Original Research Article

BIG DATA & SOCIETY

Big Data & Society
January–June: 1–15

DOI: 10.1177/2053951720985304
journals.sagepub.com/home/bds
SAGE

Encrypting human rights: The intertwining of resistant voices in the UK state surveillance debate

Amy Stevens and James Allen-Robertson

Abstract

The Snowden revelations in 2013 redrew the lines of debate surrounding surveillance, exposing the extent of state surveillance across multiple nations and triggering legislative reform in many. In the UK, this was in the form of the Investigatory Powers Act (2016). As a contribution to understanding resistance to expanding state surveillance activities, this article reveals the intertwining of diverse interests and voices which speak in opposition to UK state surveillance. Through a computational topic modelling-based mixed methods analysis of the submissions made to the draft Investigatory Powers Bill consultation, the article demonstrates the diversity and intersection of discourses within different actor groups, including civil society and the technology industry. We demonstrate that encryption is a key issue for these groups, and is additionally conflated with a human rights discourse. This serves to unite seemingly disparate interests by imbuing encryption with a responsibility for the protection of human rights, but also threatens to legitimate corporate interests and distract from their own data-driven activities of surveillance capitalism.

Keywords

Surveillance, human rights, encryption, topic modelling, computational methods

Introduction

The Snowden revelations redrew the lines of debate surrounding surveillance, exposing not just the extent of state surveillance practices in both the USA and the UK, but blurring the boundaries between state and corporate surveillance, implicating private corporations in state activities (Bauman et al., 2014; Lyon, 2015). As a result, the revelations could have been disastrous not only for state relations but for the technology industry too. The industry responded to public concerns by focusing on technical means to challenge surveillance, using strengthening encryption as a basis of their post-Snowden PR (Gürses et al., 2016). James Clapper, then US director of national intelligence, directly blamed Snowden for accelerating the onset of commercial encryption, asserting that it had 'a profound effect on [states] ability to collect [data], particularly against terrorists' (McLaughlin, 2016). States have now begun to update legislation to both retrospectively legislate for capabilities exposed by Snowden, but also to increase intelligence services' access to, what former UK PM David Cameron called, 'communication between people which . . . we cannot read' (Griffin, 2015).

In the UK, this legislation came in the form of the Investigatory Powers Act (2016). The aims of the Act were to consolidate the UK's patchwork of surveillance laws to provide transparent, legal grounding to existing powers and activities. However, concurrently, the Act included several new powers. These included the bulk collection of data surrounding online communication and web browsing activities, and requests that the technology industry maintain capabilities to remove 'electronic protection' of communications, a term widely interpreted as referring to encryption.

Department of Sociology, University of Essex, Colchester, UK

Corresponding author:
James Allen-Robertson, Department of Sociology, University of Essex, Wivenhoe Park, Colchester, Essex CO4 3SQ, UK.
Email: jallenh@essex.ac.uk

This expansion of powers in the draft bill received widespread criticism from multiple actors, throughout its development and ultimately into the Act. This legislation is particularly pertinent for research as it represents the first manifestation of legislating for increased government surveillance post-Snowden, a trend which has translated to other developed nations, as most recently demonstrated by Australia's passing of the 'Assistance and Access' Act (2018). As these legislative shifts spread, it becomes vital that shifts in opposition to surveillance capability are thoroughly explored too. These include the diversity of voices and arguments within the debate, the complexity of the relationships *between* these voices and arguments, and the extent to which different voices are heard. This article therefore addresses the following questions; When states increase surveillance, who speaks up in opposition? How is the issue of encryption situated in wider anti-surveillance/pro-privacy debates? And how do these discourses of resistance intersect and interrelate across actor groups?

To answer these questions, this research draws on written submissions made to the Investigatory Powers bill consultation process. Given the post-Snowden timing of the consultation and focus on the interrelation of state and corporate infrastructure for surveillance, the documents submitted to the consultation are therefore as much a public performance of resistance as they are an attempt to influence policy. Analysis of these documents is conducted via an innovative mixed methodology of quantitative text analysis and qualitative interpretation, underpinned by *computational grounded theory*; an approach that emphasises the cross-validation of methods using both computational and qualitative approaches (Nelson, 2017). This analysis contributes to widening our understanding of resistance as a complex interrelated *nexus* of diverse stakeholders, that within the temporarily solidified snapshot provided by the documents, has coalesced around the issue of encryption.

Whilst the analysis identified a number of actors within the debate, the article specifically examines three core groups: civil liberties groups, digital rights groups and the technology industry, and the way in which they are positioned within the debate in relation to one another. The research finds that encryption and security were of particular concern across these groups, demonstrating a strong resistance to legislative changes that interfere with the current state of encryption in the UK. However, the diversity of positions from which these concerns resonate has entangled this security focused resistance with another discourse, that of human rights protection. The article asserts that in turn the technology industry is thus utilising its privileged position as providers of encryption technologies to conflate their own activities with human rights protection, and to frame their data-driven activities of 'surveillance capitalism' (Zuboff, 2015) as innocuous and distant from state surveillance practices. This activity influences but is also enabled by civil liberties groups shifting their discourse towards encryption as a human rights solution, partly through greater alignment with Digital Rights groups, legitimating the technology industry's privileged position.

Literature review

Resisting surveillance: A multiplicity of actors

As Gary Marx (2016: 168) observes surveillance and resistance are counterparts, enthralled in an 'adversarial social dance involving strategic moves, countermoves and counter-counter moves'. Whilst the process Marx describes is rooted in individual actions, such as fooling drug and lie detector tests, and the more stringent methods of surveillance that emerge in response, the Investigatory Powers Act itself can be considered part of a cyclical resistance-surveillance process. Many of the powers the Act introduces are aimed at filling in data blind-spots or overcoming technologies which are considered as resistant to state surveillance practices. Such an approach is thoroughly characterised by the justifications for increased powers which cite that criminals and terrorists are 'going dark' or communicating in ways that cannot be accessed. This position broadly aims to frame privacy enhancing technologies, such as encryption, as enablers of terrorist and criminal activity and something which requires a response; to be stopped or controlled in order to maintain national security, thus resulting in the need for further acts of surveillance, which in turn receive further resistance.

As the Snowden revelations highlighted, state surveillance practices are today bound up in multiple relationships, drawing in a wide range of actors which are necessary to enable them, particularly from the technology industry. Whilst this creates a stake for these actors in the undertaking of surveillance, this is not always welcome, often met with unwillingness and a significant sense of resistance. As such, this has expanded the array of actors which have a stake in resisting state surveillance activities, beyond those in civil society, who have frequently been at the focus of research in this area (Bennett, 2008; Huey, 2010).

