Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 3, Pages 12-25
Doi: 10.17645/mac.v3i3.277

Article

"Veillant Panoptic Assemblage": Mutual Watching and Resistance to Mass Surveillance after Snowden

Vian Bakir

School of Creative Studies and Media, Bangor University, Bangor, LL57 2DG, UK; E-Mail: v.bakir@bangor.ac.uk

Submitted: 9 April 2015 | In Revised Form: 16 July 2015 | Accepted: 4 August 2015 |
Published: 20 October 2015

Abstract
The Snowden leaks indicate the extent, nature, and means of contemporary mass digital surveillance of citizens by their intelligence agencies and the role of public oversight mechanisms in holding intelligence agencies to account. As such, they form a rich case study on the interactions of "veillance" (mutual watching) involving citizens, journalists, intelligence agencies and corporations. While Surveillance Studies, Intelligence Studies and Journalism Studies have little to say on surveillance of citizens' data by intelligence agencies (and complicit surveillant corporations), they offer insights into the role of citizens and the press in holding power, and specifically the political-intelligence elite, to account. Attention to such public oversight mechanisms facilitates critical interrogation of issues of surveillant power, resistance and intelligence accountability. It directs attention to the *veillant panoptic assemblage* (an arrangement of profoundly unequal mutual watching, where citizens' watching of self and others is, through corporate channels of data flow, fed back into state surveillance of citizens). Finally, it enables evaluation of post-Snowden steps taken towards achieving an *equiveillant panoptic assemblage* (where, alongside state and corporate surveillance of citizens, the intelligence-power elite, to ensure its accountability, faces robust scrutiny and action from wider civil society).

Keywords
counterveillance, equiveillance, intelligence agencies, journalism, public oversight mechanisms, Snowden leaks, sousveillance, surveillance, univeillance, veillance

Issue
This article is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).

1. Introduction

Drawing from three fields of study that rarely cross-fertilise, Surveillance Studies, Intelligence Studies and Journalism Studies, I examine the contemporary condition of surveillance post-Snowden, exploring issues of intelligence agencies' accountability, and resistance to surveillance. While offering a sizeable literature on surveillance of citizens' data ("dataveillance" (Clarke, 1988, p. 499)) by commercial corporations, these three fields say little on surveillance of citizens' communications by intelligence agencies, or on how to resist surveillance. These are major lacunae given the 2013 leaks by Edward Snowden on the extensive nature and means of contemporary digital surveillance of citizens' communications by their intelligence agencies in liberal democracies, with seemingly unwilling complicity from commercial internet and telecommunications companies (Harding, 2014; Intelligence and Security Committee [ISC], 2015). More usefully, however, Surveillance Studies, Intelligence Studies and Journalism Studies each discuss how public organs can hold those in power, including the political-intelligence elite, to account (here termed *public oversight mechanisms*). Synthesising this literature provides conceptual tools and a framework for evaluating how, and the extent to which, contemporary state intelligence surveillance may be held to account by civil society, as well as how the surveillance may be resisted.

Traditional forms of intelligence oversight operate

via internal mechanisms (Inspectors General in the USA), the legislature (closed committees, such as the USA's Senate Intelligence Committee and the UK's Intelligence and Security Committee (ISC)), the judiciary (secret courts, such as the USA's Foreign Intelligence Surveillance Court and the UK's Investigatory Powers Tribunal) and the quasi-judicial (Information Commissioners in the UK). However, intelligence agencies may also be held to account through public oversight mechanisms. Those most frequently discussed by Intelligence Studies and Journalism Studies are the press acting in its fourth estate capacity. Surveillance Studies adds to this a discussion of public oversight mechanisms suited to ordinary citizens, through Mann's (2013) concepts of "veillance" or mutual watching/monitoring. These include "sousveillance", variously described as watching from a position of powerlessness, watching an activity by a peer to that activity, and watching the watchers; and "equiveillance", where a balance, is achieved between surveillant and sousveillant forces. Accepting the inevitability of surveillance in contemporary societies, Mann and Ferenbok (2013, p. 26) seek to counter-balance surveillance by increasing sousveillant oversight from below (what they term "undersight") facilitated through civic and technology practices. Once this balance is achieved, they suggest that such a society would be "equiveillant".

While it can be queried whether equiveillance is achievable given the scale and nature of the surveillance that Snowden revealed, clearly the published leaks themselves formed an important site of resistance to intelligence agencies' surveillance practices, generating international public, political and commercial interventions to counter intelligence agencies' surveillance and hold intelligence agencies to account. These struggles over multiple forms of mutual watching and monitoring involved citizens variously acting as whistle-blowers and subjects of surveillance; journalists variously acting to challenge and condone the mass surveillance; and private corporations variously acting to surveil, and block surveillance of, our communications. Given the scale, nature and political and social impact of Snowden's revelations, as a case study it presents a politically important and intense manifestation of the phenomenon of veillance, providing an information-rich site for studying veillant processes, including the role played by public oversight mechanisms therein.

This enables refinement of theory on veillance suitable to the contemporary surveillant condition. Problematising the concept of equiveillance in a post-Snowden context, I propose what I term the *veillant panoptic assemblage* (an arrangement of profoundly unequal mutual watching, where citizens' monitoring of self and others is, through corporate channels of data flow, fed back into state surveillance of citizens). Finally, I evaluate post-Snowden steps taken towards achieving what I term an *equiveillant panoptic assemblage* (where, alongside surveillance of citizens, the intelligence-power elite, to ensure its accountability, faces robust scrutiny and action from wider society). This draws on Mann and Ferenbok's (2013, p. 26) framework for encouraging equiveillance by increasing sousveillant "undersight" through civic and technology practices—namely better whistle-blower protection, public debate, participatory projects and systems innovations. Applying this framework to the Snowden case study allows evaluation of resistive forces to contemporary state intelligence surveillance. This draws critical attention to whether post-Snowden transparency arrangements are adequate, highlighting productive avenues for further research.

2. Context

2.1. The Dataveillance

The published Snowden leaks claim that the data that intelligence agencies bulk collect includes communication content (such as email, instant messages, the search term in a Google search, and full web browsing histories); file transfers; and what is called communications data (in the UK) and metadata (in the USA) (for instance, who the communication is from and to whom; when it was sent; duration of the contact; from where it was sent, and to where; the record of web domains visited; and mobile phone location data) (Canadian Journalists for Free Expression, 2015).

