Surveillance & Society

Article

Resisting Digital Surveillance Reform: The Arguments and Tactics of Communications Service Providers

Wil Chivers

Cardiff University, UK
ChiversWG1@cardiff.ac.uk

Abstract

Communications surveillance in the UK has been an increasingly contentious issue since the early 2000s. The Investigatory Powers Act 2016 is the result of a long series of attempts by the UK government to reform communications surveillance legislation. The consultations on this legislation—and on its precursor, the Draft Communications Data Bill 2012—offer unique insight into how such efforts generate resistance to surveillance. This article draws attention to the role of communications service providers (CSPs)—who are increasingly being responsibilised to collect and retain communications data—within a multi-actor network of resistance. It also identifies the reasons CSPs gave for resisting these proposed reforms. Content analysis of the consultation documents reveals three themes that were central to the CSPs' arguments: technology, territory, and trust. The article concludes by considering the implications for understanding resistance to contemporary digital surveillance.

Introduction

The Investigatory Powers Act, which passed into UK law at the end of 2016, marked the culmination of the UK government's successive attempts to reform surveillance regulation. Far from being a vital update to keep surveillance powers in line with 21st century communications technology, as it was billed, the Act was described as "one of the most extreme surveillance laws ever passed in a democracy" (Open Rights Group 2016). At the heart of these reforms, and their unsuccessful predecessor the Draft Communications Data Bill 2012, has been the "responsibilisation" (Zajko 2016) of communications service providers (CSPs).[1] As part of a broader trend toward enlisting the policing capabilities of non-state actors, CSPs are increasingly pressured to collect and retain data about our online interactions and make them available to law enforcement upon request. This move recognises the significant surveillance capacities of CSPs. Yet, at the same time it has been met with significant resistance from these companies.

Social media companies and internet providers are online surveillance agents par excellence. They enjoy privileged access to our digital transactions and routinely collect and monetise those data. However, particularly in the wake of the Snowden revelations in 2013, CSPs have sought to distance themselves and their surveillance practices from those of governments and their agencies. This paper draws on empirical

[1] I use the term CSP throughout, for simplicity, to capture the activities of both Internet Service Providers (ISPs) and Online Service Providers (OSPs).

Chivers, Wil. 2019. Resisting Digital Surveillance Reform: The Arguments and Tactics of Communications Service Providers. *Surveillance & Society* 17(3/4): 517-532.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

data to elaborate the conflicted position CSPs find themselves in. In particular, it addresses the question of how they resisted the surveillance powers the UK government was trying to enact. Examining consultation documents relating to the Investigatory Powers Bill and the Draft Communications Data Bill reveals three primary, yet occasionally paradoxical, reasons CSPs gave for resisting the proposed regulation: the technology involved, the territorial concerns relating to their respective national jurisdictions, and the trust of their customers.

This article opens by considering the existing research around nodal governance, responsibilisation (Zajko 2016), the mediation of surveillance (Bright and Agustina 2013), and resistance to surveillance. Specifically, it justifies the paper's focus on CSPs as expanding part of a broader multi-actor framework of resistance (Martin et al. 2009). There follows a brief history of surveillance regulation in the UK and an overview of the data sources that are used in the subsequent analysis. In concluding, the paper considers the implications of CSPs' involvement in these debates for understanding resistance to surveillance more broadly.

Nodal Governance, Mediation, and Responsibilisation

This article is concerned with how and why communications service providers have attempted to resist becoming complicit in the apparatus of state surveillance. In exploring how they resisted, the study examines two recent instances of surveillance regulation in the UK, one that failed and one that succeeded, and the accounts CSPs gave as to why such reforms were problematic. Why they resisted is a broader issue these arguments help illuminate later. It is helpful, first, to look at the literature around the processes and implications of what has been described as responsibilisation (Zajko 2016) and mediation (Bright and Agustina 2013), and the ways in which strategies of internet governance have seen surveillance outsourced to private actors.

In its broadest sense, this is a well-established theme in the criminological literature. Shearing and Stenning (1981, 1983, 1985), Cohen (1985), and Garland (2001) all elaborate ways in which social control has steadily become more pervasive throughout society through the recruitment of actors beyond the public authorities. These processes have led to the emergence of nodal forms of governance, wherein top-down control by the state is gradually replaced by more networked, fluid, and diffuse techniques of governance that draw on the capabilities of multiple actors or auspices of security (Johnston and Shearing 2003; Shearing and Wood 2003; Burris et al. 2005).

These practices have become increasingly pertinent as digital communications have evolved and expanded on a global scale. A broader array of actors, specifically CSPs, has been enlisted to assist the state's efforts to protect its citizens by collecting and retaining data the users of digital communications produce and that crosses their networks. While CSPs' motivations for monitoring online behaviour are profit-driven, governments increasingly define them as important providers of security in a blurring of "governing mentalities" (Wood and Shearing 2007: 29). By mandating CSPs to retain more data (through regulation), the state seeks to maintain a degree of hegemony for providing security (Dupont 2003, 2006). Zittrain (2003) describes CSPs as "points of control" on the internet. These providers occupy a strategic position (Zajko 2016) that allows them to monitor and control information flows online. As Ohm (2009: 1438) states, "no other online entity can watch every one of a user's activities, making the ISP's viewpoint uniquely broad" (see also Michaels 2010: 1438). With that in mind, Bernal (2016) is correct to state that there is no distinction in practice between contemporary state surveillance and commercial surveillance and that to consider them separately is to ignore the issues at hand. The former piggybacks on the latter, capitalising on their resources.

These themes have been equally present in surveillance studies where a good deal of attention has been paid to the surveillance functions of an increasingly broader array of public and private actors (e.g., Foucault 1977; Clarke 1988; Haggerty and Ericson 2000; Trottier 2012). Haggerty and Ericson's (2000) "surveillant assemblage"—the ways in which decentralised, shifting, multi-actor networks of surveillance may emerge between institutions in society—is particularly relevant. These rhizomatic networks are constituted of discrete nodes that carry out surveillance for their own ends but whose capabilities may occasionally be

joined or leveraged by others. Less studied are the simultaneous opportunities for multi-actor resistance such networks generate (see Martin et al. 2009, below).

Some research has analysed the specifics of how CSPs are drawn into these networks. Bright and Agustina (2013: 123) described this process as "mediation… when some or all of the 'activity' of surveillance… is conducted by agents outside of the direct control of the surveillance institution." They advance three hypotheses of mediated surveillance:

1. It occurs in situations where institutions have incomplete power or information;
2. Significant coercion is required;
3. It has significant consequences for the effectiveness with which the surveillance is carried out.

The first of these reinforces Bernal's (2016) argument that state surveillance (certainly in this context at least) is commercial surveillance. There is no divide; the state has incomplete power to access the data it requires and so it leverages commercial surveillance practices. Mediation, then, is something of a problem-solving exercise in surveillance.