A number of studies have also focused on the direct relationship between the surveyor and the surveilled, concentrating on how individuals employ forms of 'everyday resistance' (Scott, 1985) to avoid the gaze of surveillance, including activities to sabotage the collection of data or the employment of privacy enhancing technologies (Marx, 2003). These, along with the

studies focusing solely on civil society, lack recognition of what Martin et al. (2009: 213) termed the 'complex resistance nexus'. For these researchers, resistance relationships and activities in relation to challenging surveillance practices are complex, multifaceted and shift in relation to the proposals made and the groups implicated, revealing a diversity of actors and arguments whose linkages are otherwise lacking throughout research in this area. Whilst more recent work has recognised that a variety of actors influence regulatory and policy debates surrounding surveillance – including the Investigatory Powers bill and the events leading up to its creation (Hintz and Brown, 2017; Hintz and Dencik, 2016) – the impact and interplay of their actions and relationships with one another remains somewhat under-explored. In response, this article considers resistance to surveillance through the 'multi-actor', 'complex resistance nexus' identified by Martin et al. (2009) in their study of the UK's National Identity Scheme in the mid-2000s. This approach recognises the potential for a presence of multiple resistant actors in relation to surveillance proposals and removes any limitations surrounding who is selected for analysis – avoiding limiting the focus to very specific actor groups such as pro-privacy/anti-surveillance advocates and activists (Bennett, 2008; Huey, 2010) – allowing for nuance in understanding how diverse actors diverge and intersect in their resistant positions.

Resistance, however, can take many forms and as a concept is frequently used throughout sociological literature, despite little consensus emerging surrounding its definition (Baaz et al., 2017; Courpasson and Vallas, 2016; Hollander and Einwohner, 2004). To this end studies centring on processes of resistance have ranged in focus from violent protests and riots, transnational and global movements, local labour disputes, and less confrontational encounters of 'everyday resistance' such as foot-dragging, false compliance and sabotage (Scott, 1985). This flexibility has led to charges that such loose parameters allow 'some scholars to see it almost everywhere and others almost nowhere' (Weitz, 2001: 669). Hollander and Einwohner's (2004) wide-ranging meta-analysis demonstrates this lack of consensus, highlighting that *action* and *opposition* are central to the concept but with varying agreement on whether *intention* and *recognition* are necessary for an act to be considered resistance. For example, Baaz et al. argue that requiring explicit intent from those involved can narrow the object and processes explored within resistance research. Instead, they argue that intentions of the actors involved should be considered 'plural, complex, contradictory or evolving as well as occasionally something the actor is not sure about, views differently in retrospect or even is not able to explain' (Baaz et al., 2017: 23). Although such variations may seem problematic, Baaz et al. (2017: 14) refer to them as 'impressive', insisting that resistance is 'better understood as multidimensional, unstable and a complex social construction in dynamic relations that are related to differences of context'. In this sense, the strength of the concept is embedded in its ability to embrace ambiguities and respond to specific contexts and assemblages. A more narrowly articulated definition would artificially obscure new and shifting forms and sources of resistance (Courpasson and Vallas, 2016).

As such, resistance is much more a matter of the act, than the intent (De Certeau, 1984). Whilst we may think of resistance as typically emerging *from below* through activists 'acting' with political intentions, the 'interactional nature of resistance' (Hollander and Einwohner, 2004: 548) means that resistance can not only be determined and defined by resisters own perceptions, but is bound up in the complexity of interactions with others and their reactions to them. As Miller (1997) maintains, one of the problems with studies of resistance is the tendency to try to make divisions between the powerful and the powerless. This ignores that there are multiple, complex hierarchical systems within society that can result in actors being both powerful and powerless, or dominant and resistant simultaneously in different contexts. The most prominent way in which 'powerful' actors have been considered more widely in resistance studies to date is through the notion of 'astroturfing' (Lee, 2010; Walker, 2016). An act which describes how organisations manipulate or convince participants – whilst often attempting to hide their involvement – to voice corporate concerns instead of ones formed of the participants own beliefs, as in 'grassroots' activism (Walker, 2016). As Walker (2016) points out, such a negative framing elides the potential that two very different groups of actors may actually align on an issue at particular junctures, and thus be of mutual benefit to one another within a particular bounded context. As such resistance should be understood not purely as the domain of activists against a single established power, but as a more nuanced context-dependent multi-actor process.

The act of resistance focused on here is thus the official submission of responses to state surveillance legislation which aim to challenge, change or renegotiate state surveillance practices. These responses, and the objections which they contain, allow us to understand who takes part in such resistance, how concerns and proposals surrounding encryption are situated within the debate by different actors, and how these positions impact one another. As a result, it provides a wider understanding of how resistance to changes of

surveillance legislation is shaped in the UK within a multi-actor framework.

Civil liberties: The challenges of protecting privacy

Organised resistance to surveillance issues is currently most widely explored in Bennett's(2008) work *The Privacy Advocates*. For Bennet it was the diversity of issues faced, and causes privileged by 'advocates', that resulted in a 'loose' and 'fragmented' network that fell short of becoming a successful social movement. Huey (2010) has added that a key factor in this failure was in the framing of the issue, noting the lack of clarity surrounding whether the core focus for those involved was anti-surveillance or instead on strengthening privacy rights.

The two are often considered interchangeable, but others have made useful distinctions between them. Martin (1998) argues that whilst, 'focus[ing] on privacy directs attention to the individual whose privacy is invaded; a focus on surveillance directs attention to the exercise of power and to the groups that undertake it'. This view relies heavily on the idea that privacy is most frequently understood as an individual right, borne out of forms of contemporary liberal individualism in which individual judgement and conscience are privileged and defended (Fairfield, 2005). However, as Huey (2010: 706) argues, creating a movement based on 'anti-surveillance' may have proved challenging as there is no 'ready hook upon which to construct legal, moral, and ethical challenges to programs or regimes'. On the other hand, a 'right to privacy' is already visible in legislation, public discourse and enshrined in state constitutions. Bennett (2008: 23) argues that despite conceptual confusion over what we mean by privacy and how best to frame the movement, 'for better or worse, privacy is still the concept around which the major policy issues have been framed . . . and "privacy advocates" have learned to live with it'. However, as surveillance systems have become progressively more complex and everyday life has become increasingly mediated by technology, new issues are emerging which may challenge such an assumption.

Surveillance's interrelation with technology poses specific challenges for civil liberties groups, forcing new 'multi-sectoral realities' on 'traditional human-rights actors', that have not necessarily had to engage with technology as both adversary and potential activist tool (Guberek and Silva, 2014: 3). Guberek and Silva (2014) identify an emerging skills gap making it increasingly difficult for human rights advocacy to keep up with the increasing significance of technology as a social infrastructure without enhanced collaboration. This gap is further acknowledged by the privacy advocacy group, Privacy International (2018), who have argued that the human-rights sector requires a greater influx of technologists not simply as a transplant into the sector, but as part of a broader cultural shift that reorients the thinking of organisations in full. Furthermore, Dencik et al. (2016) found post-Snowden resistance to surveillance to be predominantly centred on techno-legal concerns regarding the use of encryption and advocating for improved privacy and data protection policy. They argue that this results in surveillance remaining an issue of 'tech-justice' activists which fails to resonate with wider social justice movements.

Others have argued however, that the libertarian ethos of individualistic privacy concerns does provide a concept capable of bringing together 'those who would prefer a minimal, largely technical approach- . . . and those who seek greater juridical and legislative protection against abuses of power' (Johns and Joyce, 2014), thus providing a position which allows for diverse collaborations. For the civil liberties groups concerned, one potential source of technologically astute allies is therefore digital rights advocates.

