In the UK, a draft law (Investigatory Powers Bill) has been proposed and is currently discussed. In this paper, we will trace the forces and dynamics that have shaped this particular policy response. Addressing surveillance policy as a site of struggle between different social forces and drawing on different fields across communication policy research, we suggest eight dynamics that, often in conflicting ways, have shaped the regulatory framework of surveillance policy in the UK since the Snowden leaks. These include the governmental context; national and international norms; court rulings; civil society advocacy; technical standards; private sector interventions; media coverage; and public opinion. We investigate how state surveillance has been met with criticism by parts of the technology industry and civil society, and that policy change was required as a result of legal challenges, review commissions and normative interventions. However a combination of specific government compositions, the strong role of security agendas and discourses, media justification and a muted reaction by the public have hindered a more fundamental review of surveillance practices so far and have moved policy debate towards the expansion, rather than the restriction, of surveillance in the aftermath of Snowden.

Keywords: Edward Snowden, Blanket surveillance

Article information

Received: 21 Feb 2016 **Reviewed:** 13 May 2016 **Published:** 26 Sep 2016

Funding: The article is based on research conducted as part of the collaborative project 'Digital Citizenship and Surveillance Society: State-Media-Citizen Relations After the Snowden Leaks' which was based at Cardiff University from 2014 to 2016 and funded by the UK Economic and Social Research Council (ESRC).
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/politics-surveillance-policy-uk-regulatory-dynamics-after-snowden

Citation: Hintz, A. & Dencik, L. (2016). The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review*, *5*(3). DOI: 10.14763/2016.3.424

INTRODUCTION

The revelations by whistleblower Edward Snowden on mass surveillance[1], first published in newspapers such as The Guardian from early June 2013, have transformed our understanding of how our online activities are monitored. Snowden exposed a range of different means by which security agencies collect and analyse internet communication and metadata. The public learnt about how data is harvested from the internet's backbone cables through programmes such as Tempora and collected from internet companies and social media platforms through intelligence efforts like Prism, Muscular and Squeaky Dolphin. The US National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ) have run programmes to break encryption and to hack into communications infrastructure. High-profile cases of both business and political espionage were exposed, but for normal citizens the degree of what is typically called 'bulk' data collection and analysis, i.e. the collection and potential monitoring of vast amounts of people's online communication, was, arguably, the most significant revelation.

The leaks led to a variety of concerns, public debate, and some diplomatic fallout. Key questions concerned the legality of the interventions of security agencies, the extent of state interference in civic life, and the protection of civil rights in the context of security. At the core of many of these debates was the regulatory framework of data collection and interception. In several countries, policy change has been discussed and, in some, implemented. Among them is one of the key protagonists of the surveillance practices exposed by Snowden - the UK. A new legislative framework, the Investigatory Powers Bill, was proposed by the UK government in late 2015 and has been reviewed and revised during the course of 2016.

In this article we will explore the transformations of surveillance policy after Snowden by tracing the emergence of, and debate over, this new law. We ask what has shaped the legal and regulatory framework in the UK and what are the processes that affect its current transformation and potential future direction. Our perspective focuses on the politics of policy-making, which regards policy as a site of struggle between different social forces (cf. Freedman,

2008; Pohle, Hoesl, and Kniep, 2016). We are interested in the legal status quo and governmental decisions just as much as in the work of norm-building institutions, civil society and public debate.

We will review eight different dynamics that, we will argue, have affected the regulatory environment in the UK: 1) governmental context; 2) policy norms; 3) court rulings; 4) civil society advocacy; 5) technological development; 6) private sector interventions; 7) media coverage; and 8) public opinion. While only a small section of these address laws and regulations in a strict sense, all of them have played, to different degrees, a role in shaping the policy environment of digital surveillance. Based on the case study of the Investigatory Powers Bill, we suggest that these dynamics are relevant factors for understanding the transformation (or lack thereof) of surveillance policy after Snowden.

In the following, we will first outline the conceptual background of policy and surveillance that we adopt for this article, then provide a brief summary of recent surveillance policy development in the UK, and finally discuss the role of each of the eight dynamics outlined above in affecting the post-Snowden policy debate in the UK and shaping the Investigatory Powers Bill. This case study will demonstrate the value of an interdisciplinary approach that can draw from different strands of communication policy research in order to understand developments in contemporary surveillance policy.

This article draws on research conducted as part of the collaborative research project "Digital Citizenship and Surveillance Society: UK State-Media-Citizen Relations After the Snowden Leaks" which was based at Cardiff University from 2014 to 2016. The research has included 50 expert interviews with policymakers, civil society campaigners, industry representatives, technologists and journalists, as well as focus groups with a cross-section of the British public, policy document analysis, and media content analysis.[2]

ACTORS AND FORCES IN COMMUNICATION POLICY

To explore the forces and dynamics that have shaped surveillance policy in the UK, we will begin by reviewing the contemporary context of media and communications policy. This policy environment has been described as "a complex ecology of interdependent structures" with "a vast array of formal and informal mechanisms working across a multiplicity of sites" (Raboy, 2002: 6-7). Classic forms of national (governmental and parliamentary) policy have been complemented by the activities of non-governmental actors in both national and transnational spaces. National policy has "become embedded within more expansive sets of interregional relations and networks of power" (Held and McGrew, 2003: 3), and policy authority is now located at "different and sometimes overlapping levels – from the local to the supra-national and global" (Raboy and Padovani, 2010: 16). In particular, regional institutions such as the European Union (EU) have assumed regulatory authority in some areas, and international institutions such as the various United Nations (UN) agencies, world summits and trade agreements provide relevant frameworks for national legislation.