The leaks state that communication content and communications data/metadata are collected in bulk from two sources. Firstly, the servers of US companies (via Planning Tool for Resource Integration, Synchronisation and Management (PRISM)). This has been run since 2007 by the USA's signal agency, the National Security Agency (NSA), in participation with global internet, computer, social media and telecommunications companies (Microsoft, Yahoo! Google, Facebook, Paltalk, YouTube, AOL, Skype and Apple), although not necessarily with their consent as PRISM allows the NSA to unilaterally seize communications directly from companies' servers). Due to the internet's architecture, the USA is a primary hub for worldwide telecommunications, making these servers data-rich. The second source of bulk data collection is directly tapping fibre-optic cables carrying internet traffic. The NSA does this through the UPSTREAM programme. The UK does this through TEMPORA, run since 2011 by the UK's signal intelligence agency, Government Communications Headquarters (GCHQ), in participation with BT, Vodafone Cable, Verizon Business, Global Crossing, Level 3, Viatel and Interoute. Between 10–25% of global internet traffic enters British territory through these cables en route eastwards, making the UK an important internet traffic hub. TEMPORA stores this data flowing in

and out of the UK, sharing it with the USA (Anderson, 2015; Canadian Journalists for Free Expression, 2015; Royal United Services Institute [RUSI], 2015).

Reportedly, in the UK, the content of communications is stored for three days and metadata for up to thirty days (Canadian Journalists for Free Expression, 2015). The UK's Interception of Communications Commissioner's Office (IOCCO) finds that "every agency has a different view on what constitutes an appropriate retention period for material" (May, 2015, p. 33); and RUSI (2015, p. 22) finds that British intelligence agencies keep bulk data sets for as long as they deem their utility reasonable or legitimate. (Storage lengths have not been confirmed by intelligence agencies (ISC, 2015)). In the USA, PRISM data is stored for five years and UPSTREAM data for two years (Simcox, 2015).

Intelligence agencies have analytics programs to help them select and analyse this collected content. British intelligence agencies reveal their analytics comprise "automated and bespoke searches", with "complex searches combining a number of criteria" conducted to reduce false positives (ISC, 2015, p. 4). Volunteering information not published from the Snowden leaks, UK intelligence agencies state that they generate Bulk Personal Datasets, namely large databases (up to millions of records) "containing personal information about a wide range of people" (ISC, 2015, p. 55) to identify targets, establish links between people and verify information. While intelligence agencies are largely silent on their analytics programmes, the published Snowden leaks have furnished details. They allegedly comprise PRINTAURA, which automatically organises data collected by PRISM; FASCIA, which allows the NSA to track mobile phone movements by collecting location data (which mobiles broadcast even when not being used for calls or text messages; CO-TRAVELER, which looks for unknown associates of known intelligence targets by tracking people whose movements intersect; PREFER, which analyses text messages to extract information from missed call alerts and electronic business cards (to establish someone's social network) and roaming charges (to establish border crossings); XKEYSCORE, which is an NSA program allowing analysts to search databases covering most things typical users do online, as well as engaging in real-time interception of an individual's internet activity; and DEEP DIVE XKEYSCORE that promotes to TEMPORA data ingested into XKEYSCORE with "potential intelligence value" (Anderson, 2015, pp. 330-332).

While governments maintain that their mass surveillance programs are legal, civil society express fears that the executive, mindful of protecting national security, pushes legal interpretation to its limits. For instance, the UK's Regulation of Investigatory Powers Act [RIPA] 2000 allows bulk collection only of "external" internet communications, legally defined as communications sent or received outside the UK (at least one "end" of the communication must be overseas). However, the ISC (2015, p. 40) admits that, while agencies such as GCHQ would not be legally allowed to search for a specific individual's communication from within this collected data if that individual was known to be in the UK, in practice it may be impossible for intelligence agencies to know locations of senders and recipients: as long as the analyst has a "belief" that the person is overseas, the communications would be analysed. (Similarly in the USA, individuals may be targeted for surveillance if they are "reasonably believed" to be outside the USA (Anderson, 2015, p. 368)). Moreover, British intelligence agencies classify communications collected as "external" when the location of senders or recipients is definitely unknown, as with Google, YouTube, Twitter and Facebook posts (unknown recipients); when accessing a website whose web server is located abroad; and when uploading files to cloud storage systems overseas, such as Dropbox (ISC, 2015; Simcox, 2015).

Furthermore, in terms of internet and telephony communications data, the ISC (2015) acknowledges that such data is highly intrusive given that the volume of data produces rich profiles of people. Recognising its intrusive nature, the USA has restricted its surveillance of American citizens' communications data, with the signing into law on 2 June 2015 of the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring [USA FREEDOM] Act **(**HR 2048). This imposes new limits on bulk collection of communications data on American citizens. It demands the use of more specific selection terms, and prohibits bulk collection using broad geographic terms (such as a state code) or named communications service providers (such as Verizon) (Federation of American Scientists [FAS], 2015).

2.2. The Struggle

Intelligence agencies and their official oversight bodies maintain that their mass surveillance programs are necessary to pre-empt and control security risks—this stance mirroring the post-"9/11" shift in the concept of security in the USA and European Union (EU) (Pavone, Esposti, & Santiago, 2013, p. 33). A complete data set enables discovery of new, unknown threats, as past information may help connect needed "identifiers" (such as telephone numbers or email addresses) and reveal new surveillance targets. This leads to a "collect everything" mentality (ISC, 2015; Simcox, 2015). Rejecting the term "surveillance", intelligence agencies state that rather than conducting blanket searches, as implied by press accounts of "drag-net" surveillance, they only search for specific information (Director of National Intelligence, 2013; ISC, 2015; National Academies of Sciences, 2015). The UK's intelligence oversight committee concludes that such "bulk data collection" does not

constitute mass surveillance since British intelligence agencies do not have "the resources, the technical capability, or the desire to intercept every communication of British citizens, or of the internet as a whole" (ISC, 2015, p. 2). However, given the rapidity of technological and analytical Big Data developments (as the ability to collect, connect and derive meaning from disparate data-sets expands) (Lyon, 2014); given secret intelligence-sharing relationships between "Five Eyes" countries (UK, USA, Australia, New Zealand, Canada) (Emmerson, 2014); and given that governmental "desire" is susceptible to change, especially following terrorist atrocities, this reassurance is hardly future-proof.