Digital rights discourse

Recent years have seen growth in the usage of the term 'digital rights' in discussions of the way human rights are applied to the digital age. Such discourse has been driven in part by groups such as the Electronic Frontier Foundation in the US and the Open Rights Group in the UK who, in these particular national contexts, rely on a 'digital rights' framing to focus their activities specifically on issues relating to privacy, freedom of expression and consumer rights online. In parallel there has been a growth in governments and international organisations creating declarations to protect rights and freedoms in the digital age. Initiatives such as the United Nations World Summit on Information Society (WSIS) and subsequently the Internet Governance Forum have represented global attempts to draw human rights into debates surrounding internet governance (Karppinen, 2017). These events have drawn a wide spectrum of civil society organisations attempting, with varying success (Padovani et al., 2010), to raise the relevance of human rights in relation to the emerging information society. Whilst civil liberties groups' familiarity with issues related to emerging digital technologies have therefore grown in recent years, in part due to increased integration with digital rights groups, this integration comes with a complex ideological history.

In the US context, digital rights groups, such as the EFF – which heavily influenced the founding of the UK's core digital rights presence, the Open Rights Group – are rooted in an ideology that was solidified

in the 1990s through polemics from writers such as Alvin Toffler, Esther Dyson and John Perry Barlow (see Winner, 1997). This ideology celebrated the potential of online space to liberate individual freedoms from the impositions of pre-existing state structures. Identified by Winner (1997) as 'cyberlibertarianism' and later by Coleman and Golub (2008) as rooted in broader American Liberal Libertarianism, it is an ethic that emphasises empowerment of the free individual, particularly via technological means alongside a distrust of state institutions as intrinsically limiting of individual freedoms. Whilst the reframing of the debate as pro-privacy has drawn digital rights together with civil liberties groups that still retain faith in juridical and legislative change (Johns and Joyce, 2014), digital rights' groups emphasis on tools (Daskal, 2018) continues to highlight differences with civil liberties campaigners (Aouragh et al., 2015). Although this distinction may be starting to shift, these groups retain a historical preference rooted in the liberational polemics of defending against policy rather than intervening in it.

This ideology also has a shared history with Silicon Valley and the technology industry more broadly, both emerging from the radical individualist anti-statism of the counter-cultural movement (Markoff, 2005; Turner, 2006). Despite shared roots, digital rights groups often sit in tension with the industry. Increasingly prevalent practices such as mass data harvesting, or the locking down of technology through intellectual property claims can draw these groups ire as they impinge upon individual liberties of privacy and autonomy. Messenger services Signal and Telegram illustrate this tension well. These non-profits offer open-source, encrypted communication products, near indistinguishable from industry offerings, blurring the line between tech product and activism in opposition to both state and corporate surveillance. Whilst these open source offerings are not necessarily industry products, they contribute to the broader notion that technological solutions, whatever their provenance, are the appropriate solutions. As Giridharadas (2019) argues, this is part of a larger ideological formation that encourages new companies to 'zoom-in' on societal issues to the point at which they become bounded, solvable technical problems. Solving the technical problem becomes conflated with solving the societal issue, to the extent that broader structural issues of politics, inequality and power become obscured. As such despite resisting industry surveillance, the elements of digital rights advocacy that focus on technological solutions share this Silicon Valley ethos that the technologically empowered individual can disempower an overbearing state.

The technology industry

There is often an emphasis on the way portions of the technology industry enable state surveillance practices, through their own data-driven business practices. Whilst these activities remain problematic (Vaidhyanathan, 2011; Zuboff, 2015), the industry also plays an overlooked resistant role in constraining state surveillance too. Rozenshtein (2018) posits that due to their growing involvement in mediating state surveillance demands, no accurate analysis of surveillance today can be undertaken without inclusion of how these companies 'constrain, not just enable, government surveillance' (p. 106). Although this analysis is grounded in reference to Silicon Valley's technology giants, conceiving them as 'surveillance intermediaries', his description of 'companies that stand between the government and our data' (p. 105) can be extended as more commercial entities are pushed to assist, and therefore mediate, state surveillance practices.

Taking an oppositional rather than facilitative position to state surveillance also has its benefits for the industry. By focusing the surveillance debate on state surveillance it distinguishes it from, and obscures, commercial surveillance (Gürses et al., 2016). For many sectors it is also a valuable strategy to retain custom, as they rely on public trust to maintain their customer base (Chivers, 2019). As Rozenshtein (2018: 116) puts it, the primary 'victory' of Snowden's disclosures was 'to increase incentives for the surveillance intermediaries to resist the government'. This has inverted the post-9/11 shift of greater industry and state collaboration, driven by public opinion at the time, *towards* a performance of privacy and security, guided by companies' self-interest and image concerns, and thus resistant to state intrusion into users' data.

Encryption sits as a key tool in this realignment. Historically associated both as a tool exclusive to the state, yet also as a facilitator for democratic values (Myers West, 2018), encryption generates significant tension between corporate and state actors. There is, however, a lack of empirical research exploring state resistance within the industry, especially considering their privileged 'intermediary' role. Some high-profile cases around industry provision of encryption have received attention, such as *Apple v FBI,* in which Apple announced that they would not willingly assist in unlocking an encrypted iPhone (Schulze, 2017), and Facebook's similar public positioning through the enabling of end-to-end encryption in their WhatsApp messenger service. These public expressions of concern over the undermining of security in their products both highlighted the intertwining of the technology industry and state surveillance, but also publicly signalled the industry's shift to a more defensive rather than

collaborative position. Encryption's role is significant for the industry. Whilst framed as a matter of personal liberty for users, encryption also comes with many benefits to the providing industries. Encryption allows them to distance themselves from the requirements of governments and the ethical and human rights concerns this raises. It also distances industry from responsibility for the communications they carry, whilst embedding an astute corporate strategy of user liberty and security which cannot be interfered with whatever the regulatory regime.

Methodology

This study used a mix of both quantitative text analysis and qualitative interpretation. The quantitative work was performed using the Python programming language as the framework to develop custom data extraction, analysis, and visualisation techniques suitable for the research topic. Broadly, this consisted of text processing, cleaning and normalisation techniques common to natural language processing, and topic-modelling for the extraction of themes from the corpus. Document similarity measures were used to assess corpus coherence and to check for the presence of outliers. Whilst the use of computational text analysis is growing within the social sciences, difficulties of interpreting the results require a union of both quantitative and qualitative assessment, as well as a focus on the meaningful interpretability of computational outputs (Nelson, 2017). In this study, qualitative assessment of the text analysis process outputs was used to both validate the quantitative modelling and then later to inform, direct and support the qualitative interpretation of the documents.