Similarly, Zajko (2016) elaborates the process and impact of different forms of responsibilisation. "Unfolding responsibilisation" by the state is designed to "orient actors and networks toward goals such as national security, public order, moral governance, and crime control" (2016: 80). This is pursued through legislation but also through persuasion and appeals to civic duty. The former is the subject of this paper and was a strategy the Home Office openly acknowledged during debates around the Draft Communications Data Bill: "[T]he central plank of this programme is a collaborative relationship with service providers in this country and overseas" (Joint Committee on the Draft Communications Data Bill 2012b: 19, hereafter CDB). An example of the latter has been recently seen in the UK with the Home Office's repeated appeals to Silicon Valley companies to do more to aid in preventing the spread of extremism online (Asthana and Levin 2017; Cox 2017). As before, it is not that the state looks to pass the buck but that it instead activates "the governmental powers of private agencies" and sets up "chains of co-operative action" (Garland 1996, in Zajko 2016: 79). The language is very much that of shared effort and partnerships.

Zajko (2016) also illustrates how the state can be responsive to pressures from civil society to regulate in a more favourable way (i.e., with more respect to the right to privacy). This "enfolding responsibilisation" may or may not be successful but it is, he suggests, the most effective way these groups can hope to influence the way in which the targets of unfolding responsibilisation (CSPs) carry out their surveillance functions (i.e., rather than attempting to influence them directly).

Evidently, CSPs occupy a prominent position in contemporary networks of surveillance and nodal governance. As "points of control" (Zittrain 2003) on the internet with their privileged access to our digital communications, they are under enormous pressure from governments to assist with their efforts to tackle crime and terrorism, the traces of which are left across their networks. Governments, meanwhile, occupy the privileged position of being able to regulate CSPs' activities (to a certain extent). Mediated surveillance (Bright and Agustina 2013) and responsibilisation (Zajko 2016) describe the process of law making and so it is during the times when these laws are negotiated that opportunities arise for resistance.

Resistance to Surveillance

Resistance is a crucial issue for surveillance studies. Several notable studies have explored the relationship between surveillance and resistance (Gilliom 2001; Marx 2003; Mann et al. 2003; Bennett 2008), although, in general, the attention it has received has been sporadic (see, for example, Bell 2009; Fernandez and Huey 2009; Introna and Gibbons 2009; Marx 2009; Sanchez 2009; Wells and Wills 2009). Beyond surveillance studies, Sharp et al.'s (2000) "entanglements of power" highlights some of the problems involved in framing resistance as necessarily being a counterpoint to power. Instead, they argue that it is more accurate to think

in terms of "dominating power" and "resisting power," where power is a shifting resource that is shared by many and not wielded by a sole agent. That said, resistance to surveillance remains a highly topical issue. New formations of surveillance constantly emerge, with new avenues in particular for the collection of digital communications data. Snowden's revelations in 2013 put surveillance firmly in the spotlight and have had a lasting influence on how people think about our security services, surveillance, and the personal data technology companies collect and hold. Resistance is a constant companion to surveillance and so it is vital to develop a critical understanding of how, why, where, and by whom surveillance is resisted.

This study builds on Martin et al.'s (2009) insightful description of a "multi-actor framework" for resistance, by examining how and why a number of CSPs resisted the reform of surveillance regulation introduced in the UK. Martin et al. (2009: 228) state that "the interplay of digital technologies and modern governance are bringing everyone under a shared surveillance umbrella, implicating all sorts of important actors whose roles must be understood." Each different issue that arises may bring in a different set of actors with both a stake in doing surveillance but also in resisting it for different reasons. This paper examines the cases of the Draft Communications Data Bill and the Investigatory Powers Bill as prime examples of this kind of multi-actor resistance. The proposed reforms were particularly relevant to CSPs; so, while a range of other actors was also involved, CSPs were particularly central to the whole affair.

Martin et al. conclude that "[r]esearch that addresses the *why* [of resistance] would complement our contribution very well. Exploring the *why* of resistance necessarily involves an emphasis on the context dependencies of the various actors, their roles and relationships, and shared histories" (2009: 229). The analysis in this paper draws out the three key reasons CSPs gave for resisting the proposed reforms, these being technology, territory, and trust. The first relates to the inherent problems in trying to carry out the data collection the state envisages and, thus, relates to some extent to Martin et al.'s (2009) discussion of the resistance capacities of the "surveillance artefact." The second relates to extraterritorial jurisdictions in the context of surveillance (see Warren 2015) and CSPs' unwillingness to contravene these restrictions. The third relates to CSPs' obligations to their users regarding privacy and their desire to maintain trust in an already volatile environment (Naughton 2015; Barnes 2013; Rainie 2016). As the following section outlines, the history of the regulation of surveillance and privacy is one of constant "moves and counter-moves" (Marx 2009) as the regulatory environment at the national and supra-national level fluctuates in response to changing attitudes and concerns.

It is during pivotal moments of resistance, such as in the cases examined here (and indeed in other instances of legislating in contentious areas), that we see the interplay of enfolding/unfolding responsibilisation (Zajko 2016). Many different actors argued for or against the proposed surveillance measures, sometimes in collaboration with others. The Reform Government Surveillance coalition of US-based CSPs is a prime example that "actors may work with states, but they can also coordinate nodes to resist and contest state governance" (Wood and Shearing 2007: 28).

It is timely to include CSPs in our understanding of resistance to surveillance. The case of Apple refusing to open a locked iPhone for an on-going FBI inquiry (see Holpuch 2016) illustrates companies' reticence to acquiesce to requests to hand over proprietary technology or to weaken their control over data that are under their stewardship. The Apple case shows not only the reliance of law enforcement on technology companies but equally the power such companies have to resist or subvert attempts at surveillance (despite, ultimately, the success of the FBI in opening the iPhone without assistance; see Yadron 2016). The message is that surveillance cannot be done without these companies (or if it can be done, not cheaply). This escalation in the "resisting power" of CSPs is a result of their function as vital auspices of control within digital networks; that is, their simultaneous possession of significant "dominating power" (Sharp et al. 2000).

A Brief History of Regulating Surveillance in the UK

Communications data[2] have been described as both invaluable for preventing crime and terrorism and correspondingly inaccessible owing to insufficient powers to obtain and retain such data that proliferates in the private sector. Consequently, regulation of the internet and other electronic means of communications, including the mechanisms by which data are collected and retained, reveals a complex, dynamic, and often conflicting interplay of national and international state and commercial interests and responsibilities. This brief overview reveals where CSPs, specifically in the UK context, have been targets of the state's "unfolding regulation" (Zajko 2016).

Until recently, the Regulation of Investigatory Powers Act 2000 (RIPA) was the foundation for much of the regulation of surveillance in the UK. Wide-ranging, RIPA covered the intercept of communications (e.g., wire-tapping) via a warrant, the collection of communications data, and (covert) human surveillance and intelligence. There was a significant degree of shared ground between RIPA and other Acts of Parliament and the European Directives that were concerned with collecting and retaining personal data: the Anti-Terrorism, Crime and Security Act 2001 allowed a code of practice[3] on the retention of communications data to be issued to CSPs; the Data Protection Act 1998 outlines eight principles data handlers must abide by, including the length of retention; and the EU Data Retention Directive, which came into force in 2006[4] and compelled CSPs to capture various communications data relating to their customers and retain it for between six and twenty-four months. These acts and directives have been subject to increased scrutiny in recent years, as digital communications have evolved and the industry and government have sought to respond to the opportunities and challenges these changes present.