Civil society organisations and businesses are increasingly part of multi-stakeholder processes that expand policy authority beyond governments. Civil society actors typically intervene into policy debate by setting agendas, providing expertise, exerting public pressure, lobbying and public campaigns, and by lending or withdrawing legitimacy to policy goals, decisions and processes (Keck and Sikkink, 1998). While civil society groups ground this role in their strong

normative and value-based positions, the business sector can invest significant material resources. Google, for example, has invested over $16 million in lobbying the US government in 2015 (Open Secrets, 2015).

Yet in addition to influencing public policy, non-state actors increasingly create and pre-empt regulation. We see this, for example, in the development of standards, protocols and practices that have become de-facto cornerstones of communication technology. The creation of data exchange protocols, file formats and communication standards is a latent form of policymaking outside the spotlight of public policy (DeNardis, 2009; Lessig, 1999). The 'terms of service' (ToS) that regulate the use of social media and other internet platforms constitute a further form of private sector-based policy that sets the boundaries and conditions for free speech and privacy on commercial online spaces (Youmans and York, 2012). Private sector rules such as ToS demonstrate a trend towards the privatisation of communication policy (Hintz, 2015; Leistert, 2015) and a "shift of the responsibility for monitoring and policing Internet conduct onto strategically positioned private sector intermediaries" (Mueller, 2010: 149). Civil society activists have responded to these shifts in policy authority by addressing the private sector directly - for example, through campaigns such as #FBrape in 2013 to have social media companies change their terms of service and content policies (Moyer, 2015), and through projects such as 'Ranking Digital Rights' (https://rankingdigitalrights.org/) that focus on corporate policies to advance user privacy and freedom of expression. Yet they have also created their own alternative infrastructure to bypass, rather than change, regulatory obstacles. This may include self-organised and non-profit communication platforms that aim at protecting user privacy (Hintz and Milan, 2013) as well as other 'privacy by design' strategies that incorporate concerns about civil rights into the technical infrastructure (Guerses, Troncoso and Diaz, 2011).

Such developments have been reflected in several strands of communications policy research that address the roles of different forces and dynamics in the shaping of the regulatory environment. Theoretical approaches informed by political-economic concerns have highlighted the conditions and implications of interactions between social forces, and have examined prevalent societal norms and ideologies that underlie and advance specific policy trends (Freedman, 2008; Chakravartty and Zhao, 2008). Similarly, field theory has investigated policy as a field of struggle in which different social actors create meaning (Pohle, Hoesl, and Kniep, 2016). Science and technology studies (STS) have highlighted the politics of technical architecture and the networked interactions of human and nonhuman actors (Musiani 2014), while social movement studies have focused on the interventions by non-state and non-commercial actors (Keck and Sikkink, 1998). Yet an emphasis of certain types of (mostly institutional) actors is predominant, and a systematic integration of less prominent forces, such as technological activists and media reporting, is rare (Hintz and Milan, 2013). In this article, we therefore argue for a comprehensive perspective that considers a wide range of social forces and dynamics.

For the field of surveillance policy such a perspective is important as it illustrates the interaction of public and private actors at different levels. While the Snowden revelations focused largely on state surveillance programmes carried out by agencies such as the NSA and GCHQ (The Guardian, 2015; Fidler, 2015), these programmes depend on the 'big data' generated through social media platforms for commercial profit that is at the heart of current surveillance trends (Lyon, 2014). It is this 'valorisation of surveillance' (Cohen, 2008) in which user data is mined and analysed that sustains the business model of corporate actors such as Google and Facebook. What is more, in the 'data mine' (Andrejevic, 2012: 71) of social media, the users themselves (voluntarily) generate (and, potentially, limit) the data that is processed by commercial

intermediaries and analysed by both corporate data brokers and state agencies (Trottier, 2015). Multiple processes of 'veillance' (Bakir, 2015) thus generate data flows, tracks and traces, implicating a wide range of stakeholders in how these processes are regulated and overseen.

AN OVERVIEW OF SURVEILLANCE POLICY IN THE UK

Data collection and analysis in the UK have been regulated by a jigsaw puzzle of different laws that each address specific aspects and practices. These have included the Data Protection Act of 1998 which controls access to and use of personal data. It provides limitations for data collection and sharing but also includes exemptions for the protection of "national security" and the prevention or detection of crime. The Regulation of Investigatory Powers Act (RIPA) from 2000, as amended by the Data Retention and Investigatory Powers Act 2014, allows a Secretary of State to authorise the interception of the communications of a specific individual but also of wide-ranging and vaguely defined types of traffic in bulk. These more specific regulations are underpinned by technology- and platform-specific laws, such as the Telecommunications Act of 1984 and the Wireless Telegraphy Act of 2006, and agency-specific rules such as the Intelligence Services Act from 1994 which provides the core legal basis for the surveillance activities by GCHQ (Brown, 2015).