Data collection and preparation

To construct a suitable corpus of documents for analysis, researchers manually collected PDF copies of all 220 submissions to the Investigatory Powers consultation (November 2015–January 2016) from three parliamentary committees: The Science and Technology Committee, the Joint Committee on Human Rights and the Joint Committee on the draft bill. Each document was manually classified into nine different categories of actor. Priority was given to the way in which authors identified themselves either within their submission or in public facing material. Where there was a lack of clarity in classification a number of strategies were adopted. First, the authors distinguished between civil *society* and civil *liberties* NGOs as civil society groups represented a highly diverse range of issues without overall coherent aims that would warrant grouping into a single classification. This resulted in a further distinction being made between civil Liberties groups and those that focus on digital rights based on their histories, and the groups' self-framing within their submissions and mission statements. For example, groups classified as digital rights included the Electronic Frontier Foundation and the Open Rights Group who have a lineage of working within the digital rights space since the 1990s and early 2000s. Conversely the civil liberties groups such as Liberty and Amnesty International are characterised by their emphasis on protecting human rights, usually through campaigns and legal actions, and have long established historical roots, dating back decades in the UK. Whilst these groups have a long history of legal actions and campaigns against surveillance practices, compared to the digital rights groups, they are relative newcomers to commenting on digital and technological issues. Submissions from individuals that also held a key role in a sector such as Government or Industry were categorised according to their professional role. Individuals and public figures with specialist knowledge, but not representing the views of a particular sector, such as academics and independent consultants, were categorised as 'Independent Experts', similarly to those termed 'informed advocates' elsewhere (Whitley and Hosein, 2008). Retired individuals that no longer worked in a sector were categorised as 'Other', recognising that they may not express the contemporary concerns of the relevant sector. This category also included a range of submissions from members of the public, alongside think tanks and independent regulators whose organisational status excluded them from other categories such as Government or Industry. The diversity of their priorities also meant that grouping them together into their own organisational categories would have been redundant as they lacked a coherent voice or concern. A description of the categorisation can be seen in Table 1.

Each document in the corpus was cleaned and tokenised to common text pre-processing standards. Processing stages included cleaning the text of low informational content such as URLs, the removal of punctuation and 'stop' words such as 'be', 'is', 'this'[1] and common collocations of words were identified to isolate phrases such as 'Human rights' and 'freedom of expression'.[2]

Topic modelling

Topic modelling is a well-established technique of unsupervised machine learning, favoured by social scientists (for examples see Marciniak, 2016; Nelson, 2017; Torabi Asr and Taboada, 2019) for its potential to support the exploration of latent structures in textual data (DiMaggio, 2015). In other words, topic modelling can assist social scientists in unearthing the

Table 1. Final document classification after outlier removal.

Author category	Document freq.	Total words	Avg. words per document
Civil liberties	16	119,660	7478
Digital rights	19	73,110	3847
Government	11	85,344	7758
ISP/Telecomms	20	74,232	3711
Independent expert	46	127,916	2781
Legal professional/Body	17	68,410	4024
Media/Journalism	7	14,733	2104
Other	70	127,427	1820
Tech industry	13	32,219	2478

discourses that exist across a set of documents. The result of a topic modelling process is the decomposition of a corpus of documents into a document-to-topic array and a term-to-topic array. For each array, every term and every document are given a score indicating the extent to which it is affiliated with each topic. Firstly, these affiliation scores allow us to understand what each topic is about, based on the most strongly affiliated terms in the term-to-topic array. Secondly, by providing each document an affiliation score for every topic in the document-to-topic array, topic modelling recognises that a single document may express a multitude of topics. As such it is possible to examine the extent to which a single document expresses a range of different topics.

This study utilised a less conventional topic modelling technique called Non-Negative Matrix Factorisation (NMF) which performs well when discerning nuanced topics within a relatively homogenous corpus. Homogeneity in this context refers to the similarity of vocabulary. LDA works well in distinguishing documents when their vocabulary differs substantially but struggles to tease out the nuance of differing uses of the same vocabulary. NMF is able to better discern this nuance because of its reliance on weighted word scores. These scores factor in how each word is used within each document, and across the entire corpus of documents. However, NMF scales poorly, making it less popular in applied large scale text processing tasks where topic modelling is normally deployed. NMF produces affiliation scores that indicate the extent to which a document expresses each topic through its use of topic related words. This adds a level of complexity where each document will vary in its degree of affiliation not just with each topic, but with all topics entirely, requiring additional steps when interpreting the result of the modelling. Whilst a quantitative approach, topic modelling should be understood as an interpretative method. The exact figures produced by the model are better understood as indicators of potential patterns for exploration, making it particularly useful for a mixed-methods approach.

Implementing and refining the topic model

A limitation of topic modelling is that the model is unable to determine how many topics exist within the corpora and requires the number of topics (often referred to as k) to be assigned before it begins modelling. This is a key issue for researchers and often the recommendation is to rely on domain knowledge, such as knowing you are modelling text from four different forums, to specify the most likely number for k. This limitation can be problematic for research applications where computationally aided pattern extraction is wanted without necessarily introducing bias by manually selecting the number of themes to be identified.

Initially, an exploratory topic model was run with k corresponding to the number of actor categories, as an assessment of the technique's viability for the corpus. Qualitative assessment of the model was performed by examining the top words for each topic and the scores that indicated what proportion of each document affiliated to each topic. Whilst the model had generally performed well indicating strong topics such as 'encryption' and 'oversight' it was also highly sensitive, with entire topics dominated by the content of one or two documents. To address this, outliers were identified by visualising document similarity using a common document similarity measure.[3] This identified a single document which was qualitatively assessed to be distinctive in its style and approach and inordinately influential in the overall modelling. This outlier was removed, giving us a final corpus size of 219 documents. After removing the outlier from analysis, the appropriate number of topics (k) was selected by assessing the model for topic stability and topic coherence (see Greene et al., 2014; O'Callaghan et al., 2015).[4] These measures indicated that a seven-topic model produced the most stable topics with a high level of coherence that was representative of the majority of the corpus. After running the final model, a label was derived for each topic by examining the top 20 most affiliated terms and each topic's most strongly affiliated documents (Table 2).

Table 2. Topics.