Mass surveillance of citizens' communications by intelligence agencies was undertaken without citizens' knowledge (prior to Snowden's leaks) or consent. Against mass surveillance stand those who fear government tyranny, such as the author of the Church report (Church Committee, 1976). Senator Frank Church's problem with NSA electronic communications surveillance capabilities in the Nixon era was that if the government ever became tyrannical, "there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know" (Parton, 2014). Forty years later, Snowden's revelations provoke similar warnings. For instance, the European Committee on Civil Liberties, Justice and Home Affairs (2014, Finding 14) warns that "infrastructure for the mass collection and processing of data could be misused in cases of change of political regime". Meanwhile, a study of 2000 citizens from nine European countries regarding security-oriented surveillance technologies (smart Closed Circuit Television, smartphone location tracking and deep packet inspection) shows public concerns about state surveillance. It finds that the public rejects blanket mass surveillance; tends to reject security-oriented surveillance technologies where they are perceived to negatively impact non-conformist behaviour; and demands enforced and increased accountability, liability and transparency of private and state surveillant entities (Pavone, Esposti, & Santiago, 2015).

This struggle between a political-intelligence elite that has imposed mass surveillance, and those who object, initiated legislative consultation across political bodies. The United Nations and EU parliament called for evaluation and revision of national legislation concerning oversight of intelligence agencies' surveillance practices (European Committee on Civil Liberties, Justice and Home Affairs, 2014; United Nations, 2014). Legislative consultation ensued in multiple nations, taking evidence from businesses, Non-Governmental Organisations (NGOs), privacy advocates, the media, intelligence agencies, governments and legislatures. From the USA, four oversight reports have been delivered (National Academies of Sciences, 2015; The President's Review Group on Intelligence and Communications Technologies, 2013; The Privacy and Civil Liberties Oversight Board [TPCLOB], 2014a, 2014b). The UK has delivered one oversight report from the Intelligence and Security Committee (ISC, 2015); reports by the IOCC (May, 2015); and government-commissioned reports on counter-terrorism measures (Anderson, 2015) and British surveillance (RUSI, 2015). Most of these reports commend the existing surveillance regime as lawful, necessary, and valuable in protecting national security and producing useful foreign intelligence, but also recommend changes to legislation and oversight concerning intelligence agencies' surveillance, and greater transparency.

More critically, TPCLOB (2014a) concluded that NSA collection of telephone metadata was of minimal value, illegal, and should be ended. Accordingly, on 2 June 2015, the USA Freedom Act was passed, restricting bulk collection of telephone metadata of American citizens, although not of foreigners. Meanwhile, the British government has maintained the status quo on surveillance legislation. In response to a ruling from the EU Court of Justice declaring invalid the EU Data Retention Directive, the UK passed emergency legislation, the Data Retention and Investigatory Powers Act [DRIPA], in July 2014. This allows security services to continue to access people's phone and internet records, by requiring telecommunications service providers to retain communications data in line with RIPA. As DRIPA expires at the end of 2016, the Anderson Report was commissioned to help Parliament determine whether DRIPA should be renewed. Neither Anderson (2015) nor RUSI (2015) recommend that bulk collection in its current form should cease given its utility in fighting terrorism. Anderson (2015) does, however, recommend that bulk collection of communications data should take place without (as currently) simultaneously needing to collect content.

3. Methodology

As this is a complex, unfolding phenomenon, a case study approach is utilised (Yin, 2013). Snowden's leaks and their aftermath present a politically important and intensely manifested case study on "veillance"—Mann's (2013) term for processes of mutual watching. This enables assessment of resistive possibilities by civil society to contemporary state intelligence mass surveillance; and an evaluation of civil society's ability to hold intelligence agencies to account. This case study identifies core American and British actors participating in the struggle against intelligence agencies' mass surveillance, distilling their central arguments and actions. Writing from the perspective of two years after Snowden's leaks, this enables an evaluation of the relative strengths of different aspects of sousveillant "undersight" identified by Mann and Ferenbok (2013), and

hence of the likelihood of achieving "equiveillance".

While Snowden leaked over 1.7 million intelligence files, few are published (Canadian Journalists for Free Expression, 2015). Better documented is what the leaks signify to core actors, with various perspectives gleaned for this case study. The US intelligence community's public perspective is derived from the website of the Office of the Director of National Intelligence (*IC on the Record*) launched in August 2013 to provide "the public with direct access to factual information related to the lawful foreign surveillance activities carried out by the Intelligence Community" (Clapper, 2013). This contains declassified documents, official statements, interviews, fact sheets, oversight reports and updates on oversight reform efforts. British intelligence agencies' public perspectives are gleaned from GCHQ's website (GCHQ, n.d.); a public statement following an investigation to establish if GCHQ was circumventing the law (ISC, 2013); an ISC report stemming from an 18-month inquiry into privacy and security (ISC, 2015); an IOCC report (May, 2015); and government-commissioned reports on counter-terrorism measures (Anderson, 2015) and UK surveillance (RUSI, 2015) that interviewed the British intelligence agencies.

Perspectives from journalists involved in the leaks are gleaned from the leaks' reportage in two press outlets: the primarily British newspaper, *The Guardian*, with which Snowden's desired first contact, Glenn Greenwald was affiliated, and *The Intercept,* a Web-based reporting consortium which Greenwald then helped start. Books have been written by the journalists involved: Greenwald (2014) and *The Guardian*'s Luke Harding (2014). The leaks have been discussed by Greenwald and Alan Rusbridger (*The Guardian*'s then editor) in publications, television interviews and appearances at UK-based anti-surveillance NGO meetings that I attended across 2014. Perspectives from whistleblower Snowden are garnered from his public declarations online (Snowden, 2013a, 2013b); Greenwald's (2014) and Harding's (2014) books; and *CitizenFour*, the Oscar-winning documentary about Snowden by Laura Poitras (2014)—the first person that Snowden successfully contacted in attempting to reach Greenwald.