These national rules are embedded in regional and international policy, such as the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) from 1998. Article 8 of the Convention guarantees everyone's "right to respect for his private and family life, his home and his correspondence" (Council of Europe, 1998). Moreover, the actors that intersect in the making of surveillance policy include national and regional courts and bodies that hear complaints about surveillance, such as the Investigatory Powers Tribunal (IPT) and the European Court of Human Rights (ECHR). Normative institutions such as the UN Special Rapporteurs on freedom of expression and on privacy influence the limits of acceptable behaviour for states, and civil society organisations and internet companies affect the course of policy development through their various means.

The Snowden revelations led to significant debates over surveillance policy in the UK and elsewhere but, initially, failed to generate a substantial overhaul of surveillance powers. On the contrary, government policy in the immediate aftermath of the Snowden leaks was marked by the continuation and expansion of surveillance powers. So, as the EU Data Retention Directive was revoked following a decision by the Court of Justice of the European Union, the UK government proposed and adopted 'emergency legislation' – the Data Retention and Investigatory Powers (DRIP) Act – which requires telecommunication operators to store 'communications data' (metadata) and thus continues key provisions of the Directive.

However, in October 2015, the government presented comprehensive draft legislation that would combine the fragmented legislative framework of data collection and analysis into one law. The draft Investigatory Powers Bill (IP Bill) is to regulate a wide range of surveillance practices – from bulk data collection to 'computer network exploitation' (i.e. hacking into targeted systems). The draft has been welcomed by many observers as it opens up many of the traditionally secret surveillance measures to public scrutiny and oversight, but its proposed measures have been criticised heavily for their excessive range and vague limitations (Hintz and Brown, 2016). The draft is currently under parliamentary review, which is to be concluded by the end of the year 2016.

The bill constitutes a major shift in British surveillance legislation, with potentially significant implications for surveillance policy elsewhere, and it also demonstrates the impact of the Snowden revelations. In the remainder of this article we will discuss a number of dynamics that shaped the draft Bill and thus formed a key part of the post-Snowden policy environment.

EIGHT DYNAMICS OF POLICY CHANGE AFTER SNOWDEN

1. GOVERNMENTAL CONTEXT AND POLITICAL COALITIONS

The Snowden revelations emerged when the UK government was formed by a coalition between the Conservative Party and the Liberal Democrats. Plans for a Communications Data Bill – nicknamed 'Snooper's charter' – were advanced by the Conservative majority in the coalition government before the revelations started but halted due to resistance by the junior party in the coalition, the Liberal Democrats, whose political agenda had a strong focus on civil rights. Instead, parliamentary commissions and reviewers were tasked with an investigation into the regulatory environment of surveillance (see point 2 below). This stalemate changed with the general election in May 2015, which led to a Conservative only government. One of the first announcements by Conservative ministers on the morning of their election victory was to move ahead with the bill (The Guardian, 2015c) that would expand data collection and, for example, require internet service providers and mobile phone companies to maintain records of users' internet browsing activity. The election thus opened a 'policy window' (Kingdon, 1984) to pursue a more aggressive surveillance agenda.

The institutional setting for developing the new bill favoured this agenda. The Home Office (which is responsible for domestic security) was placed at the centre of the process, whereas ministries dealing with digital communication and with civil liberties were left in a complementary role. This gave security and intelligence agencies closer access to the policy development debate than other actors, such as industry and civil society organisations (Hintz and Brown, 2016). Parliamentary scrutiny was limited for most of the drafting and review period, due to a combination of factors - a lack of knowledge of complex technological issues, a "certain deference to security agencies" (Interviewee 1, 2016) among politicians in the UK, and pressure from government (ibid.).

The goal to expand surveillance powers in the UK was reflected by developments in countries like France and Denmark, where new laws were proposed in response to terrorist attacks. In the US, on the other hand, the USA Freedom Act, adopted in May 2015, restricts data collection by state agencies and thus reversed a trend towards ever-increasing surveillance for the first time since the 1970s (Wizner, 2015). The recent communications law 'Marco Civil' in Brazil provides stronger protection of citizens' privacy and anonymity online.

2. POLICY NORMS

While the political and institutional context in the UK has pointed towards a broader surveillance agenda, a number of normative statements, declarations and reports suggested a different direction of policy change. Typically such documents are not legally binding but are recognised and, sometimes, responded to by national policymakers.