Topic #	Highly associated terms	Qualitative review – illustrative quotation	Topic label
1	Data, bill, power, service, communication, draft, provider, cost, CSPS, business, retain, provide, obligation, UK, would, require, may, access, security, retention	'The need for CSPs to store data for twelve months and to provide wider assistance to law enforcement organisations will increase operating costs and the cost of compliance will ultimately fall to their UK customers'	Impact on industry
2	Data, packet, use, internet, log, IP address, ICR, ICRS, ISP, service, would, connection, retention, ISPS, record, communication, protocol, TCP, server, email	'ICR is not a recognised term, and its broad wording has the potential to include vast amounts of data that [companies] do not retain, and potentially cannot retain, for business purposes . . . it could involve some communications services having to be altered or redesigned.'	Technical implementation
3	Encryption, security, use, software, vulnerability, would, computer, government, user, equipment interference, technology, system, bill, hack, company, device, attack, internet, service, CNE	'Given the expertise of technology companies, they should be able to construct a system that keeps the data of nearly all users secure but still allows the data of very few users to be read covertly when a proper warrant is served. But the Government does not know in advance which individuals will become targets of investigation, so the encryption system necessarily would need to be compromised for everyone.'	Encryption and security
4	Bulk, data, intelligence, agency, personal datasets, power, GCHQ, use, bill, collection, communication, record, information, NSA, interception, evidence, committee, write evidence, target	'bulk personal datasets involve the collection and storage of the private or personal data of any and all British citizens . . . The extent to which the privacy of citizens will be intruded upon must be properly explained. Without clarity on the issue of bulk personal datasets . . . it is impossible to properly scrutinise the proposal.'	Surveillance structures
5	Journalist, source, protection, journalistic material, medium, pace, police, journalistic, application, material, journalism, RIPA, safeguard, identify, press, bill, public, power, right	'The Draft Bill would enshrine sweeping powers affecting all citizens, including journalists and their sources . . . Comprehensive and stronger safeguards than those provided by the current draft Bill for journalism and journalistic sources are necessary.'	Special Exemptions
6	Human right, IP bill, right, surveillance, draft, data, privacy, access, communication, retention, law, international, government, bulk, freedom of expression, user, provide, article	'Data retention mandates infringe upon individual privacy and chill the exercise of human rights including freedom of expression and freedom of association. This infringement is particularly pronounced in situations without meaningful limits to the scope of the data that provider can be compelled to retain.'	Human Rights
7	Warrant, power, clause, judicial commissioner, authorisation, communication, judicial, interception, commissioner, bill, draft, act, IPT, secretary of state, public, intelligence, investigatory, make, review	'The so-called 'double-lock' process fails to ensure a proper independent authorisation process. As is reflected in judgments from both the European Court of Human Rights and the Court of Justice of the European Union, the decision as to whether to issue a warrant should be made by a judicial authority with sufficient independence from the executive. Otherwise, the prior authorisation cannot provide an effective fetter on executive discretion – it is not a true safeguard against abuse.'	Authorisation and oversight

Findings

An overview of the topics identified

Table 2 displays the top 20 terms identified by the Topic Modelling process for each topic, followed by an illustrative quotation, selected through a qualitative examination of the documents most strongly associated with each topic. The qualitative examination then allowed for an appropriate label to be ascribed to each topic.

Figure 1 demonstrates the intertwining of voices within the debate by first grouping the documents by actor type before calculating the mean affiliation score. The thickness of the line from actor type to topic illustrates this averaged affiliation. The height of the bars to the left indicate how strongly each actor group affiliated to all the topics identified. As expected, the documents with the weakest affiliation scores, i.e. the shortest bar, were those categorised as 'Other'. These were the anomalous documents without clear affiliation, and consequently, this group was disregarded from further analysis. In addition, 'Independent Experts' similarly covered a range of topics, but were grouped as one due to the 'informed' (Whitley and Hosein, 2008) nature of the concerns they expressed, this is reflected in their submissions which are relatively evenly distributed across all topics. The diversity of their concerns without a clear sector affiliation meant their documents were unsuited to this particular method and therefore excluded from further analysis. However, these independent experts made valuable submissions to the consultation, which would warrant follow-up qualitative work examining their role in challenging the legislation and the impact of their contribution. The government express focus on particular areas but their voice within the debate acts not as an external stakeholder, but to legitimate policy proposals, often writing in direct response to other submissions and public debate and are therefore not resistant to the legislation.

Figure 2 also shows these topic distributions and provides scores that indicate the percentage of submission text (after normalising affiliation scores) that affiliates to each topic, per author category.

An initial reading of Figure 2 indicates a range of findings. First were the sectors that engaged almost exclusively with a specific element of the debate. 'Media and Journalism bodies' focused heavily on 'special exemptions' which related to the protection of journalistic sources indicating less a stake in wider debates, but more concern with a single issue. Similarly, ISPs and Telecomms groups spread their focus across 'impact on industry' and the 'technical implementation' of the bill, whilst Legal Professionals' central concern was 'authorisation and oversight'.

Of particular interest to our research questions is how diverse voices contribute to the debate. Of the remaining actors there were indications of an overlap in their topic affiliation, centralising around the issues of encryption and human rights, suggesting a blurring of actor domains within the debate.

Intertwining voices

As expected, the technology industry submissions have particularly strong affiliations with the topics of 'Encryption and Security' and 'Impact on Industry'. However, the findings also highlight the Industry's affiliation with the topic of 'Human Rights', supporting findings from recent research (Jørgensen, 2017, 2018) which suggests that Industry actors view themselves as committed to Human Rights, working to actively promote and

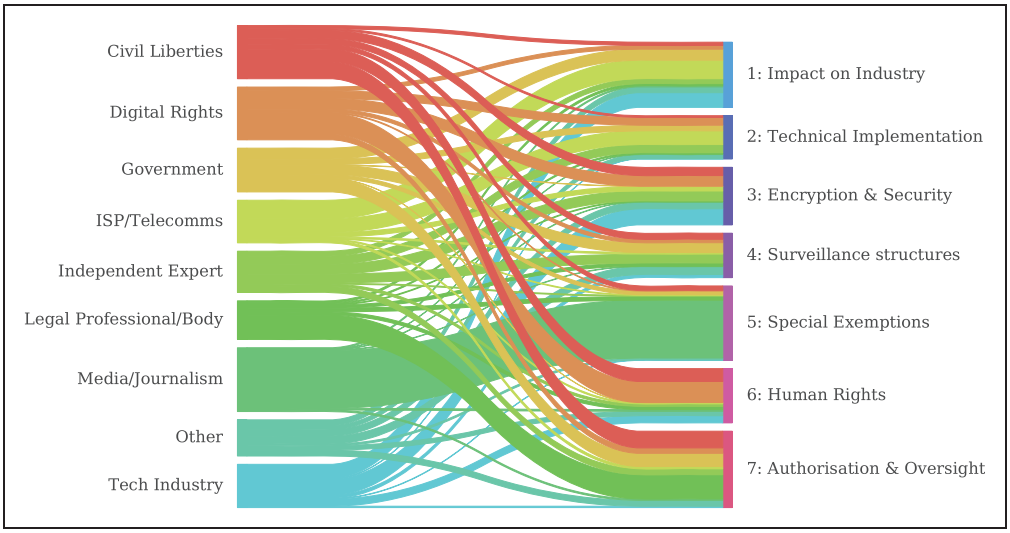

Figure 1. Average distribution of submission text to topic per author category.

Figure 2. Heatmap of categories against topic affiliation – mean of per category affiliation score.

challenge issues in this area. Whilst Civil Liberties groups showed strong affiliation with the legal process through 'Authorisation and Oversight' they also expressed affiliation with the issue of 'Encryption and Security', despite research suggesting that these groups need to work on improving their knowledge and understanding surrounding technical issues (Guberek and Silva, 2014). Digital Rights groups' submissions show a stronger affiliation with 'Technical Implementation' and 'Encryption and Security' than they do with 'Authorisation and Oversight', reflecting their focus on the nuances of technology over legal concerns. However, the findings also show that Digital rights groups' arguments were strongly affiliated with 'Human Rights' discourse. This suggests a convergence of digital rights and human rights discourse as the locus of concern for these different groups within civil society, exemplified further by emerging and diverse campaigning coalitions such as 'Don't Spy Us'.[55] Guided by these findings from the topic modelling, the following sections report insights from the qualitative examination of the submissions strongly affiliated with the theme of 'Encryption and Security', to consider the emergent effects of the intersection of these different key groups around the issue of encryption.