NGO perspectives are gathered from public statements at UK-based anti-surveillance workshops and conferences; and documentation abounds online. For instance, NGOs consulted by American and British review and oversight boards spanned civil liberties, human rights, privacy, transparency and press freedom groups. Furthermore, in the UK, Privacy International, Bytes for All, Liberty, and Amnesty International have been pursuing a legislative remedy against the British surveillant state since Snowden's leaks, this generating public documentation (Privacy International, 2015).

Business perspectives from leading technology firms involved in the surveillance are derived from major corporations' own collective public actions, such as their formation of the Reform Government Surveillance coalition in 2013, and their open letters to Obama and the US Congress in December 2013, and to the US Senate in November 2014, calling for surveillance laws and practices to be changed - especially that governments should not bulk collect internet communications (Reform Government Surveillance coalition, 2014). Also consulted were business' written perspectives to the review boards. For instance, TPCLOB (2014b) heard from technology trade associations representing over 500 American and foreign based companies from the information and communications technology sector, spanning infrastructure, computer hardware, software, telecommunications, consumer electronics, information technology, e-commerce and Internet services. Anderson (2015) and RUSI (2015) also discuss industry's views having taken evidence from a broad range of telecommunications service providers.

Having explained the case study's context and methods, the following sections address the literature from Surveillance Studies, Intelligence Studies and Journalism Studies on public oversight mechanisms and the political-intelligence elite. This teases out relevant concepts and develops a framework for evaluating resistance to contemporary state intelligence mass surveillance, applying these insights to the Snowden case study.

4. Public Oversight Mechanisms: Surveillance Studies

Surveillance studies examines routine ways in which attention is focused on personal details by organisations wishing to influence, manage or control certain persons or population groups (Lyon, 2003, 2014). However, Lyon (2015, p. 139) observes that the field's response to Snowden's revelations lacks understanding of the "complex, large-scale, multi-faceted panoply of surveillance". This includes ignorance of the technical infrastructure of global information flow and surveillance; lack of clarity on who surveils, given the blurring between public and private sectors; and lack of understanding of surveillance cultures—for instance, how and why target populations enable, respond to, and resist surveillance. Furthermore, as Klauser and Albrechtslund (2014, p. 284) propose in their research agenda on big data and surveillance, we need detailed research on "how different purposes of surveillance can be distinguished conceptually, with a view to interrogating the mutual imbrications of different forms, functions and problems of surveillance." I attempt, here, to progress conceptual interrogation of surveillance by attending to the complexity of the surveillance that Snowden revealed.

Surveillance is discussed through two main theoretical frameworks: the panopticon and assemblage. Foucault (1977) invokes Bentham's (1791) *Panopticon* (a novel architecture enabling potentially constant sur-

veillance of people within a specific space, such as prisons) as a symbol for contemporary methods of social control, highlighting the exercise of power through self-discipline, self-reflection and training of one's soul under the eye of authority. By contrast, drawing on Deleuze (1992) and the metaphor of the surveillant assemblage, Haggerty and Ericson (2000, p. 606) argue that surveillance works by computers tracking persons, abstracting physical bodies from territorial settings into data flows to be reassembled as virtual "data-doubles", these then targeted for intervention. In a society of ubiquitous computing and networks, this extends surveillance to everyone. This represents a shift from Foucault's disciplinary enclosure to an amorphous "control society" (Deleuze, 1995, pp. 178-179) leading to "ceaseless control in open sites" (Deleuze, 1995, p. 175). In simple terms, our digital identities (or data doubles) are assembled by aggregating and cross-referencing multiple data trails that we leave across the de-centered, geographically dispersed, digital network. These digital identities, while in constant flux, are temporarily and spatially fixed (that is, captured, analysed and acted upon) at multiple sites in the network (for instance by marketers and state security agencies - the heterogeneous surveillant assemblage). This has consequences for our physical selves as the assemblage presumes to know who we are; what we say and do, where and with whom; and from this predict what we may be persuaded to consume, and what we might do in the future (Andrejevic, 2007, Haggerty & Ericson, 2000; Lyon, 2003, McStay, 2014).

These metaphors of panopticon and assemblage have generated many studies of processes and consequences of surveillance control, but few have studied issues of resistance (Fernandez & Huey, 2009). A prominent exception is Steve Mann who, several decades ago, proposed the concept of sousveillance and developed sousveillant technologies. However, Mann's conception of sousveillance draws solely on the panopticon metaphor: as I argue below, we need a fusion between the metaphors of panopticon and assemblage to understand Snowden-revealed mass surveillance and possible resistance.

Mann discusses two types of sousveillance. "Hierarchical" sousveillance refers to politically or legally motivated sousveillance (Mann, 2004; Mann, Nolan, & Wellman, 2003). Here, sousveillant individuals use tools (such as camera-phones) to observe organisational observers, enhancing people's ability to access and collect data about their surveillance in order to neutralise it, and acting as a consciousness-raising force to the Surveillance Society. Hierarchical sousveillance involves recording surveillance systems, proponents of surveillance and authority figures to uncover the panopticon and "increase the equality" between surveillee and surveiller (Mann et al., 2003, p. 333). Mann (2004) also discusses "personal" sousveillance—the recording of an activity by a person who is party to that activity, from first-person perspectives, without necessarily involving political agendas. With the mass take-up of social media globally, personal sousveillance is rife, involving people curating and creating content, thereby revealing their lives, thoughts and feelings (Pew Internet Research Centre, 2014). While hierarchical sousveillance is less common than personal sousveillance, the latter may serendipitously morph into the former. A prominent example is when Military Police at Abu Ghraib prison in Iraq took multiple photos on their camera-phones of their involvement in prisoner torture, these shared within their in-crowd and later leaked to the press, leading to the unraveling of the George W. Bush administration's secret torture-intelligence programme (Bakir, 2010, 2013).