The coalition government commissioned the 'Independent Reviewer of Terrorism Legislation', David Anderson Q.C., to conduct a review of investigatory powers. His report, published in June

2015, did not fundamentally reject previous surveillance practices but criticised the British legal framework as 'fragmented', 'obscure', 'undemocratic' and 'intolerable', and called for a significant review and re-development (Anderson, 2015). Further reports were completed by the Intelligence and Security Committee of Parliament (ISC) and the Independent Surveillance Review of the Royal United Services Institute (RUSI), which called for a "democratic licence" for the surveillance activities of intelligence agencies (RUSI, 2015). These reports were instrumental in guiding and shaping the development of the IP Bill, and they provided a strong normative framework (and limitation) for the government's intended expansion of surveillance powers.

At the international level, several United Nations rapporteurs have condemned surveillance in no uncertain terms. A few days before the first Snowden leaks were published in June 2013, then-UN Special Rapporteur on Freedom of Expression and Opinion, Frank William La Rue, delivered a landmark report that highlighted the right to privacy as an essential requirement for the realisation of the right to freedom of expression (UN General Assembly, 2013). Since then, the current Special Rapporteur David Kaye published a report on the essential role of encryption and anonymity for people's rights to freedom of opinion and expression and to privacy (Human Rights Council, 2015). In 2015 the UN Human Rights Council appointed a new Special Rapporteur on the right to privacy who has since criticised the surveillance practices of, and insufficient legal restrictions in, countries such as the UK. While these UN reports have a less immediate effect on national policy development, they can underline and legitimise civil society advocacy and influence public debate.

3. COURT RULINGS AND LEGAL CHALLENGES

Legal challenges provided a further requirement for policy reform and offered direction for legislative change. Following the Snowden revelations, a number of UK and international campaign groups brought claims at national and international courts. Organisations such as Privacy International, Liberty and Amnesty International argued at the UK Investigatory Powers Tribunal (IPT) that various aspects of GCHQ's surveillance practices were unlawful. A first decision by the tribunal in December 2014 maintained that the agency's activities were compatible with the European Convention's privacy and freedom of expression guarantees, but subsequent decisions found some of these practices unlawful. This concerned, in particular, the sharing of data between GCHQ and NSA, and the spying on human rights organisations by GCHQ (Hintz and Brown, 2016).

Other organisations, including the Open Rights Group, Big Brother Watch, and Human Rights Watch, chose the European level and filed complaints at the European Court of Human Rights against the UK government. The European Court of Justice had already declared the EU's Data Retention Directive invalid in 2014, pointing out that the mass collection of internet data interferes with fundamental rights to respect for private life and to the protection of personal data. More recently, it revoked the safe harbor agreement between the EU and the US that allowed the transfer of personal data of European social media users to the servers of US-based internet companies.

The Snowden revelations provided essential facts, without which these legal challenges would not have been possible. As one civil society campaigner noted: "We have the Snowden documents as a compass (..) you need a compass to know what you're aiming at" (Interviewee 2, 2016). The court decisions have been significant in requiring action by policymakers and, at the same time, constraining the latter's responses. They have forced legislators to review existing practices and develop more robust policy frameworks.

4. CIVIL SOCIETY ADVOCACY AND CAMPAIGNS

The 'legal route' chosen by civil society organisations was complemented by a wider range of advocacy efforts. Organisations such as Privacy International, the Open Rights Group, Big Brother Watch, Article 19 and Liberty have regularly issued statements regarding their concerns about surveillance, have organised public debates, have lobbied legislators, and have grown significantly in membership. As an immediate response to the Snowden leaks, these groups and others formed a coalition – Don't Spy On Us – which combines some of this advocacy work towards a common campaign. Their voice, in this regard, has been significant in the specialised discourses around the draft IP Bill. They were increasingly seen as a constructive, knowledgeable participant in policy debates - according to one civil society campaigner they became "less seen as the angry voice and rather as a useful collaborative voice" (Interviewee 3, 2016).

Some organisations held public awareness-raising meetings across the country, and involved the public in campaigns such as 'Did GCHQ Illegally Spy on You?' (by Privacy International) which gained traction as a pressure tactic on the Investigatory Powers Tribunal. However, wider public protest to surveillance in the form of street protests has been far more limited in the UK, in contrast to larger 'Stop Watching Us' demonstrations in the US and 'Freedom not Fear' protests in Germany. Also, the ability to incorporate a broader political movement across civil society organisations in the UK has been restricted as concerns with and advocacy around surveillance issues have been largely confined to specific digital rights groups. Arguably, this has limited the impact and pressure of civil society on the UK government (Dencik et al., forthcoming).

5. TECHNOLOGICAL DEVELOPMENT AND STANDARDS

Digital rights activism has involved campaigning but, crucially, it has also extended to forms of prefigurative action that include the development of alternative tools and infrastructure. Technology activists have developed anonymisation tools such as the Tor browser[3], advanced the incorporation of strong encryption in email and other online data exchanges[4], offered self-organised and privacy-enhanced internet services such as riseup.net, and experimented with various methods of obfuscation in digital environments. While these strategies are still far from mass public adoption, they have increased since the Snowden leaks broke (O'Neill, 2015). Internet companies, too, have focused more attention on data security and user privacy, not least in response to criticism of their close interactions with state agencies prior to Snowden. These technological interventions - by both grassroots activists and industry - have influenced the capabilities of security agencies and the focus of policy debate. Both the British Prime Minister and the Home Secretary have called for limits to encryption and for legal backdoors to enable data monitoring by security agencies (Temperton, 2015).