The technology industry and human rights

As indicated by the topic modelling, whilst the technology industry substantially discussed the impact of the bill on industry and encryption, their submissions also utilised a human rights discourse otherwise predominantly used by the digital rights and civil liberties groups. In part this can be seen in the submissions as a recognition of the industry's emerging influence in social and power relations;

> we recognise that our products, technology, and operating footprint increasingly intersect with human rights issues . . . and that as a company, we have an obligation

> to engage responsibly, to respect the rights of our users and to promote the principles of free expression and privacy. (Technology Industry – Joint Committee)

With others noting that they have a role in 'ensuring that citizens' human rights and privacy rights are protected' (Technology Industry – Joint Committee).

This interest in promoting themselves as protective of user safety and users' rights is strongly linked to discussions of their implementation of user level encryption as protection from state surveillance powers and a rejection of state-imposed regulation of encryption: '[A]ll Internet users have an expectation of privacy . . . and companies and technologists continue to support this expectation through policy and through technology' (Technology Industry – Science and Technology Committee). '[E]ncryption is . . . crucial to ensuring the safety of web users worldwide. We reject any proposals that would require companies to deliberately weaken the security of their products via backdoors, forced decryption, or any other means' (Technology Industry – Joint Committee).

In the case of one submission, this responsibility is elaborated into a broader moral imperative: 'We will continue to deploy strong encryption methods because we firmly believe [it is] ultimately in the best interests of humanity' (Technology Industry – Joint Committee).

As providers of encrypted services, this conflation of encryption with a user rights discourse allows the industry not only to position themselves as acting in the best interests of their users, but to construct themselves as *the* protectors of our rights in online spaces. The position held by the industry, whilst recognising that technological development has contributed to the problem of expanding surveillance practices, is that individual-level encryption is *the* solution to protecting individual freedom; an ultimately cyberlibertarian view. More concretely, as the providers of those solutions, their discourse also drives more users to the industry's communication platforms, as the only means by which trust in secure technology and communications can be maintained. This follows long strained debates surrounding the regulation of encryption, often led by digital rights groups along with the industry who have argued strongly that it must remain free from state intervention (Levy, 2001). Through these arguments, encryption is positioned as central to the protection of privacy and rights online in response to increasing state surveillance practices. An argument which was also identified in the submissions of civil liberties and digital rights groups.

Civil liberties, digital rights and encryption as protection

In the past, technical arguments and approaches to countering state surveillance were often considered the domain of the 'geeks' (Bennett, 2008: 82), solely residing within the campaigns of digital rights groups and wider expert communities (Levy, 2001), supported by research which highlights a lack of engagement with technical issues from civil liberties groups (Guberek and Silva, 2014). However, this appears to be shifting as encryption is presented as an important topic for many civil liberties organisations, in part due to a larger declaration at the UN level which supports an explicit link between encryption and human rights (Myers West, 2018).

A closer reading of the documents affiliated with the 'Encryption and Security' topic revealed that core to much of the discussions from Civil Liberties groups surrounding encryption was in framing it as an enabler and protector of human rights online. Statements such as; 'end-to-end encryption is essential to the protection of privacy and free expression in the digital era' (Civil Liberties Group – Joint Committee), and that '[a]ny provisions that could be interpreted to require companies to weaken secured services or build backdoors into encryption raises serious human rights concerns' (Civil Liberties Group – Joint Committee). Encryption and other technical issues such as equipment interference, data retention and security issues also featured frequently throughout the submissions of these groups, highlighting a broadening in their focus towards technology and technical issues. This emergent concern from civil liberties groups that technological interventions should be considered 'essential' to the protection of human rights in the digital era is more akin to what was expected from the digital rights groups, who have historically shared the technology industry's ideologically libertarian and technologically determinist roots and their championing of technology as a viable solution to social problems (Coleman and Golub, 2008; Winner, 1997).

This approach was illustrated throughout Digital Rights groups' submissions, as concern for human rights, integrity of the internet and the health of the economy were concurrently highlighted whilst retaining a strong focus on the role of technology in their maintenance; 'Encryption not only facilitates the free exercise of human rights, but it also benefits the economy, dissuades against device theft, and protects against unauthorised access [to] sensitive data.' (Digital Rights – Science and Technology).

However, through arguing for the value of encryption as a tool to ensure individual liberties, there also appears to be increasing recognition of the unequal gaze of surveillance powers, and who may be most affected by their expansion; 'encryption allows journalists, activists, and members of at-risk populations to communicate . . . For example, in spite of threats of harassment, imprisonment, or death, encryption

allows LGBT persons the ability to communicate and seek knowledge and support' (Digital Rights – Science and Technology).

This frames the case for encryption through a lens of supporting and protecting the rights of those who are most vulnerable within societies, broadening the political approach to consider who and what should be protected from expanding state surveillance practices. This politicises their arguments in line with civil liberties groups whose concerns most frequently lie with the vulnerable or marginalised, who often find themselves central to the gaze of surveillance. However, this alignment towards technological solutions for the protection of human rights from both digital rights and civil liberties groups, also affords opportunities for the providers of these technologies to position themselves as central to, and the guarantors of, human rights in digital spaces. This position was also strengthened by several of these groups who – far from taking a critical position towards the industry – in their own submissions, directly quoted comments made in support of protecting encryption from well-known industry figures, such as Tim Cook and Mark Zuckerberg. For example, as one civil liberties group stated;

> A number of technology companies have warned that this could be a threat to strong encryption in the UK. Encryption protects ordinary citizens and is vital to a myriad of online activities. Its use has been supported by the ICO, Mark Zuckerberg, the Information Technology Industry Council and Tim Cook. Any clauses that seem like they may weaken it will also harm innocent citizens...

Consequently, this demonstrated an endorsement of industry views within this context of challenging the state. Such a practice further highlights the entanglement of different voices within the debate and how the presence of multiple actors can influence one another's engagement with different issues.

Discussion: Encrypting human rights

A key insight illuminated by the quantitative analysis is the intertwining and interconnectivity of diverse resistant voices and discourses within the surveillance debate, particularly surrounding encryption. Not only are a range of actors involved in the debate, but they also share intersecting positions, demonstrating the importance of taking a multi-actor approach to studying processes of resistance. These broader insights guided the qualitative analysis, which in this case, highlighted an emerging focus on encryption as a key component in the protection of human rights, a position shared by civil liberties, digital rights groups and the technology industry.

Within this intersecting discussion, encryption is positioned as the enabler and protector of the right to privacy and freedom of expression online and therefore something which must be protected from interference by state surveillance practices. This notion centralises technical solutions to political and civil issues in resistance debates, which is strengthened through association with the logic of individual human rights protection. This imbues encryption and broader technological interventions as an 'all-encompassing agent of change', characterised by its viability to meet the desired social goal of privacy protection (Marx, 2010: 564). Under this identity, encryption becomes the final frontier to state surveillance, as a technology which bypasses any legislative declarations or any future political or moral debates.