While this restrictive and complex environment has tempered government efforts to enhance surveillance powers, it has not prevented successive attempts to do so. In 2006, the Labour government proposed the Intercept Modernisation Programme (IMP). In 2009, however, this was dropped after an unpublished (and unfavourable) public consultation on the government's plans to retain and store greater amounts of communications data in a centralised government database (see Prince 2008). Despite their opposition at the time to these plans, in 2010 the Coalition government revived the IMP as the Communications Capabilities Development Programme. While departing from the idea of a centralised database, these plans aimed "to preserve the ability of the security, intelligence and law enforcement agencies to obtain communications data" (HM Government 2011: 52). This commitment was translated into the Draft Communications Data Bill 2012. However, following a consultation process that revealed significant resistance to the proposals from a broad spectrum of respondents (including CSPs), the Bill was abandoned. While the case for updating RIPA was acknowledged, the Joint Committee stated, "[T]he draft Bill pays insufficient attention to … the right to privacy, and goes much further than it need or should for the purpose of providing necessary and justifiable official access to communications data" (Joint Committee on the Draft Communications Data Bill 2012a: 3).

The Snowden revelations, the following year, cast what was to become a looming shadow over the security and intelligence services. In a growing climate of increased public awareness of surveillance and mistrust of the government and law enforcement, there followed a frenetic period of legislative change in the UK and the EU. In April 2014, the earlier EU Data Retention Directive was declared invalid:

> [B]y requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data. (Court of Justice of the European Union 2014)

[2] This is typically described as the *who*, *when*, and *where* of electronic communications, i.e., not the content of messages.

[3] The Retention of Communications Data (Code of Practice) Order 2003.

[4] Implemented into UK law by the Statutory Instrument (Data Retention (EC Directive) Regulations 2009).

To counteract this, the UK government enacted emergency legislation in the form of the Data Retention and Investigatory Powers Act (DRIPA), despite vocal concern about the democratic process (see Powles 2014) and the dangers of rushing through legislation on such a topical and contemporary issue (Hansard 2014). Continued disquiet about the spectacular haste with which DRIPA was enacted and the publication of three separate reports on the state of surveillance and privacy in the UK (Anderson 2015; ISC 2015; RUSI 2015) mounted pressure on the government. An ensuing legal challenge from MPs Tom Watson and David Davis led the High Court to find the legislation unlawful in July 2015 (Bowcott 2015). The government was given until the end of March 2016 to draft new legislation; in November 2015, it introduced the Investigatory Powers Bill. The subsequent public consultation on the Bill garnered even more responses than the CDB in 2012, not to mention as much criticism. Regardless, the Investigatory Powers Act was passed in April 2016 with amendments that did little to assuage the concerns of privacy advocates and civil liberties campaigners (see Open Rights Group 2018). Key provisions of the Act, and the responsibilities placed on CSPs (such as those below relating to technology and territory) include:

- Internet Connection Records—CSPs must retain and make available to law enforcement and security services for 12 months records of the websites visited by their customers;
- Encryption—CSPs can be forced to remove encryption from messages but only if it is "technically feasible" (see Hern 2017);
- Bulk Interception/Acquisition—introduction of warrants for obtaining bulk datasets, which may include data relating to overseas individuals.

Sources of Data

Previous research (for example, Akdeniz et al. 2001) examined the implications of surveillance-focused regulation but it has not systematically analysed the process of the creation of regulations in the same way the processes involved in the Draft Communications Data Bill (CDB) and the Draft Investigatory Powers Bill (IPB) have allowed—nor have the circumstances arisen to do so. The opportunity to examine the role of CSPs in resisting surveillance reform came in the form of the consultations that took place on the CDB and the IPB. The value of these documents as sources of data should not be overlooked. Very rarely can researchers gain such detailed insight into the reasons why such a broad spectrum of actors, from interested individuals with no technical expertise to multinational companies, considers proposals for enhanced surveillance practices to be problematic (or necessary, as the case may be).

The public consultation on the CDB was issued in July 2012. Written evidence submissions were received from 145 respondents and oral evidence sessions were held with testimonies received from 54 witnesses. While some of the oral evidence was redacted or not made public, most of the written and oral responses are available on the UK parliamentary website.[5] The IPB consultation was issued in November 2015. Written submissions were received from 148 respondents and oral evidence sessions were held with 59 witnesses. The quantity of the written evidence submitted was far greater for the IPB, totalling over 1,500 pages compared to 600 pages for the CDB.

Documents were downloaded in full and respondents were sorted into seven categories, including the Telecoms Industry. The responses of the CSPs involved in these consultations were drawn from this category. Seventeen different CSPs from the UK and the US were identified across both consultations, including: Apple, British Telecom (BT), EE, Facebook, Google, GreenNet, Microsoft, Mozilla, Sky, TalkTalk, Telefonica, Three, Twitter, Virgin Media, Vodafone, and Yahoo. In total, the CSPs submitted 49 pages of written evidence to the CDB consultations and 122 pages to the IPB consultations. These submissions were coded thematically in their entirety.

[5] Draft Communications Data Bill available at: http://www.parliament.uk/draft-communications-bill/ and Investigatory Powers Bill available at: https://www.parliament.uk/draft-investigatory-powers.

Reasons for Resistance

Given the volume of the data involved, what is presented here is selective, although an effort has been made to represent a range of different voices. The findings are grouped into three themes that re-appeared most strongly throughout the responses given by the CSPs in 2012 and 2015; these are technology, territory, and trust. When taken together, these give a good sense of how, on two separate occasions, CSPs resisted the proposed reforms. The broader question of why they resisted is returned to later.

Technology

Given the nature of the reforms—of the collection and retention of online data –numerous technological aspects of the bills were debated throughout the course of both consultations. A whole report could (and indeed has) been dedicated to drawing some of these out; those presented here are some of the most prominent points that were made.

A central aspect of both consultations was a dichotomy between communications data and the content of communications. The Joint Committees repeatedly requested respondents' opinions regarding the distinction between the two. The rationale for this is clear: the ability of government or law enforcement to read the contents of private citizens' communications would be incredibly intrusive. However, as Justice (2011: 71) notes, this intention or capability was a misconception; there was a lack of public understanding of what constitutes communications data, fuelled by speculative media reports (see Kirkup 2008).

While government representatives defended their claim that accessing content data was not their intention, several respondents challenged the technical feasibility of separating the communications data from the content in electronic communications. According to the director of the Communications Capability Directorate of the Home Office, responsibilisation would solve the problem: "We will be working with them [CSPs] to retain, in some cases, aspects of communications data and, in that case, it is very easy to separate content from CD" (Richard Alcock [Home Office], CDB Oral Evidence 2012b: 17).

In practice, it appeared to be far from straightforward.