Given the prevalence of surveillance and sousveillance's rapid expansion, Mann and Ferenbok (2013, p. 19) describe a "veillance" society of mutual watching and monitoring. They posit that if sousveillance becomes ubiquitous, and if coupled with political action to enact change from below, then we may reach a state of "equiveillance" where surveillance and sousveillance balance out (Mann & Ferenbok, 2013, p. 26). They suggest that equiveillance would be achieved when:

> veillance infrastructures are extensive and the power requirements to enact change from below are marginal. This type of system would likely protect whistle-blowers, encourage public fora and debate, and implement participatory projects and innovations to the system. Even the powers of oversight in this configuration are likely to be seen from below and subject to evaluation. (Mann & Ferenbok, 2013, p. 30)

Pre-Snowden writings that apply sousveillance to contemporary social practices are drawn to the liberatory and consciousness-raising potential of sousveillance, but also note that anonymity for hierarchical sousveillers is paramount for such social practices to take root (Bakir, 2010). Yet anonymity is precisely what is compromised by contemporary state mass surveillance. Here, the assemblage and panopticon mutually inform each other, with the assemblage (spear-headed by telecommunications companies) providing a stock of analysable material that the panopticon (state intelligence agencies) can appropriate. Lyon (2003) observed this soon after "9/11", as governments traced terrorists' activities through their data trails generated from financial transactions and travel. Today, however, governments' data stock is exponentially greater, as digital communications are central to modern life. That intelligence agencies accumulate and physically store this data for later searching and analysis to reveal new threats and to investigate persons of interest, and that

this has a chilling effect on society, reinforces the panoptic nature of this data re-appropriation. For instance, the Obama administration surveilled journalists' personal emails to reveal the identity of national security leakers so that they can be prosecuted, such activity then discouraging government sources from discussing even unclassified information with journalists (Papandrea, 2014). To flag up state re-appropriation of citizens' communications for disciplinary purposes, including data derived from personal and hierarchical sousveillance (from selfies to whistle-blowing), I call this the *veillant panoptic assemblage*.

I have introduced this new term in an effort to bring conceptual clarity to the complicated post-Snowden condition of mutual watching, while also highlighting resistive possibilities to surveillance. Others have played with the term "panoptic" to capture contemporary mediated, technological surveillance. Examples include the synopticon (the "viewer society" where the many watch the few (Mathiesen, 1997, p. 219)); the super-panopticon (where computer databases construct subjects with dispersed identities (Poster, 1997)); the banopticon (the security state's power to ban inadequate individuals (Bigo, 2006)); and the oligopticon (a networked form of surveillance nodes comprising special places such as parliaments, courtrooms and offices where sturdy but narrow views of the (connected) whole are generated, as long as connections hold (Latour, 2005)). In contrast to such terminological playfulness with the central metaphor of panopticon, I posit that conceptual clarity of the post-Snowden condition is heightened by maintaining intact the term "panoptic" (with its centralizing, state-oriented and disciplinary functions) and coupling it with "assemblage" (highlighting the multi-site and fluctuating nature of data capture to form data-doubles). Bringing these words together with "veillance" highlights two further important aspects. Firstly, that flows of watching and monitoring are multidirectional: they may comprise citizens monitoring themselves and others (including power-holders), retail and communications companies monitoring customers, and the state monitoring everybody. Secondly, this new term highlights that resistance to surveillance may be attempted through different types of veillance. For instance, Mann and Ferenbok (2013) argue for more sousveillance to strive towards equiveillance—their solution for rebalancing the Surveillance Society. However, increased sousveillance is not the only possible mode of resistance to surveillance. Other modes include "counterveillance" and "univeillance" (Mann, 2013).

"Counterveillance" comprises measures taken to block both surveillance and sousveillance (Mann, 2013, p. 7). While Mann describes counterveillant technologies that detect and blind cameras, a non-technological, if extreme, example is going off-grid—total disengagement with all networked, mediated communications in the manner of Osama bin Laden in hiding. Indeed, as Anderson (2015, p. 160) observes, given the centrality of networked digital communications to everyday life, "one can opt out of data collection, but only by opting out of 21st century society"."Univeillance" is where surveillance is blocked but sousveillance enabled (Mann, 2013, p. 7). This can include technological solutions such as anonymisation and end-to-end encryption (which provides security at either end of the communication, so that only the recipient, not the company running the communications service, can decrypt the message). These solutions resist surveillance while encouraging people to continue with their normal communicative activities, including sousveillance. Certainly, many telecommunications and internet companies compelled by the state to participate in bulk collection have since sought to strengthen their privacy and encryption technologies. For example, in November 2014, the popular messaging service, Whatsapp, announced that it would implement end-to-end encryption. In September 2014 Apple and Google moved towards encrypting users' data by default on their latest models of mobile phones, using their operating systems in a way that the companies themselves cannot decrypt (as the encryption on the device is user-controlled), so making it difficult for governments to compel corporations to secretly participate in mass surveillance (Anderson, 2015; ISC, 2015; RUSI, 2015). Such measures, while an expression of the pro-libertarian ethos of Silicon valley companies, are also a form of brand maintenance, designed to regain consumer trust in companies' ability to protect private data, as trade bodies anticipated that Snowden's revelations would lose the US cloud industry $35 billion over three years (Anderson, 2015, p. 203; TechNet, 2013). Journalists also increasingly use anonymisation and end-to-end encryption to protect their sources' identity, their stories and themselves from state snooping (Carlo & Kamphuis, 2014; Harding, 2014).

Post-Snowden, some telecommunications service providers have attempted to raise users' awareness of surveillance. Twitter's policy is to inform its users if they are under surveillance (unless specifically prohibited from doing so by court orders) (Twitter, 2014). Yahoo!, Twitter and Google have published transparency reports (since 2013 for Yahoo!, 2012 for Twitter and 2009 for Google) showing how many requests from governments worldwide they have met (Google, 2015; Twitter, 2015; Yahoo, 2015). Such measures, in unveiling the secrecy of the surveillance, provide a first step for users to assess if they want to take resistive measures such as counterveillance, or univeillance. Yet, making people understand and care about such issues is challenging given their abstract, complex nature. The role of national security whistle-blowers and the press then becomes paramount if hierarchical sousveillance is to flourish, or indeed equiveillance to be attempted.

With this in mind, the following section discusses the fields of Intelligence Studies and Journalism Studies together, as their insights on public oversight mechanisms largely concern the press.