Encryption, however, is not valueless but carries a history of crypto-freedom politics couched within a broader cyberlibertarian ethic (Coleman and Golub, 2008; Golumbia, 2016; Winner, 1997). These politics are maintained in contemporary debates through a discourse of digital rights which often champion personal protection from social issues through technological solutions such as encryption (Daskal, 2018). Whilst more traditional civil liberties groups maintain a focus on legislative or policy reform, they are also embracing technologies promoted by digital rights groups and the industry. This has shifted encryption out of the technical domain and embedded it within civil liberties groups' ongoing human rights focus, strengthened through collaborative projects such as the 'Don't Spy on Us' campaign. This convergence has also meant that the more focussed priorities of the digital rights groups have been broadened, from a strict focus on internet sovereignty and the implied cybercultural elite of the past, to a recognition of more vulnerable groups and their needs within societies. Together, these two groups for civil and digital liberties are producing intersecting discourses that can provide reciprocal legitimation for their emerging, and converging, positions.

However, this entanglement of resistant actors, influences, and is influenced by the third key group identified within the debate, the technology industry itself. Those who control the mainstream implementations of encryption technologies and communications have seized the opportunity to reframe themselves as guarantors of liberty in opposition to the state, or as providers of what Mejias (2012) terms 'liberation technologies'. In their utilisation of a human rights discourse, they situate themselves within the moral economy of civil society, legitimated by the activist groups who contribute heavily to instilling encryption technology with social power. Meanwhile, many of the

corporations utilising this position are themselves built on a data-driven logic of accumulation, constitutive of 'surveillance capitalism' (Zuboff, 2015), through which the extraction and commodification of Big Data threaten privacy in numerous ways (Lyon, 2014). This self-positioning of companies as our protectors, therefore also presents an attempt to reinforce a false dichotomy of intrusive and dangerous state surveillance practices and benevolent corporate surveillance, strategically redirecting public attention away from the activities upon which surveillance capitalism thrives.

Whilst encryption can allow individuals to better protect themselves from both state and corporate surveillance, the push towards popular encryption services also further perpetuates the 'infrastructure imperialism' that monopolises our everyday communication structures (Vaidhyanathan, 2011). Within that infrastructure privacy becomes a valued consumer feature that perpetuates a depoliticisation of surveillance and privacy issues (Gürses et al., 2016). Surveillance, and protection from it, are rendered instead as part of neoliberal market rationality in which privacy becomes a consumer preference or marketable consumer feature (Jørgensen, 2018). As such, human rights abuses related to surveillance are framed as occurring solely within state activities, and activities to protect human rights through technological self-protection become 'anchored in a commercial rather than civic domain' (Jørgensen, 2017: 292). This is characteristic of a cyberlibertarian way of thinking, which frequently 'conflate[s] the activities of freedom seeking individuals, with the operations of enormous, profit seeking business firms' (Winner, 1997: 16), discounting that such an approach reduces privacy to something which is only available to either the most technologically skilled, or those who can afford to pay for premium privacy services.

Whilst civil liberties groups do of course retain their role in human rights protection within the political and judicial sphere, they too recognise and increasingly promote encryption as protecting human rights and limiting the reach of state surveillance, despite this position threatening to legitimate the 'protector' identity adopted by the industry. Whilst enabling the industry's self-serving narratives of human rights protection is presumably unintentional, this will likely remain a pragmatic path to follow for the civil liberties groups. The industry's powerful PR machine can undoubtedly be a helpful ally in highlighting government practices and providing a form of resistance both legally through challenges to state requests, and technologically through the integration of encryption solutions into their tools and platforms. These moments of alliance between activist groups and industry may even present opportunities for activists to intervene in the tech companies' trajectory. However, whilst this growth in the range of actors discussing encryption and human rights suggests a promising step towards a more critical approach to the use of a technical counter-surveillance, such as strong encryption, it also suggests that these arguments must be made and considered with caution. As such, this also highlights the importance of considering resistance to surveillance as a multi-actor phenomenon within which actors can influence and strengthen one another's positions within the debate, even if not directly or explicitly.

Conclusion

This article has highlighted the intertwining arguments of multiple actors within the surveillance debate, focusing on the complex convergence of encryption and human rights concerns. The implications of the findings outlined suggest that as much as corporate influence can be a powerful ally against overzealous state aspirations, it is crucial that in this alliance, civil society is not utilised to legitimate a narrative that re-directs attention strictly to state surveillance, and positions corporate entities as the protectors of the public. This will be a difficult alliance for activists to maintain whilst remaining critical of corporate surveillance practices in the future. Furthermore, if the industry is to appear honest about supporting our rights in online spaces, beyond self-promotion, they may need to move towards working more closely with their critics who understand the social implications of all corporate actions, not just those that fit within the protector narrative.

For academic work within surveillance, the intertwining of these arguments highlights the complexity of resistance to surveillance and the need to approach and explore this phenomenon from a multi-actor perspective. The resistance debate is thus a blurring of domains across and within actor groups, and an intersection of sometimes conflicting interests between them. Consequently, this should be a central consideration of any research which seeks to explore similar cases in the future.

Acknowledgements

The authors would like to thank all those who contributed to the development of this article including Prof. Pete Fussey and Dr Katerina Hadjimatheou, as well as the editors and reviewers for their insightful feedback. Example code for this project will be available at https://github.com/Minyall/encrypting_human_rights

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This article was supported by the ESRC Human Rights and Big Data Technology Project at the University of Essex [grant number ES/M010236/1].

ORCID iDs

Amy Stevens https://orcid.org/0000-0003-4304-6458
James Allen-Robertson https://orcid.org/0000-0002-1668-8140

Notes

1. Stop word list provided by NLTK (https://www.nltk.org)
2. Collocations identified using Gensim's Phraser class https://radimrehurek.com/gensim/models/phrases.html
3. Implemented in Gensim's Doc2Vec class https://radimrehurek.com/gensim/models/doc2vec.html
4. Topic Stability: https://github.com/derekgreene/topic-stability– Topic Coherence: https://github.com/derekgreene/topic-model-tutorial – Parameter Selection for NMF.
5. https://www.dontspyonus.org.uk

References

Aouragh M, Gürses S, Rocha J, et al. (2015) On division of labour and techno-political practices of delegation in times of crisis. *The Fibreculture Journal* (26): 208–235. https://twentysix.fibreculturejournal.org/fcj-196-lets-first-get-things-done-on-division-of-labour-and-techno-political-practices-of-delegation-in-times-of-crisis/

Baaz M, Lilja M and Vinthagen S (2017) Resistance studies as an academic pursuit. *Journal of Resistance Studies* 3(1): 10–28.

Bauman Z, Bigo D, Esteves P, et al. (2014) After snowden: Rethinking the impact of surveillance. *International Political Sociology* 8(2): 121–144.

Bennett CJ (2008) *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT.