> **Lord Armstrong of Ilminster:** Are you confident that you can always distinguish between communications data and content in these activities?
>
> **Bob Hughes (Telefonica O2):** It all comes down to the definition and the guidance we get about where that line exists. Currently … there is debate and disagreement as to where the line between content and the comms data sits, and has been for the last few years. We could not sit here and say that we are confident that it is clearly defined within the Bill or any other piece of paper at the moment. It is something that we could struggle with…
>
> **LA:** It is very important philosophically, you might say, that content is out in the Bill. But it is not as easy as that, really, is it?
>
> **BH:** No.
>
> (CDB Oral Evidence 2012b:187, qq. 499-500)

It illuminates the difficulty of this issue that it persisted in 2015 even after the extensive examination of the CDB five years earlier. However, progress had been made; it appeared that separating content from communications data was not technically impossible but it rested, again, on the definition of data.

> **Hugh Woolford (Virgin)**: On how easy it is to separate communications data from content … we feel that we need more work to get more clarity over what is considered content versus communications data … We need to move forward and get some more detail in place around some of those nuances and how to handle some of them.

> **Mark Hughes (BT)**: Technically, it is feasible to separate various parts of the packets; we can deploy tools to do that. The point about that is that, increasingly, especially in the future, with more and more encryption, the ability becomes more limited to take you back to purely an entity level piece of communications data as opposed to richer parts of communication data.
>
> (Joint Committee on the Draft IPB Oral Evidence 2016a q. 102; hereafter, IPB Oral Evidence)

As this conversation indicates, encryption was an inseparable issue, particularly where UK CSPs may have been requested to retain third-party data (e.g., data from Facebook or Google) that transited their networks:

> Once we can identify the packets of data, we would need to find a way technically to say, "Okay, we understand that we now need to retain these," but they are encrypted, or not, on an application-by-application basis. If they are fully encrypted, we need to be able technically to unpick it and say, "Here is the traffic data but obviously we have not touched the content," which is very difficult.
>
> (Mark Hughes [Vodafone], CDB Oral Evidence 2012b: 179)

There are two problems here. First, the presence and form of encryption varies and, thus, there is no single way to separate content from communications. Second, content and communications may not be separately identifiable prior to "unpicking" the encryption, so that, once decrypted, CSPs would unintentionally be in possession of both, regardless of their aim to only access communications data. A third problem arose when the CSPs were asked about the technical feasibility of decrypting third-party messages:

> Only with the keys. That is what they are designed for. We would not have the keys. And of course it is proprietary encryption, so it is not necessarily just the keys. It could be that you have got to have the language with which to decrypt it.
>
> (Bob Hughes [Telefonica O2], CDB Oral Evidence 2012b: 172)

Finally, aside from the matter of collecting the data, there was the question of retaining it, which brought its own issues. This time, the problem was not the technical feasibility but the cost:

> **Lord Strasburger:** Would retention of more data for a lot longer cause you any technical difficulties?
>
> **Mark Hughes (Vodafone):** I do not think it is technical difficulties, necessarily. I think that it is just cost. More data equals much more expense, to build it and to run it every year.
>
> **Jonathan Grayling (EE):** On top of that, there is the querying aspect. The more data that you store, the more data there is to query. Again, that would be additional cost because you have to develop the querying techniques on top of that.
>
> **Bob Hughes (Telefonica O2):** There is nothing in the Bill as it stands that is not technically feasible. It is just throwing enough money at it.
>
> (CDB Oral Evidence 2012b: 185, q. 492)

In short, this theme addresses the issue of CSPs' technological capacities. It was not impossible to do something akin to what they were being asked, but it rested on unsolved problems of defining the data in question, how to ensure content would not be captured or viewed, how to overcome technological barriers such as encryption, and the associated high costs of developing existing technological infrastructure.

Territory

Entering the debate in regard to this theme were representatives from US-based CSPs, including Facebook, Google, Microsoft, Twitter, and Yahoo! The majority of their input came in 2012, when they attended an oral evidence session. However, they refused to attend the 2015 session—arguably a separate act of resistance—although a coalition of these groups made a written submission. It is from these international actors that data is mostly drawn here. This is because the issue of territory concerned proposals that the existing extraterritorial mechanisms for requesting third-party data, known as Mutual Legal Assistance Treaties (MLATs), may have been circumvented by tasking UK-based CSPs with retaining the data and making it accessible to law enforcement. In many ways, this is a similar concern to the Microsoft Ireland case,[6] where the United States government requested the contents of emails held overseas via warrant under the Stored Communications Act 1986, legislation Microsoft argued was unfit for the purpose (see Franklin 2018 and Matsakis 2018). It is likely that this case informed the CSPs' position in 2015.

The issue of territory surfaced differently during each consultation. It received much more attention during the debates around the CDB, owing to the fact that the wording of the Bill had changed in 2015—presumably as a result of previous resistance to the proposed arrangements. In 2012, representatives from Google, Hotmail/Microsoft and Yahoo! presented a straightforward argument: There are existing routes to follow to obtain data the UK is not permitted to access (MLATs); and while there may be room for improvement, these routes provide some clarity and legal protection in an already complex regulatory arena. Statements from representatives of Yahoo! and Twitter clearly show their concerns on this matter:

> The UK would be the first country to extend its jurisdiction and take a reserve power to require UK providers to retain data that they could not obtain directly. We believe that other countries would follow, including countries that would use legislation of this kind to limit free expression and infringe privacy rights of internet users. From our perspective, that would create a bewildering patchwork of overlapping and potentially conflicting legislation.
>
> (Emma Ascroft [Yahoo!], CDB Oral Evidence 2012b: 214)

> [O]ne of our concerns would be about a UK-based carrier ordered to collect Twitter data here…That would therefore pose problems to us in terms of our terms of service and privacy policies…We would also have issues with respect to not knowing when an access request for such user information was served on the company that was UK based and collecting our data.
>
> (Colin Crowell [Twitter], CDB Oral Evidence 2012b: 231)

Echoing the technical issues, there was also the problem of encrypted third-party data. For CSPs the encryption of data is typically proprietary; consequently, when retaining their own data, decryption would be straightforward for UK CSPs but this would not be the case for third-party data. Asserting their position on this issue, overseas CSPs stated that they were usually willing to decrypt these data but only when issued with a valid RIPA/MLAT request:

> **Sarah Hunter (Google)**: If a valid RIPA request comes in or UK law enforcement goes through the MLAT, receives a court order and in turn gets Gmail user data, we will obviously provide that data decrypted. If it was to use a third-party provider to gather the encrypted data, I think it very unlikely that Google Inc. would provide anyone outside Google Inc. with that key. That is simply because, as everyone said earlier, security is our most important asset. Our relationship with our users is predicated on trust. Without that, we have no business.

[6] Microsoft Corp. v. United States. In 2013, Microsoft challenged a government warrant requesting emails that were stored on servers based in the Republic of Ireland (the stated country of residence of the customer in question), on the basis that the Stored Communications Act (SCA) 1986 was unfit to be applied to Internet communications and data storage. Initially, the case ruled in favour of the government, stating the SCA was not restricted by territorial concerns, and then later in favour of Microsoft, during appeal. The case was mooted in 2018, following the passage of the Clarifying Lawful Overseas Use of Data (CLOUD) Act by Congress (see EPIC 2018).