5. Public Oversight Mechanisms: Intelligence Studies and Journalism Studies

An emerging literature from Intelligence Studies and Journalism Studies examines the press' ability to ensure public oversight of intelligence agencies (Hillebrand, 2012; Johnson, 2014). However, while in liberal democracies the press claims to guard the public interest (Boyce, 1978), the balance of research is pessimistic about how far this is possible in intelligence issues. Instead, most research finds that intelligence agencies successfully manipulate the press through strategies of secrecy and propaganda. These strategies are discussed below, with reference to the Snowden case study.

Intelligence agencies deploy various secrecy-maintaining techniques, the most basic of which is to withhold information (Bakir, 2013). The surprise of Snowden's leaks in 2013 attests to the successful secrecy of surveillant intelligence practices, these dating back to changes in US surveillance law introduced under Bush under s.215 of the Patriot Act [2001], and s.702 of the FISA Amendments Act [2008]. The most draconian secrecy-enforcing technique is prior constraint on what journalists can publish (Dee, 1989). Although this is usually associated with 17th and 18th century Britain (Curran, 1978), *The Guardian* believed that its biggest threat in the Snowden story was legal injunctions to prevent publication (Moore, 2014). Other secrecy-maintaining techniques are threats of criminal prosecution against whistle-blowers (Murakami Wood & Wright, 2015), although historically these rarely occur in the USA, with only three leakers prosecuted prior to Obama. Yet, not including Snowden, the Obama administration has indicted seven government officials for leaking classified information; and on 14 June 2013, Snowden was charged under the Espionage Act [1917]. Through such actions, the US government hopes to discourage further leaks in a digital age where technology makes leaking easy regarding scale of data that can be rapidly copied and the rise in online outlets like Wikileaks that resist censorship. Another secrecy-maintaining technique is blacklisting and harassing non-compliant press employees (Bewley-Taylor, 2008). Indeed, *The Guardian*'s employees were forced to physically smash their computer hard drives in London, under GCHQ's tutelage, in July 2013 after *The Guardian* refused to hand back or destroy Snowden's documents, even though its editor pointed out that such destruction was meaningless as its New York office held copies of the documents, as did Greenwald in Brazil and Poitras in Berlin (Rusbridger, 2013). The most common secrecy-maintaining technique is to engender self-censorship by journalists, with journalists complying with state secrecy requests to ensure continued access to official information, or because they are persuaded by governments' national security arguments (Bakir, 2013). In the UK, press self-censorship is institutionalised through the Defence Advisory (DA) Notice system where editors unofficially seek advice on security matters before publishing (Creevy, 1999). While *The Guardian* did not seek such guidance before publishing its first story for fear of provoking an injunction (Purvis, 2014), British media largely complied with the DA notice issued by the British government as Snowden's leaks broke, barely covering the story, unlike the American and German press (Harding, 2014, p. 178; Moore, 2014; Rusbridger, 2013).

Research on the propagandising of the domestic press in liberal democracies by their own intelligence agencies finds journalistic collaboration with intelligence agencies as well as opposition to them. Collaborative journalistic practices include spreading intelligence-sourced, but disguised, propaganda (Lashmar, 2013; Olmsted, 2011); and providing uncritical reportage of intelligence agencies (Bakir, 2013). Systematic analysis of press coverage of Snowden's leaks shows the *International Herald Tribune* acting as apologists for US surveillance, and focusing on tangential issues (such as bilateral foreign relations) rather than addressing issues of surveillance over-reach (Goss, 2015). British press representation of the Snowden leaks privileges political sources seeking to justify and defend the security services. Prominent press themes are that social media companies should do more to fight terror, and that while surveillance of politicians is problematic, surveillance of the public should be increased. There is minimal discussion around human rights, privacy implications or regulation of the surveillance (Cable, 2015). Moving beyond content analyses of the press, journalists' own analysis of US mainstream press coverage of Snowden shows it supporting the Obama administration's War on Terror justification and vilifying Snowden. It also highlights two dominant narratives, both centered on Snowden's motives: treacherous spy and heroic whistle-blower (Epstein, 2014; Grey, 2013; Papandrea, 2014). Such narratives tally with Greenwald's description of press tropes on national security whistleblowers, these focusing on the person of the whistleblower rather than the leaks' substance and including tropes of madness, loners and losers.

As well as intelligence agency practices of secrecy and propaganda and the collaboration of journalists with intelligence agencies, the literature also documents oppositional journalistic practices of highlighting intelligence failures, demanding reform (de Vries, 2012) and exposing secret policies (Bakir, 2013; Murakami Wood & Wright, 2015). However, oppositional journalistic practices are far more rare than collaborative journalistic practices. As such, it is unsurprising

that Snowden sought very specific journalists for his leak—Poitras and Greenwald. Laura Poitras is a US filmmaker who had made critical documentaries about the post-"9/11" US national security state (Poitras, 2006, 2010). Greenwald has cultivated a reputation for independence as a national security political blogger and opinion writer since 2005 when, as a constitutional and civil rights lawyer, he blogged to more widely counter the Bush government's radical and extreme theories of executive power, extensively covering the 2005 story of NSA warrantless wire-tapping (Greenwald, 2014, p. 1). Snowden believed that Greenwald would understand the leaks' significance, and be able to withstand pressure to patriotically self-censor (Greenwald, 2014, p. 2; Harding 2014, p. 71). Certainly, Greenwald is publicly scathing of mainstream press reporting of politics (*Newsnight*, 2013), for instance, lambasting the *Washington Post* for "excessive closeness to the government, reverence for the institutions of the national security state, routine exclusion of dissenting voices" (Greenwald, 2014, p. 54). Although Greenwald took the leaks to *The Guardian*, a newspaper he had joined in August 2012 as an online daily columnist, attracted by its "history of aggressive and defiant reporting" (Greenwald, 2014, p. 67), he states that he retained complete editorial independence. In 2014, he started *The Intercept* where he and Poitras continue to report on Snowden's leaks. *The Intercept* belongs to First Look Media, founded in October 2013 by billionaire ethical investor and eBay founder, Pierre Omidyar. *The Intercept* is grounded in the principle that its journalists have absolute editorial freedom and independence (Rusbridger, 2013).