Underneath the level of public and political debate, standards bodies have tried to respond to the vulnerabilities exposed by Snowden. Institutions such as the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF) and the World Wide Web Consortium (W3C) have established working groups to examine the incorporation of human rights in protocols and standards; have strongly condemned pervasive monitoring; and have advanced solutions to privacy threats. The involvement of security agencies in some standards bodies has led to controversies post-Snowden as the NSA had collaborated with the US National Institute of Standards and Technology (NIST) in the development of backdoors to a widespread encryption standard. Whilst this was known prior to 2013, the Snowden revelations prompted an examination of the processes. The IETF has consequently reviewed its use of NIST standards (Eden and Rogers, 2016).

6. THE PRIVATE SECTOR

Internet companies such as Google and Facebook have been at the core of the post-Snowden debate, partly because they collect a significant amount of user data, and partly because that data has been used by state agencies through programmes such as Prism. In addition, British politicians and security agencies have exerted significant public pressure on companies to comply with data requests by the state. GCHQ Director Robert Hannigan has called social media networks "terrorists' command and control networks of choice" (Hannigan, 2014) and Prime Minister David Cameron demanded that they "do more to co-operate with the intelligence agencies" (The Guardian, 2015b).

Many of the larger companies have been concerned about the implications of the Snowden revelations for user trust in their services and thus, ultimately, about the loss of customers. As one industry representative noted, the Snowden leaks led to a "massive loss in confidence from users, which had large ramifications for industry and resulted in a lot of work to try and regain that trust" (Interviewee 4, 2016). A coalition of tech companies including Apple, Facebook, Google and Microsoft issued a set of principles titled 'Global Government Surveillance Reform' (https://www.reformgovernmentsurveillance.com/) asking governments for a revision of surveillance practices and announcing an improvement to the security of user data by deploying encryption and pushing back on government requests. While this agenda may have been informed by public relations and marketing requirements, it has made some forms of state-based data collection more difficult. Perhaps more importantly, it has introduced tensions into the previously harmonious relationship between governments and the corporate sector and has separated, to some extent, the powerful forces of government and internet business (Wizner, 2015). Companies like Apple have strongly condemned the idea of opening backdoors to encryption systems, and have claimed that this would weaken the integrity of internet infrastructure as a whole (The Guardian, 2015d).

More broadly, the adoption of technical protocols, the involvement with public debate and direct interactions with legislators offer significant leverage and opportunity for the private sector to influence policy development and implementation. During the development of the IP Bill, the British IT industry was actively consulted by the UK government (Hintz and Brown, 2016).

7. MEDIA COVERAGE

While the dynamics that we discussed so far have a more direct influence on policy development, we will now turn to two final dimensions which have a less direct impact and are therefore often neglected in policy analysis. Yet, as the case of post-Snowden policy reform demonstrates, they play a significant role. The media coverage of surveillance, in particular, has generated the discursive framework within which policy is developed. The journalistic representation of the Snowden leaks can set agendas for public debate as it may investigate misconduct and require public officials to respond or, alternatively, legitimise government conduct. In the UK, parts of the media and, particularly, The Guardian, reported on the Snowden leaks and directed public attention towards the existence of programmes of mass surveillance, rose public awareness and thus aligned with the classic 'watchdog' function of the media. However, predominantly the media advanced justifications of mass data collection and monitoring, and research looking at a two-year period of mainstream British media coverage following the initial revelations has shown that the most frequent opinions covered in the media were largely supportive of mass surveillance efforts by both corporate and state actors (Wahl-Jorgensen and Bennett, 2016). The Snowden coverage unfolded within a larger - and long-established - ideological framework which positions national security and concerns over terrorism as a key regime of justification, largely legitimising this perspective (Hintz et al.,

2016). By contrast, more critical views that focused on the privacy rights of citizens were largely absent from the reporting. This bias in coverage was partly due to the fact that mediated debates were largely framed by elites, with politicians being by far the most frequently used sources (Wahl-Jorgensen and Bennett, 2016). This also meant that surveillance of political leaders, such as revelations regarding spying on Angela Merkel, was scandalised whereas mass surveillance of citizens was treated with significantly less urgency.

This pattern may not hold true around the world as debates over surveillance are shaped by social and political contexts. For example, German coverage of the Snowden revelations showed that the role of surveillance technologies in violating privacy and freedom was a more prominent theme of coverage there (Hintz, Dencik and Wahl-Jorgensen, 2016). However, in the UK and many other countries, the mediated debates have largely failed to ignite a broader debate around the democratic consequences of mass surveillance. Governments, accordingly, have only felt limited pressure to restrict surveillance and put more focus on the protection of human and civil rights. Instead, the strong emphasis on state security in media coverage pushed policy discourses towards an expansion of surveillance and allowed, or encouraged, governments to prioritise their role as providers of security over and above other potential roles (Wahl-Jorgensen and Bennett, 2016).