> **Emma Ascroft (Yahoo!)**: The encryption question is rather a red herring because the UK law enforcement agency can obtain the data direct from us using international legal channels such as the MLAT. If it came to us through those channels, we would disclose those data in the clear. If those channels work properly, this backstop power is unnecessary.
>
> (CDB Oral Evidence 2012b: 226)

Their stance reinforces the position that the existing methods for requesting data were sufficient. Encryption appeared as a bargaining chip of sorts, with the justification that this was in the best interests of service users. By attempting to circumvent the lengthy RIPA/MLAT process, UK law enforcement (via UK CSPs) would need to decrypt the data themselves, which would be both time consuming and costly.

In the Investigatory Powers Bill this issue had shifted but by no means disappeared. As expected, the government was still interested in accessing data relating to users of Facebook, Gmail and other US- or UK-based "over-the-top"[7] services. However, the language was couched in different terms. The then Home Secretary, Theresa May, stated, "We have made it very clear that we will not require CSPs to retain third-party data" (Joint Committee on the Draft Investigatory Powers Bill. Oral Evidence 2016a: 433); and indeed, CSPs were not required to retain these data in the same way the CDB had proposed. Nevertheless, the extraterritorial powers the Investigatory Powers Act ultimately outlined were broad in scope.

Virgin Media identified their concern over "the inclusion of sweeping extraterritorial powers" that gave "a misleading impression that overseas companies will be subject to the same obligations as UK companies" (Joint Committee on the Draft Investigatory Powers Bill. Written Evidence 2016b: 1326 [hereafter, IPB Written Evidence]). They suggested that the government should instead favour the use of MLATs and that the use of the Bill's powers should be restricted to matters concerning services provided to British customers. This was a view a coalition of US-based CSPs (Facebook, Google, Microsoft, Twitter, and Yahoo!) shared. In a joint submission that highlighted the potential for conflicts of law, they stated that this would

> create an increasingly chaotic legal environment for providers, restricting the free flow of information and leaving private companies to decide whose laws to violate. These decisions should be made by Governments, grounded in fundamental rights of privacy, freedom of expression, and other human rights. If the UK legislation retains authority to reach extraterritorially, the Bill should consistently and explicitly state that no company is required to comply with any notice/warrant, which in doing so would contravene its legal obligations in other jurisdictions.
>
> (Reform Government Surveillance, IPB Written Evidence 2016b: 388)

They went on to take issue with a perceived degree of inequality between the extraterritorial powers the UK authorities would be granted and those they were willing to allow others to exercise regarding accessing data in the UK. They advocated developing an international framework to "resolve conflicts across jurisdictions" and "facilitate more efficient requests in cases that provide adequate protections for user privacy" (IPB Written Evidence 2016b: 388). This time, they resorted to the language of privacy rights, indicating, perhaps, a desire (or at least acknowledging) that service users are central to the issue. Their refusal to attend oral evidence sessions could also be read as wanting to avoid any damaging association with the whole unresolved process. In the post-Snowden era, this is to be expected. Governments will be similarly aware of their own precarious positions. However, it remains doubtful to what extent they will pursue legislation in a transparent fashion.[8]

---

[7] Such as social media or messaging services, like WhatsApp, that are carried by other fixed or mobile telephone operators.

[8] The Sheinwald Report in 2015, for instance, was commissioned to examine data sharing between the UK and US with a view to expediting existing mechanisms, although in a highly criticised move this was not made public (Travis 2015).

Trust

The final theme concerns CSPs' worries that reforms would undermine users' trust. Despite occurring "pre-Snowden," the CDB consultation frequently referred to this question. The subject was one closely connected to the issue of territory:

> We are a company that is built on consumers' trust and confidence, and in order to honour that commitment we aim to be consistent in how we engage law enforcement around the world.
>
> (Emma Ascroft [Yahoo!], CDB Oral Evidence 2012b: 223)

This outlook, shared by representatives from Microsoft and Google, positions overseas CSPs as accountable, first and foremost, to their consumers. Nevertheless, although increased faith in data protection is favourable for service users, it is not cynical to suggest that the CSP's motivation is to retain a valuable customer base:

> **Lord Jones:** I heard, and liked, your reference to the user's right to privacy … how often do you dig in over looking after the rights of the user?
>
> **Stephen Collins:** From a Microsoft perspective—I am sure it is very similar for my colleagues—we would not have a successful business without the trust and confidence of our users. That is a kind of base assumption for building a successful business, particularly where there is an awful lot of competition … so we have a robust privacy policy which we follow and implement rigorously.
>
> (CDB Oral Evidence 2012b: 222)

As expected, this position had not changed in 2015, and there were signs that CSPs were aware of the increased likelihood or risk of their systems being targeted beyond requests for communications data:

> Customer trust is essential to our business, and the priority for us is to ensure that we provide a secure and resilient network. That is what our customers will expect. If there are any powers or any activity that is undertaken by the agencies in relation to equipment interference, whether that is proportionate and lawful is a matter for Parliament and the agency itself, but EE would not accept it if those activities had any impact on the security of our customers' data or the resiliency of our networks.
>
> (Jonathan Grayling [EE], IPB Oral Evidence 2016a: Q159)

Nor was it—or is it—simply the case that these statements are unsupported by action of any kind. Both in 2012 and in 2015, CSPs cited evidence of their active promotion of these principles:

> We are all committed to protecting our users' rights and privacy. Together, Google, Microsoft and Yahoo! are founder members of the Global Network Initiative, a global organisation that brings together internet companies, civil society groups, academics and investors specifically to develop a collaborative approach to protect and advance free expression. This organisation has developed principles and implementation guidelines that guide responsible company action in engaging law enforcement in response to valid requests for data disclosure.
>
> (Emma Ascroft [Yahoo!] CDB Oral Evidence 2012b: 224)

In 2015, these companies and others formed the US-based Reform Government Surveillance coalition of CSPs. In their joint written submission, they state that "the ultimate test we apply to each of the authorities in this Bill is whether they will promote and maintain the *trust* users place in our technology" (IPB Written Evidence 2016b: 391, emphasis added). The example of computer network exploitation, whether conducted in the UK or the US, was again held up as setting a dangerous precedent for undermining this trust.

These inter-related themes illustrate the tactics and arguments the CSPs used during both consultations. Other issues arose, but those of technology, territory and trust indicate the key and unifying concerns that ran through both consultations. They also draw our attention to the matters CSPs, as nodes in the multi-actor framework of resistance, are specifically capable of bringing to the table.

Understanding Resistance to Surveillance

The cases of the CDB and the IPB illustrate the ways in which the state seeks to govern the risks posed by constantly evolving communication technologies through the mediation or responsibilisation of CSPs. The reason these strategies have continued to appeal to successive governments, as Bright and Agustina's (2013) first hypothesis states, is because the state has incomplete power or information and this is something CSPs can supply. However, to add to Zajko's (2016) argument, the semantics of responsibilisation are also important. It is not just the case that CSPs are responsible for data collection and retention; they are also responsible if something goes wrong. As a governance strategy, it is a useful way to try to avoid users' anger and backlash. Similarly, it would be partly the CSPs' responsibility if a terrorist incident were to occur that inaccessible communications data could have helped prevent (Hosenball 2017).