Thus, Intelligence Studies and Journalism Studies suggest, and the Snowden case study demonstrates, the continuing practice of a wide range of secrecy-maintaining techniques; and indicates journalistic promotion of the agenda of intelligence agencies and their political masters. These twin strategies of secrecy and propaganda challenge the press' accuracy and independence from the state, compromising its ability to act as a meaningful public oversight mechanism regarding intelligence agencies. Simultaneously, however, the Snowden case study also evidences the rare journalistic oppositional practice of exposing a secret intelligence policy, pointing to the continued relevance of the press in ensuring public oversight of the political-intelligence elite. It also highlights three conditions that foster effective press oversight. These comprise, firstly, international cooperation to enable journalists to avoid their own nation's censorship. For instance, fearing that its stories would be closed down in the UK by police seizing the data from *The Guardian*'s offices, *The Guardian* collaborated with *The New York Times*, exchanging its exclusive access to Snowden's documents for US First Amendment protection (Harding, 2014, pp. 186-189). The second condition for effective press oversight of intelligence agencies is political independence of press ownership, with voluminous and critical reporting coming from *The Guardian* (funded by the Scott Trust Limited, ensuring the newspaper's independence from commercial or political interference) and *The Intercept* (funded by a pro-transparency ethical investor). The third condition is the support of at least part of the mainstream national press. Greenwald (2015) explains that, before breaking Snowden's story, they considered avoiding mainstream press, but found themselves depending on the press' institutional resources. These comprised technical experts to secure the data; editorial experts to ensure robust stories; and financial resources and legal expertise as they had since spent millions of dollars on legal fees. As such, it is doubtful whether, had Snowden acted alone as a citizen, posting his data online, or if Greenwald had merely blogged about the story, that these acts of hierarchical sousveillance would have generated similar attention to the mass surveillance policy.

6. Discussion

Synthesising three normally separate fields of study—Surveillance Studies, Intelligence Studies and Journalism Studies—generates insights into the nature of contemporary state intelligence surveillance; the role of public oversight mechanisms in holding surveillant intelligence agencies to account; and how to resist such surveillance. These areas are thoroughly under-researched in all three fields. The Snowden case study provides conceptual tools and a framework for evaluating how contemporary state intelligence surveillance may be held to account and resisted, identifying areas for future productive research.

6.1. Conceptual Tools: The Veillant Panoptic Assemblage

Addressing Lyon's (2015) observation that Surveillance Studies ignores the technical infrastructure of global information flow and surveillance, lacks clarity on who is doing the surveillance, and lacks understanding of surveillance cultures, I introduce a new term: "*veillant panoptic assemblage*". This term aims to bring conceptual clarity to the complicated post-Snowden condition of mutual watching, while also highlighting resistive possibilities to surveillance. Retaining the words "panoptic" (with its centralizing, state-oriented, disciplinary functions) and "assemblage" (emphasizing the multi-site, fluctuating nature of data capture to form data-doubles), and bringing these together with "veillance" (highlighting that flows of watching are multidirectional involving citizens, retail and communications companies, and state agencies) accurately describes the contemporary condition of mutual watching. Given the various types of veillance possible (including not just

surveillance but also sousveillance, counterveillance, univeillance and equiveillance), this term also suggests that resistance to surveillance may be attempted in different ways, rather than focusing scholars' attention solely on surveillance.

6.2. A Framework for Evaluating Equiveillance

With the exception of NSA collection of US citizens' telephone metadata, the American and British review groups, reports and oversight boards into intelligence agencies' surveillance concluded that the mass surveillance programs are valuable and effective in protecting the nation's security and producing useful foreign intelligence. The state, then, refuses to give up its surveillance of digital communications, as it is too valuable. Accepting the inevitability of surveillance, Mann's goal is to move us towards a state of equiveillance, where there is equality between the forces of surveillance and sousveillance. However, can the *veillant panoptic assemblage* that describes post-Snowden society ever become an *equiveillant panoptic assemblage*? Further research into what would constitute an equal balance in power relationships between state and individual concerning surveillance would be valuable. For now, though, Mann and Ferenbok (2013, p. 30) suggest it would encompass power mechanisms to readily enact change from below, embracing innovations to the system, participatory projects, whistleblower protections and encouragement of genuine public debate. This final section evaluates the health of these civic and technological infrastructures in light of the Snowden case study.

In terms of innovations to the system, as well as technology industry campaigns for changes to surveillance and transparency laws and practices, several leading technology companies developed encryption technologies so that the state could not compel them to disclose people's communications. This form of univeillance blocks surveillance while encouraging citizens to communicate as they normally would (including practices of sousveillance). This has caused intelligence agencies much concern, as noted in public speeches and intelligence oversight reports, which express dire warnings about the internet "going dark" (ISC, 2015, p. 9; RUSI, 2015, p. 14). Indeed, given the centrality of commercial surveillance in the veillant panoptic assemblage, these univeillance-enabling actions, alongside trenchant lobbying by global telecommunications service providers for legislative change, are likely to be key drivers spurring governments to revise their surveillance laws and oversight of their intelligence agencies' surveillance powers. The struggle between corporations seeking to retain consumer trust in the privacy of their communications, and the state's secret demands for access, will no doubt continue to play out. Critical attention should be paid to ensuing privacy/surveillance rhetoric and arms races, and levels of trust in corporate and state surveillance practices.

Unlike innovations to the system, it is less clear how participatory projects have fared in enacting change from below. Certainly, the American and British review groups and oversight boards set up to study intelligence agencies' surveillance broadened their scope of consultation beyond official intelligence oversight bodies to include wider members of the legislature and civil society, especially NGOs and telecommunications companies. This is a good start, but what weight was given to concerns expressed by these broader voices, and which voices were most influential, would be worthy of systematic study. For instance, in the UK, JUSTICE, Liberty and Rights Watch UK told the ISC inquiry that they were against bulk collection of data in principle because of its 'chilling effect' on a free society, and that their opposition would remain even if such collection was proven to have averted terrorist acts and even if properly legally authorised (ISC, 2015, pp. 35-36). The ISC, however, simply took the opposite view: 'we do not subscribe to the point of view that it is acceptable to let some terrorist attacks happen in order to uphold the individual right to privacy—nor do we believe that the vast majority of the British public would' (ISC 2015, p. 36). By contrast, the more critical Anderson (2015) and RUSI (2015) reports take on board a number of the views expressed by NGOs, arguing, for instance, for legal limits on when and how communications may be intruded on, 'even if those limits from time to time diminish the effectiveness of law enforcement and result in more bad things happening than would otherwise be the case' (Anderson, 2015, p. 250). Whether their recommendations will be apparent in future British legislation remains to be seen.