8. PUBLIC OPINION

Unsurprisingly, given the nature of media coverage, public response in the UK has been notably muted. Although opinion polls with the British public conducted in the immediate aftermath of the Snowden leaks have shown high levels of support for Snowden and his actions, concerns have persisted regarding the potential dangers of the media reporting on issues of state security (Cable, 2015). State surveillance of digital communications and online privacy matter to the British public, and research has shown that although the public think some surveillance technologies are useful for combating national security threats, they also believe these technologies compromise human rights and are abused by security agencies (Bakir et al., 2015). UK-based focus group research shows that there are particular concerns regarding the lack of transparency and legal safeguards for how and why personal data is collected. Also, many people would like to know more about, and have more control over, what happens to their data and would actively circumvent forms of surveillance if they were aware of alternatives and felt sufficiently skilled in their adoption (Dencik and Cable, 2016; Bakir et al. 2015).

This theme of public feelings of disempowerment with regards to 'bulk' data collection has also been prominent in research on public attitudes in the US where despite concerns with civil liberties, the predominant public response has been one of resignation (Turow, Hennesy, and Draper, 2015). Partly this has been explained by the institutionalisation of surveillance practices in the everyday life of ordinary people (Turow, McGuigan, and Maris, 2015) or the normalisation of surveillance as it has come to 'colonise the domains of emotion, symbolism and culture' (Wood and Webster, 2009: 264). As one member of a UK-based focus group said: 'I think because so much of what we do is capable of being collected now, I think we've gone beyond that point [of challenging the collection of data].' (Focus Group 1, 2015) Turow, McGuigan, and Maris (2015) have gone as far as describing the extraction of data (and its discriminatory effects) as a new 'social imaginary' in which individuals are being institutionalised into taken-for-granted values, habits and expectations. Although basing their argument on a study of the shifting nature of the retail space, such understandings can be applied to negotiations with surveillance more broadly, exemplified also by the widespread public internalisation of the 'nothing to hide, nothing to fear' discourse in relation to state surveillance (Dencik and Cable, 2016; see also Mols, forthcoming)

As Foucauldian notions of normalisation and discipline highlight (cf. Foucault, 1977), these processes in which norms of conduct are enforced through discursive practices and institutional sanctions (see also Wahl-Jorgensen and Bennett, 2016) are often an exertion of social control and can lead to a 'chilling effect' (Lyon, 2003) in people's movements, actions and communication, which undermines critical debate and dissident voices. Such 'effects' of the Snowden leaks have been particularly documented in the US such as in the survey carried out by the PEN American center with writers in which they found that writers are engaging in self-censorship as a result (PEN, 2013). Further studies have shown a reluctance amongst citizens to engage with politically sensitive topics online, such as a decline in 'privacy-sensitive' search terms on Google (Marthews and Tucker, 2015), a decline in page views of Wikipedia articles relating to terrorism (Penney, 2016), and a 'spiral of silence' in surveillance debates on social media (Hampton et al. 2014). Such an environment limits the possibilities for public concerns to be voiced and heard in any policy debate.

CONCLUSION

The Snowden revelations have led to intensified debates over policy reform. In the UK, one of the main actors identified in the Snowden leaks, a major reform project is currently underway that will transform the regulatory environment of digital surveillance and, potentially, provide a model for policy change in other countries. While providing a more transparent legislative framework, the proposed law largely combines (and expands) existing capabilities rather than reviewing them more thoroughly.

In this article, we have traced several dynamics that have contributed to the shaping of this legislative undertaking. We have argued that the new law is the result of a complex interplay of forces and contexts that have affected the transforming policy environment in the UK, have pulled the policy debate in different directions at different times, and have constrained its possible outcomes. Through a close reading of the policy debate and related concerns (such as media coverage and public opinion) and by conducting a wide range of interviews with stakeholders, we have identified eight dynamics and forces that have played a particular role in shaping post-Snowden surveillance policy. We propose that such an interdisciplinary approach that combines the focus of different strands within communication policy research is necessary to understand contemporary policy change in relation to surveillance.

With regards to the specific case of surveillance policy in the UK, we found that the kinds of states surveillance exposed by Snowden were met with criticism by parts of the technology industry, standards bodies and civil society, and that policy change was required as a result of legal challenges, review commissions and normative interventions. However a combination of specific government compositions, the strong role of security discourses, media justification and a muted reaction by the public have hindered a more fundamental review of surveillance practices so far and have moved policy debate towards the expansion, rather than the restriction, of surveillance in the aftermath of Snowden.

REFERENCES

Anderson, David Q.C. (2015) 'A Question of Trust – Report of the Investigatory Powers Review', https://terrorismlegislationreviewer.independent.gov.uk

Bakir, V. (2015) "The Veillant Panoptic Assemblage: Critically Interrogating Power, Resistance and Intelligence Accountability through a Case Study of the Snowden Leaks." Paper presented at the conference "Data Power" in Sheffield, 22 June 2015.