Yet because of their central role, and despite the fact that they are surveillance agents in their own right, these companies are uniquely positioned to resist. In this context, examining the role of CSPs to understand resistance to surveillance means understanding: 1) that they can resist because they have ownership of the technology; 2) they are beholden to multiple and often conflicting laws; and 3) that they are self-motivated to protect their users as a way to protect their businesses. Nevertheless, the reasons they can resist and have done so does not necessarily tell us why they resist. A more nuanced understanding is required.

Of the themes above, trust is perhaps the most noteworthy. It illustrates most clearly how CSPs deploy altruistic arguments to maintain their privileged and profitable positions. Without trust, CSPs will lose their customer base. For companies that are built on extracting value from data, user buy-in is crucial. Post-Snowden, CSPs have done much to reassure users around the world that they are not complicit in government mass-surveillance programmes (Greenwald et al. 2013). Aligning themselves with users' values arguably helped reinforce the distinction between their "good" commercial surveillance practices and the state's "bad" ones. Of course, no such distinction exists in practice (Bernal 2016).

Continuing in this vein, paradoxes are visible in CSPs' behaviour. For instance, on the issue of technology CSPs are natural proponents of the "technological solutionism" discussed by Morozov (2013). Yet, in these cases, they said technology was not the answer. Protecting content data, managing encryption, and storing more data were all cited as barriers to implementation. When this argument appeared to be insufficient in 2015, CSPs cited economic disincentives instead; it would cost them and, therefore, the government more to do it. Territory presents similar paradoxes. The laws and regulations of their home jurisdiction can protect CSPs against access requests from another, yet they simultaneously resist their own government introducing enhanced controls. The location of their services overseas further permits them to resist access requests from their own government. CSPs operate globally and so, again, it is in their interest to be as free from national control as possible.

Acknowledging these paradoxes is useful for understanding resistance. They highlight inconsistencies, which in turn reveal where arguments may disguise altruism for self-interest. To reiterate; CSPs are businesses and so prioritise profit-making. This is not at all to say they do not also value privacy. But we should remain alert to the fact that how they go about protecting privacy—or at least being seen to advocate privacy—will be influenced by their corporate motives. We can apply the same logic to governments and the familiar (yet false) dichotomy of security and privacy. Governments need to be seen to be protective of both, yet by enacting ill-thought-out legislation, such as the Investigatory Powers Act, they are arguably doing neither.

Thinking about technology as a form of capital further illuminates this conundrum. As we have seen, it may be technically feasible to do as the government requests aside from being concerned with matters of cost or time. Yet CSPs are reliant on their technological capital and are unlikely to want to lose control of this. Consequently, it will be interesting to see how CSPs respond as debates around MLATs, the IPA, the CLOUD Act, and other inter-state regulations continue; what they consider feasible may shift over time.

Contemporary formations of control and governance are constantly in flux. As Fuchs (2008) and Wood and Shearing (2007) observe, they are characterised by competition (i.e., resistance) as much as by co-operation. Undoubtedly, everyone with a stake in this legislation wishes to protect society from harm. However, there is significant disagreement about how best to do that or, indeed, what the harm to be protected against is. Agamben's (2005) notion of a "state of exception" describes how normalising emergency legislation, such as DRIPA, creates the paradox that measures to protect civil liberties (safety, freedom, security) simultaneously erode them (undermining online privacy). Working toward a shared goal does not mean achieving consensus on how to achieve it, particularly where the government, private sector, and civil society collide. Akin to Zajko's (2016) description of the enfolding and unfolding of priorities and goals, resistance in this context is a process of competing for the right to define how social order should be protected.

CSPs are not the only entities that resisted the CDB and IPB. Other sets of actors played important roles. The media were concerned about protections of journalistic sources, while privacy advocate groups championed the protection of civil liberties online. The multi-actor framework (Martin et al. 2009), therefore, draws attention to how resistance may be a co-operative endeavour. For instance, privacy advocacy organisations consulted with academic and legal experts, as well as CSPs, to construct robust and thorough written submissions to the consultations. And within the CSP community, formal coalitions such as Reform Government Surveillance emerged. Both illustrate how assemblages can be "resistant" as well as "surveillant," while the potential to resist is amplified at those points of control (Zittrain 2003).

The centrality of CSPs within networks of internet governance will not diminish. Their business models set the tone for how online data are generated, collected, and analysed. Moreover, as Zajko (2016) notes, the scope of online activity that each of these global companies covers continues to expand. Consequently, the breadth of the responsibilities that have been placed upon them has also expanded. The example of the resistance this paper has addressed—to surveillance—is one among many issues CSPs have been involved with. Both Zajko's (2016) and Bright and Agustina's (2013) work, for instance, focused on copyright and the pressures CSPs face in tackling infringements on their networks. Their role will continue to be a precarious one and the outcome for digital forms of surveillance will depend on the persuasiveness and persistence of their resistance.

Conclusion

This paper has attempted to enhance our understanding of resistance to digital forms of surveillance by examining the responsibilisation of CSPs. Empirical data shows how this set of actors, among a broader multi-actor framework (Martin et al. 2009) of interested individuals and groups, resisted surveillance—or being implicated in the process of doing surveillance. In that regard, the paper also illuminates how agents of surveillance can also resist when it is in their interest to do so.

It is an inescapable fact of contemporary digital surveillance that governments will continue seeking to draw on the capabilities of technology companies to obtain data that may assist them in preventing crime and terrorism. CSPs are gatekeepers of vast amounts of data, and as those data come to reveal more about people, governments will have a greater interest in accessing them. It is because CSPs have developed enormously profitable forms of surveillance that they are central to networks of governance. However, they are also able to offer significant resistance to such attempts, despite the fact this seems to be a losing battle. This duality is matched by paradoxes in the way CSPs argue against surveillance while, at the same time, building their reputations on the public good their services provide. Ultimately, both CSPs and governments appear Janus-

faced as they try to first establish and then position themselves favourably in respect to the divide between "good" and "bad" technology and surveillance practices.

While the mediation of surveillance is not a new phenomenon, the characteristics of surveillance in the information society complicate the process. Specifically, regulation in this area must fit within a global surveillant assemblage (Haggerty and Ericson 2000) and not only within the boundaries of the nation state in which it is enacted. As a consequence, resistance to these newly regulated forms of surveillance is amplified as this opens it up to a much broader set of actors who simultaneously work to codify or enfold (Zajko 2016) their interests within the law. As these issues continue to play out globally, they will bring in a wider range of actors with more motivations, which may either assist or (more likely) complicate matters for governments in this area. In the UK and European context, for example, we should pay attention to the possible impacts of Brexit on data protection and privacy legislation. As we have seen, European law has restricted the UK government in the past; but once the UK has left the EU, such limitations may be more easily overcome.