Chivers W (2019) Resisting digital surveillance reform: The arguments and tactics of communications service providers. *Surveillance & Society* 17: 517–532.

Coleman EG and Golub A (2008) Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory* 8(3): 255–277.

Courpasson D and Vallas S (2016) *The SAGE Handbook of Resistance*. 1st ed. London: SAGE Publications.

Daskal E (2018) Let's be careful out there . . . : How digital rights advocates educate citizens in the digital age. *Information, Communication & Society* 21(2): 241–256.

de Certeau M (1984) *The Practice of Everyday Life*. Berkeley: University of California Press.

Dencik L, Hintz A and Cable J (2016) Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society* 3(2): 1–12.

DiMaggio P (2015) Adapting computational text analysis to social science (and vice versa). *Big Data & Society* 2 (2): 1–5.

Fairfield P (2005) *Public/Private*. Lanham, MD: Rowman & Littlefield Publishers.

Giridharadas A (2019) *Winners Take All: The Elite Charade of Changing the World*. London: Penguin Books.

Golumbia D (2016) *The Politics of Bitcoin: Software as Right-Wing Extremism*. Minneapolis: University of Minnesota Press.

Greene D, O'Callaghan D, Cunningham P (2014) How Many Topics? Stability Analysis for Topic Models. In: Calders T, Esposito F, Hüllermeier E, Meo R (eds) *Machine Learning and Knowledge Discovery in Databases*. ECML PKDD 2014. Lecture Notes in Computer Science, vol 8724. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-44848-9_32

Griffin A (2015) Whatsapp and iMessage could be banned under new surveillance plans. https://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html (accessed 4 February 2019).

Guberek T and Silva R (2014) *Human rights and technology*. PRIMA International.

Gürses S, Kundnani A and Van Hoboken J (2016) Crypto and empire: The contradictions of counter-surveillance advocacy. *Media, Culture & Society* 38(4): 576–590.

Hintz A and Brown I (2017) Enabling digital citizenship?: The reshaping of surveillance policy after snowden. *International Journal of Communication* 11(2017): 782–801.

Hintz A and Dencik L (2016) The politics of surveillance policy: UK regulatory dynamics after snowden. *Internet Policy Review* 5(3).

Hollander JA and Einwohner RL (2004) Conceptualizing resistance. *Sociological Forum* 19(4): 533–554.

Huey L (2010) A social movement for privacy/against surveillance. *Case Western Reserve Journal of International Law* 42(3): 699–711.

Johns F and Joyce D (2014) Beyond privacy: Is prevailing legal debate too analog for a digital age? *Human Rights Defender* 23(3): 24–26.

Jørgensen RF (2017) What platforms mean when they talk about human rights. *Policy and Internet* 9(3): 280–296.

Jørgensen RF (2018) Framing human rights: Exploring storytelling within internet companies. *Information, Communication & Society* 21(3): 340–355.

Karppinen K (2017) Human Rights and the Digital Age. In: Tumber H and Waisbord S (eds) Routledge Companion to Media and Human Rights. Abingdon: Routledge.

Lee CW (2010) The roots of astroturfing. *Contexts* 9: 73–75.

Levy S (2001) *Crypto: Secrecy and Privacy in the New Code War*. London: Allen Lane.

Lyon D (2014) Surveillance, snowden and Big Data: Capacities, consequences, critique, *Big Data & Society* July–December: 1–13.

Lyon D (2015) The snowden stakes: Challenges for understanding surveillance today. *Surveillance & Society* 13(2): 139–152.

McLaughlin J (2016) Spy chief complains that Edward Snowden sped up spread of encryption by 7 years. Available at: https://theintercept.com/2016/04/25/spy-ch

ief-complains-that-edward-snowden-sped-up-spread-of-encryption-by-7-years/ (accessed 24 September 2018).
Marciniak D (2016) Computational text analysis: Thoughts on the contingencies of an evolving method. *Big Data & Society* July–December: 1–5.
Markoff J (2005) *What the Dormouse Said: How the Sixties Counter-Culture Shaped the Personal Computer Industry*. London: Penguin Books.
Martin B (1998) *Information Liberation: Challenging the Corruptions of Information Power*. London: Freedom Press.
Martin AK, van Brakel RE and Bernhard DJ (2009) Understanding resistance to digital surveillance: Towards a multi-disiplinary, multi-actor framework. *Surveillance & Society* 6(3): 213–232.
Marx GT (2003) A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues* 59(2): 369–390.
Marx GT (2016) *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago, IL: University of Chicago Press.
Marx L (2010) Technology: The emergence of a hazardous concept. *Technology and Culture* 51(3): 561–577.
Mejias UA (2012) FCJ-147 liberation technology and the Arab spring: From Utopia to Atopia and beyond. *The Fibreculture Journal* 20: 204–217.
Miller LL (1997) Not just weapons of the weak: Gender harassment as a form of protest for army men. *Social Psychology Quarterly* 60: 32–51.
Myers West S (2018) Cryptographic imaginaries and the networked public. *Internet Policy Review* 7(2): 1–16.
Nelson LK (2017) Computational grounded theory: A methodological framework. *Sociological Methods & Research* 49(1): 3–42.
O'Callaghan D, Greene D, Carthy J, et al. (2015) An analysis of the coherence of descriptors in topic modeling. *Expert Systems with Applications* 42(13): 5645–5657.
Padovani C, Musiani F and Pavan E (2010) Investigating evolving discourses on human rights in the digital age. *International Communication Gazette* 72(4–5): 359–378.
Privacy International (2018) Human rights and technology: Building a modern rights movement one fellow at a time. Available at: https://privacyinternational.org/blog/1717/human-rights-and-technology-building-modern-rights-movement-one-fellow-time (accessed 1 July 2019).
Rozenshtein AZ (2018) Surveillance intermediaries. *Stanford Law Review* 70(1): 99–189.
Schulze M (2017) Clipper meets apple vs. FBI – A comparison of the cryptography discourses from 1993 and 2016. *Media and Communication* 5(1): 54–62.
Scott JC (1985) *Weapons of the Weak: Everyday Forms of Peasant Resistance*. New Haven, CT / London: Yale University Press.
Torabi Asr F and Taboada M (2019) Big Data and quality data for fake news and misinformation detection. *Big Data & Society* January–June: 1–14.
Turner F (2006) *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago, IL: University of Chicago Press.
Vaidhyanathan S (2011) *The Googlization of Everything: (And Why we Should Worry)* Berkeley: University of California Press.
Walker ET (2016) Between Grassroots and "Astroturf": Understanding Mobilization from the Top-down. In: Courpasson D and Vallas S (eds) The Sage Handbook of Resistance. London: Sage.
Weitz R (2001) Women and their hair: Seeking power through resistance and accommodation. *Gender & Society* 15: 667–686.
Whitley EA and Hosein IR (2008) Doing the politics of technological decision making: Due process and the debate about identity cards in the U.K. *European Journal of Information Systems* 17(6): 668–677.
Winner L (1997) Cyberlibertarian myths and the prospects for community. *ACM Sigcas Computers and Society* 27(3): 14–19.
Zuboff S (2015) Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30(1): 75–89.