Bakir, V. et al. (2015) "Public Feeling on Privacy, Security and Surveillance" report by DATA-PSST and DCSS. Retrieved from http://sites.cardiff.ac.uk/dcssproject/files/2015/11/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf

Cable, J. (2015) "Working Paper: An Overview of Public Opinion Polls Since the Edward Snowden Revelations in June 2013". Cardiff University, Cardiff. Retrieved from http://sites.cardiff.ac.uk/dcssproject/files/2015/06/UK-Public-Opinion-Review-180615.pdf

Chakravartty, P., and Y. Zhao (2008) *Global Communications: Towards a Transcultural Political Economy*. Lanham: Rowman & Littlefield.

Cohen, N. (2008) 'The valorisation of surveillance: Towards a political economy of Facebook.' *Democratic Communiqué, 22*(1): 5-22

Council of Europe (1998) European Convention of Human Rights. https://www.echr.coe.int/Documents/Convention_ENG.pdf

DeNardis, L. (2009) *Protocol Politics: The Globalization of Internet Governance*. Cambridge: MIT Press.

Dencik, L., Hintz, A. and Cable, J.(forthcoming) 'Towards Data Justice? The ambivalence of anti-surveillance resistance in political activism' Special issue "Veillance and Transparency: A Critical Examination of Mutual Watching in the Post-Snowden, Big Data Era" in *Big Data & Society*

Dencik, L. and Cable, J. (2016) 'The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks' *International Journal of Communication, forthcoming*.

Guerses, S., C. G. Troncoso and C. Diaz (2011) 'Engineering privacy by design', Paper delivered at Computers, Privacy & Data Protection, 2011.

Eden, G., and M. Rogers (2016) 'The Role of Technical Standards in the Making of Surveillance Infrastructure', *International Journal of Communication, forthcoming*.

Fidler, D.P., ed. (2015) *The Snowden Reader*. Bloomington: Indiana University Press.

Focus Group 1 (2015) Focus group conducted in London by Lina Dencik. May 2015

Foucault, M. (1977) *Discipline and punish: The birth of the prison*. London and New York: Vintage

Freedman, D. (2008). *The politics of media policy*. London: Polity Press.

Hampton, K.N., Rainie, L., Lu, W., Dwyer, M., Shin, I., and Purcell, K. (2014) 'Social Media and the 'Spiral of Silence''. Pew Research Center, Washington, DC. Retrieved from http://www.pewinternet.org/files/2014/08/PI_Social-networks-and-debate_082614.pdf

Hannigan, R. (2014, November 3). The Web is a terrorist's command-and-control network of choice. *Financial Times*. Retrieved from: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3TywRsOQ2

Held, D., and McGrew, A. C. (2003). The Great Globalization Debate. In D. Held and A. G. McGrew (Eds.), *The Global Transformations Reader* (pp. 1-50). Cambridge: Polity Press.

Hintz, A. (2015) 'Social Media Censorship, Privatised Regulation, and New Restrictions to Protest and Dissent'. In L. Dencik and O. Leistert (Eds.), *Critical Perspectives on Social Media and Protest: Between Control and Emancipation* (pp. 109-126). Lanham: Rowman and Littlefield.

Hintz, A., and Milan, S. (2013). Networked Collective Action and the Institutionalised Policy Debate: Bringing Cyberactivism to the *Policy Arena? Policy & Internet, 5*(1), 7-26.

Hintz, A., and I. Brown (2016) 'Policies for Digital Citizenship? Post-Snowden Changes and Continuities', *International Journal of Communication, forthcoming*.

Hintz, A., Dencik, L. & Wahl-Joergensen, K. (2016). "Surveillance in a Digital Age." In: Franklin, B. & Eldridge II, S. (eds.), *The Routledge Companion to Digital Journalism Studies*, New York and Abingdon: Routledge

Human Rights Council (2015) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

Interviewee 1 (2016) Former Member of Parliament (2010-2015), Liberal Democratic Party. Interview by Arne Hintz, January 2016.

Interviewee 2 (2016) Director of the civil society coalition Don't Spy On Us. Interview by Arne Hintz, January 2016.

Interviewee 3 (2016) Chief Executive of Big Brother Watch. Interview by Ian Brown, September 2015.

Interviewee 4, (2016) Head of Cyber and National Security Programme, TechUK. Interview by Arne Hintz, January 2016.

Keck, M. E., and Sikkink, K. (1998). *Activists beyond Borders. Advocacy Networks in International Politics*. Ithaca: Cornell University Press.

Kingdon, J.W. (1984) *Agendas, Alternatives, and Public Policy*. Boston: Little Brown.

Leistert, O. (2015). The Revolution Will Not Be Liked: On the Systematic Constraints of Corporate Social Media Platforms for Protest. In L. Dencik and O. Leistert (Eds.), *Critical Perspectives on Social Media and Protest: Between Control and Emancipation* (pp. 35-52). Lanham: Rowman and Littlefield.

Lessig, L. (1999). *Code and other Laws of Cyberspace*. New York: Basic Books.

Lyon, D. (2003) *Surveillance after September 11*. Cambridge: Polity

Lyon, D. (2014) "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* (July–December 2014), 1–13.