The obvious difference between the CDB and the IPB are that the latter ultimately became law in 2016, and so resistance on that occasion failed. But this does not discount the efforts of everyone who challenged the proposals, whether they were Google and Facebook or interested individuals with no technical expertise. Nor does it mean the regulation is now a closed book. It is highly likely that the Act will encounter difficulties as its various constituent parts come to be implemented. At the time of writing, analysis is forthcoming from consultations on five Codes of Practice that will be issued under the Act. These will provide detailed insight into the specifics of responsibilisation/mediation in practice and may also give rise to other opportunities for CSPs to resist. What may be more opaque—unless another prominent case makes the news—is the nature of interactions between the UK government and the CSPs based both in the UK and overseas. The CLOUD Act may have ramifications in this respect, while the government's refusal to publish the Sheinwald Report into data sharing between the UK and the US, for instance, signifies a lack of transparency in how CSPs may be obliged to share user data.

Further studies on the relationship between CSPs and the state and how this shapes surveillance would contribute much to this area. Methodologically, we should be aware of opportunities to gain insight into the processes by which surveillance in our society is implemented. The CDB and IPB precisely illustrate the multi-actor framework Martin et al. (2009) proposed. For that reason, a comprehensive understanding of resistance could also be gained by examining the roles of other actors during these events and as they continue to unfold.

Acknowledgments

The author would like to thank Professors Martin Innes, Matthew Williams, and Ian Rees Jones for their comments and suggestions on early drafts of this paper, along with participants at the 2016 Surveillance Studies Network conference, where the ideas in this paper were first discussed. This writing of this paper was funded by the Economic and Social Research Council (ESRC) grant ES/L009099/1, WISERD Civil Society.

References

Agamben, Giorgio. 2005. *State of Exception*. Translated by K. Attell. Chicago, IL: Chicago University Press.

Akdeniz, Yaman, Nick Taylor, and Clive Walker. 2001. BigBrother.gov.uk: State Surveillance in the Age of Information and Rights. *Criminal Law Review* February, 73-90.

Anderson, David. 2015. *A Question of Trust: Report of the Investigatory Powers Review*. London: HMSO.

Asthana, Anushka, and Sam Levin. 2017. UK urges tech giants to do more to prevent spread of extremism, *The Guardian*, Tuesday, August 1.https://www.theguardian.com/technology/2017/aug/01/uk-urges-tech-giants-to-do-more-to-prevent-spread-of-extremism. [Accessed Aug 2017]

Barnes, Anthony. 2013. Edward Snowden warns over global threat to privacy during Channel 4's Alternative Christmas Message. *The Independent*, Tuesday, December 24. http://www.independent.co.uk/news/people/news/edward-snowden-warns-over-global-threat-to-privacy-during-channel-4-s-alternative-christmas-message-9024541.html. [Accessed Jul 2017]

Bell, David. 2009. Surveillance is Sexy. *Surveillance & Society* 6 (3): 203-212.

Bennett, Colin. 2008. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press.

Bernal, Paul. 2016. Data Gathering, Surveillance and Human Rights: Recasting the Debate. *Journal of Cyber Policy* 1 (2): 243-264.
Bowcott, Owen. 2015. High Court rules data retention and surveillance legislation unlawful. *The Guardian*, Friday, July 17.https://www.theguardian.com/world/2015/jul/17/data-retention-and-surveillance-legislation-ruled-unlawful. [Accessed Jul 2017]
Bright, Jon, and José R. Agustina. 2013. Mediating Surveillance: The Developing Landscape of European Online Copyright Infringement. *Journal of Contemporary European Research* 9 (1): 120-137.
Burris, Scott, Peter Drahos, and Clifford Shearing. 2005. Nodal Governance. *Australian Journal of Legal Philosophy* 30: 30-58.
Clarke, Roger. 1988. Information Technology and Dataveillance. *Communications of the ACM* 31(5): 498-512.
Cohen, Stanley. 1985. *Visions of Social Control*. Cambridge, UK: Polity Press.
Court of Justice of the European Union. 2014. C-293/12 and C-594/12. *Digital Rights Ireland and Seitlinger and Others*. Press Release No. 54/14. Luxembourg.
Cox, Josie. 2017. Amber Rudd to 'urge tech companies in Silicon Valley' to do more to crack down on terrorism. *The Independent*, Monday, July 31. http://www.independent.co.uk/news/business/news/amber-rudd-silicon-valley-terrorism-attack-crackdown-tech-companies-home-secretary-you-tube-facebook-a7868691.html. [Accessed Sep 2017]
Dupont, Benoit. 2003. Public Entrepreneurs in the Field of Security: An Oral History of Australian Police Commissioners. Paper presented at *In Search of Security: An International Conference on Policing and Security*. Montreal, QC: Law Commission of Canada.
Dupont, Benoit. 2006. Power Struggles in the Field of Security: Implications for Democratic Transformation. In *Democracy, Society and the Governance of Security*, edited by Jennifer Wood and Benoit Dupont, 86-110. Cambridge, UK: Cambridge University Press.
EPIC. 2018. *The CLOUD Act*. https://epic.org/privacy/cloud-act/. [Accessed Mar 2018]
Fernandez, Luis A., and Laura Huey. 2009. Is Resistance Futile? Thoughts on Resisting Surveillance. *Surveillance & Society* 6 (3): 199-202.
Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. New York, NY: Vintage Press.
Franklin, Sharon Bradford. 2018. The Microsoft-Ireland Case: A Supreme Court Preface to the Congressional Debate. *Lawfare*. Thursday, February 22. https://www.lawfareblog.com/microsoft-ireland-case-supreme-court-preface-congressional-debate. [Accessed Mar 2018]
Fuchs, Christian. 2008. *Internet and Society: Social Theory in the Information Age*. New York, NY: Routledge.
Garland, David. 1996. The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society. *British Journal of Criminology* 36 (4): 445-471.
Garland, David. 2001. *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford: Oxford University Press.
Gilliom, John. 2001. *Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy*. Chicago, IL: University of Chicago Press.
Greenwald, Glenn, Ewen MacAskill, Laura Poitras, Spencer Ackerman, and Dominic Rushe. 2013. Microsoft handed the NSA access to encrypted messages. *The Guardian*. Friday, July 12. https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data. [Accessed Jul 2013]
Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *The British Journal of Sociology* 51 (4): 605-622.
Hansard. 2014. House of Lords Debate 2014-15, vol. 755, col. 641.
Hern, Alex. 2017. UK government can force encryption removal, but fears losing, experts say. *The Guardian*, Wednesday, March 29. https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act. [Accessed Apr 2017]
HM Government. 2011. *CONTEST: The United Kingdom's Strategy for Countering Terrorism*. London: The Stationery Office.
Holpuch, Amanda. 2016. Tim Cooks says Apple's refusal to unlock iPhone for FBI is a 'civil liberties' issue. *The Guardian*, Monday, February 22. https://www.theguardian.com/technology/2016/feb/22/tim-cook-apple-refusal-unlock-iphone-fbi-civil-liberties. [Accessed Feb 2018]
Hosenball, Mark. 2017. Rudd asks Silicon Valley to do more to counter militants, *Reuters*, Monday, July 31.https://uk.reuters.com/article/uk-britain-security/rudd-asks-silicon-valley-to-do-more-to-counter-militants-idUKKBN1AG162. [Accessed Aug 2017]
Intelligence and Security Committee. 2015. *Privacy and Security: A Modern Transparent Legal Framework*. London: HMSO.
Introna, Lucas, and Amy Gibbons. 2009. Networks and Resistance: Investigating Online Advocacy Networks as a Modality for Resisting State Surveillance. *Surveillance & Society* 6 (3): 233-258.
Johnston, Les, and Clifford Shearing. 2003. *Governing Security: Explorations in Policing and Justice*. London: Routledge.
Joint Committee on the Draft Communications Data Bill. 2012a. *Draft Communications Data Bill: Report, together with appendices and formal minutes*. London: The Stationery Office.
Joint Committee on the Draft Communications Data Bill 2012b. *Draft Communications Data Bill: Session 2012-13, Oral Evidence*. London: The Stationery Office.
Joint Committee on the Draft Communications Data Bill. 2012c. *Draft Communications Data Bill: Session 2012-13, Written Evidence*. London: The Stationery Office.
Joint Committee on the Draft Investigatory Powers Bill. 2016a. *Draft Investigatory Powers Bill: Oral Evidence*. London: The Stationery Office.
Joint Committee on the Draft Investigatory Powers Bill 2016b. *Draft Investigatory Powers Bill: Written Evidence*. London: The Stationery Office.
Justice. 2011. *Freedom from Suspicion: Surveillance Reform for a Digital Age*. http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf. [Accessed Aug 2013]

Kirkup, James. 2008. Phones tapped at the rate of 1,000 a day. *The Telegraph*, Tuesday, January 29. http://www.telegraph.co.uk/news/uknews/1576937/Phones-tapped-at-the-rate-of-1000-a-day.html. [Accessed Jul 2013]
Mann, Steve, Jason Nolan, and Barry Wellman. 2003. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society* 1 (3): 331-355.
Martin, Aaron K., Rosamunde E. van Brakel, and Daniel J. Bernhard. 2009. Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework. *Surveillance & Society* 6 (3): 213-232.
Marx, Gary T. 2003. A Tack in the Shoe: Neutralising and Resisting the New Surveillance. *Journal of Social Issues* 59 (2): 369-390.
Marx, Gary T. 2009. A Tack in the Shoe and Taking off the Shoe: Neutralisation and Counter-Neutralisation Dynamics. *Surveillance & Society* 6 (3): 294-306.
Matsakis, Louise. 2018. Microsoft's Supreme Court Case Has Big Implications for Data. *Wired*, Tuesday, February 27.https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/. [Accessed Mar 2018]
Michaels, Jon D. 2010. Deputizing Homeland Security. *Texas Law Review* 88: 1435-1473.
Morozov, Evgeny. 2013. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York, NY: Public Affairs.
Naughton, John. 2015. Don't trust your phone, don't trust your laptop—this is the reality that Snowden has shown us. *The Guardian*, Sunday, March 8. https://www.theguardian.com/commentisfree/2015/mar/08/edward-snowden-trust-phone-laptop-sim-cards. [Accessed Apr 2015]
Ohm, Paul. 2009. The Rise and Fall of Invasive ISP Surveillance. *University of Illinois Law Review* 1417-1496.
Open Rights Group. 2016. *Investigatory Powers Act is UK's most extreme surveillance law*. https://www.openrightsgroup.org/press/releases/2016/investigatory-powers-act-most-extreme-surveillance-law.
Open Rights Group. 2018. Investigatory Powers Act 2016, *Open Rights Group Wiki*.https://wiki.openrightsgroup.org/wiki/Investigatory_Powers_Act_2016.
Powles, Julia. 2014. UK's Drip law: cynical, misleading and an affront to democracy, *The Guardian*, Friday, July 18. http://www.theguardian.com/technology/2014/jul/18/uk-drip-ripa-law-sceptical-misleading-democracy-martha-lane-fox. [Accessed Oct 2014.]
Prince, Rosa. 2008. Jacqui Smith plans broad new 'Big Brother' surveillance powers. *Daily Telegraph*. Wednesday, October 15. http://www.telegraph.co.uk/news/politics/3202766/Jacqui-Smith-plans-broad-new-Big-Brother-surveillance-powers.html. [Accessed Apr 2014.]
Rainie, Lee. 2016. The state of privacy in post-Snowden America. *Pew Research Center*. http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/. [Accessed Feb 2018]
Royal United Services Institute. 2015. *A Democratic License to Operate: Report of the Independent Surveillance Review*. London: Stephen Austin and Sons
Sanchez, Andrés. 2009. Facebook Feeding Frenzy: Resistance-through-Distance and Resistance-through-Persistence in the Societied Network. *Surveillance & Society* 6 (3): 275-293.
Sharp, Joanne P., Paul Routledge, Chris Philo, and Ronan Paddison, eds. 2000. *Entanglements of Power: Geographies of Domination and Resistance*. London: Routledge.
Shearing, Clifford, and Philip Stenning. 1981. Modern Private Security: Its Growth and Implications. *Crime and Justice* 3: 193-245.
Shearing, Clifford, and Philip Stenning. 1983. Private Security: Its Implications for Social Control. *Social Problems* 30: 125-138.
Shearing, Clifford, and Philip Stenning. 1985. From the Panopticon to Disney World: The Development of Discipline. In *Perspectives in Criminal Law*, edited by Anthony N. Doob and Edward L. Greenspan, 335-349. Toronto, ON: Canada Law Books.
Shearing, Clifford, and Jennifer Wood. 2003. Nodal Governance, Democracy and the New 'Denizens'. *Journal of Law and Society* 30 (3): 400-419.
Travis, Alan. 2015. Secret report urges treaty forcing US web firms' cooperation in data sharing. *The Guardian*, Tuesday, June 2.https://www.theguardian.com/world/2015/jun/02/web-firms-data-sharing-secret-treaty. [Accessed Apr 2016]
Trottier, Daniel. 2012. *Social Media as Surveillance: Rethinking Visibility in a Converging World*. Farnham: Ashgate.
Warren, Ian. 2015. Surveillance, Criminal Law and Sovereignty. *Surveillance & Society* 13 (2): 300-305.
Wells, Helen, and David Wills. 2009. Individualism and Identity: Resistance to Speed Cameras in the UK. *Surveillance & Society* 6 (3): 259-274.
Wood, Jennifer, and Clifford Shearing. 2007. *Imagining Security*. Cullompton: Willan.
Yadron, Danny. 2016. San Bernadino iPhone: US ends Apple case after accessing data without assistance. *The Guardian*, Tuesday, March 29.https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone. [Accessed Feb 2018]
Zajko, Mike. 2016. Telecom Responsibilization: Internet Governance, Surveillance and New Roles for Intermediaries. *Canadian Journal of Communication* 41: 75-93.
Zittrain, Jonathan. 2003. Internet Points of Control. *Boston College Law Review* 44: 653-688.