Marthews, A. and Tucker, C. (2015) 'Government Surveillance and Internet Search Behaviour.' Retrieved from SSRN: http://ssrn.com/abstract=2412564

Mols, A. (forthcoming) '"Not interesting enough to be followed by the NSA" Framing Dutch privacy attitudes in the aftermath of the NSA revelations.' *Digital Journalism*

Moyer, E. (2015, November 8). Twitter teams with women's group on anti-harassment tool. *Cnet*. Retrieved from: http://www.cnet.com/news/twitter-teams-up-with-womens-group-on-anti-harassment-tool

Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge: MIT Press.

Musiani, F. (2015) 'Practice, Plurality, Performativity, and Plumbing: Internet Governance Research Meets Science and Technology Studies'. *Science, Technology & Human Values 40*(2), 272-286.

O'Neill, P. H. (2015) 'The state of encryption tools, 2 years after the Snowden leaks', *The Daily Dot*. 20 June 2015, http://www.dailydot.com/politics/encryption-since-snowden-trending-up/

Open Secrets (2015, October 23). Google Inc. https://www.opensecrets.org/lobby/clientsum.php?id=D000022008

PEN (2013) *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*. New York: PEN American Center. Retrieved from http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf

Penney, J. (2016) 'Chilling Effects: Online Surveillance Wikipedia Use. *Berkeley Technology Law Journal*. Retrieved from SSRN: http://ssrn.com/abstract=2769645

Pohle, J., Hoesl, M., and Kniep, R. (2016) 'Analysing internet policy as a field of struggle.' *Internet Policy Review 5*(3), http://policyreview.info/articles/analysis/analysing-internet-policy-field-struggle

Raboy, M. (2002). Global Media Policy in the New Millennium. Luton: University of Luton Press.

Raboy, M., and Padovani, C. (2010) 'Mapping Global Media Policy: Concepts, Frameworks, Methods', http://www.globalmediapolicy.net/sites/default/files/Raboy&Padovani%202010_long%20version_final.pdf

RUSI (2015) 'A Democratic Licence to Operate: Report of the Independent Surveillance Review, https://rusi.org/publication/whitehall-reports/democratic-licence-operate-report-independent-surveillance-review

Temperton, J. (2015) 'No U-turn: David Cameron still wants to break encryption', *Wired*. 15 July 2015, http://www.dailydot.com/politics/encryption-since-snowden-trending-up/

The Guardian (2015a) "The NSA Files." http://www.theguardian.com/us-news/the-nsa-files.

The Guardian (2015b) 'Facebook and Twitter have social responsibility to help fight terrorism, says Cameron', 16 January 2015. http://www.theguardian.com/world/2015/jan/16/cameron-interrupt-terrorists-cybersecurity-cyberattack-threat

The Guardian (2015c) 'Theresa May to revive her 'snooper's charter' now Lib Dem brakes are off', 9 May 2015, http://www.theguardian.com/politics/2015/may/09/theresa-may-revive-snoopers-charter-lib-dem-brakes-off-privacy-election

The Guardian (2015d) 'UK surveillance bill could bring 'very dire consequences', warns Apple chief', 10 November 2015, http://www.theguardian.com/world/2015/nov/10/surveillance-bill-dire-consequences-apple-tim-cook

Trottier, D., and Lyon, D. (2012) "Key Features of Social Media Surveillance." In C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval, eds., *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, 89–105. Abingdon: Routledge.

Turow, J., Hennesy, M. and Draper, N. (2015) "The Tradeoff Fallacy". Report from the Annenberg School of Communication, University of Pennsylvania. Retrieved from https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Turow, J., McGuigan, L. and Maris, E. R. (2015) "Making data mining a natural part of life: Physical retailing, customer surveillance and the 21st century social imaginary". *European Journal of Cultural Studies, 18*(4-5), 464-478.

UN General Assembly (2013) Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression. Frank La Rue, 17 April 2013. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

Wahl-Jorgensen, K. and L. Bennett (2016) 'Media Coverage and Journalistic Challenges in the Surveillance Society', *International Journal of Communication, forthcoming*.

Wizner, B. (2015). Keynote address to the conference 'Surveillance and Citizenship', Cardiff, 18 June.

Wood, D. M. and Webster, C.W.R. (2009) 'Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example'. *Journal of Contemporary European Research (5)*2: 259-273

Youmans, W. L., and J. C. York (2012). 'Social Media and the Activist Toolkit: User Agreements, Corporate Interests, and the Information Infrastructure of Modern Social Movements', *Journal of Communication*, 62, 315-329.

FOOTNOTES

1. In this article we focus on online or internet surveillance. We define it as the collection and analysis of user data. We include what the UK government calls 'bulk collection' in our understanding of mass surveillance.

2. Detailed results from this research and systematic analyses of the interviews will be published in late 2016 / early 2017 in the International Journal of Communication (IJoC.org).

3. The Onion Browser (TOR) anonymises a user's web browsing by moving website requests and data transfer through a distributed network of relays.

4. Examples are the PGP (Pretty Good Privacy) tool for encrypting email and the software Signal for encrypting text messages and phone conversations.