The remaining civic and technological infrastructures for enacting change from below have fared less well. In terms of whistleblower protections, Snowden was not technically a whistleblower, as he did not follow national security whistleblower protocols (which would have entailed giving his information to an authorised member of Congress or Inspector General—a process that assumes that internal reform then ensues, but that Snowden had no faith in). As such, Snowden remains stranded in Russia and does not enjoy even the limited protections afforded to national security whistleblowers in the USA, despite initiating an international public and political debate that has led to re-evaluations of surveillance policy and intelligence oversight. What constitutes a national security whistleblower therefore needs re-examining, including, as Papandrea (2014) suggests, a re-writing of the Espionage Act [1917] to clearly distinguish between leaks intended to reach the enemy and those intended to inform the US public. However, rather than address this fundamental question, The President's Review Group on Intelligence and Communications Technologies (2013) merely recommends better and more continuous na-

tional security employee vetting to prevent leaks; and that the Civil Liberties and Privacy Protection Board should be an authorised recipient for whistle-blower concerns related to privacy and civil liberties from intelligence employees. As such, whistle-blowing to the press is discouraged, diverted, and remains a weak formal mechanism to enact change from below, particularly given multiple indictments of national security whistleblowers by Obama under the Espionage Act.

In terms of the final civic and technological infrastructure for enacting change from below—encouragement of a genuine public debate—this was certainly started by Snowden's revelations, spearheaded by *The Guardian* in the UK, and continued by *The Intercept,* among other press outlets. Yet, despite this stream of oppositional reporting, the focus of this debate in the wider American and British mainstream press is driven by politicians, and as such avoids issues of human rights and surveillance over-reach or regulation (Cable, 2015; Goss, 2015). As the previous section identifies, three conditions foster effective public oversight of intelligence agencies via the press, namely: international cooperation to enable journalists to avoid national censorship; political independence of press ownership; and support of at least part of the mainstream press and their institutional resources (financial, technical, editorial and legal expertise). Further research into these conditions would help us better understand how to increase oppositional journalistic practices (to the political-intelligence elite), rather than collaborative journalistic practices. Also in need of systematic research is what aspects of the public debate proved influential, particularly as the ISC invokes the will of the British public as erring on the side of bulk data collection to prevent terrorism. Indeed, the nine-nations study on the European public's attitudes towards security-oriented surveillance technologies finds that, notwithstanding national differences, few people are willing to give up privacy in favour of more security (Pavone et al., 2015, p. 133). Further research into why different nations' publics refuse this trade-off, and whether this is influenced by public discourses on surveillance and privacy, is needed. In terms of continuing the public debate, the governments' review groups and oversight boards agreed that technology companies should be allowed to be more transparent with their customers regarding government requests for citizens' data, and that more government documents regarding surveillance should be declassified to build public trust (ISC, 2015; TechNet, 2013; TPCLOB, 2014a). The extent to which such transparency calls are enacted, and the quality and meaningfulness of the information entering the public sphere from intelligence agencies and companies, requires monitoring, not least to ensure that partial declassification is not used to mislead the public, as found in the political publicisation of previous intelligence programs (Bakir, 2013).

To conclude, of the various civic and technological infrastructures for ensuring change from below, the strongest are innovations to the system, led by global telecommunications service providers; and participatory projects, involving global telecommunications service providers and NGOs. Far weaker are whistle-blower protections and genuine public debate. It appears, then, that the *veillant panoptic assemblage* is still a long way from achieving equiveillance.

Acknowledgments

This article was conceived thanks to multiple seminar contributions supported by the Economic and Social Research Council (ESRC) Seminar Series (2014-16), *DATA - PSST! Debating & Assessing Transparency Arrangements: Privacy, Security, Surveillance, Trust.* Grant Ref: ES/M00208X/1

Conflict of Interests

The author declares no conflict of interests.

References

Anderson, D. (2015). *A question of trust: Report of the investigatory powers review*. OGL. Retrieved from https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. Kansas: University of Kansas Press.

Bakir, V. (2010). *Sousveillance, media and strategic political communication: Iraq, USA, UK.* New York: Continuum.

Bakir, V. (2013). *Torture, intelligence and sousveillance in the war on terror: Agenda–building struggles*. Farnham: Ashgate.

Bentham, J. (1791). *Panopticon.* Dublin: T.Payne.

Bewley-Taylor, D. (2008). Crack in the lens: Hollywood, the CIA and the African-American response to the "Dark Alliance" series. *Intelligence and National Security*, *23*(1), 81-102.

Bigo, D. (2006). Security, exception, ban and surveillance. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 46-69). Oregon: Willan Publishing.

Boyce, G. (1978). The fourth estate: The reappraisal of a concept. In G. Boyce, J. Curran, & P. Wingate (Eds.), *Newspaper history: From the 17th century to the present day* (pp. 19-40). London: Constable.

Cable, J. (2015). The press, Snowden and mass surveillance. *DATA-PSST!* Retrieved from http://data-psst.blogspot.co.uk/search?updated-max=2015-07-05T08:51:00-07:00&max-results=7

Canadian Journalists for Free Expression. (2015).

Snowden surveillance archive. Retrieved from https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/about.html

Carlo, S. & Kamphuis, A. (2014). *Information security for journalists*. Centre for Investigative Journalism.

Church Committee. (1976). *Final report of the select committee to study governmental operations with respect to intelligence activities, United States Senate*. Washington: US Government Printing Office. Retrieved from https://archive.org/details/finalreportofsel01unit

Clapper, J. (2013). Official statement. *Welcome to IC on the Record*. Retrieved from http://icontherecord.tumblr.com/post/58838654347/welcome-to-ic-on-the-record

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498-512.

Creevy, M. (1999). A critical review of the Wilson government's handling of the D-notice affair 1967. *Intelligence and National Security*, *14*(3), 209-227.

Curran, J. (1978). The press as an agency of social control: An historical perspective. In G. Boyce, J. Curran, & P.Wingate (Eds.), *newspaper history: From the 17th century to the present day* (pp. 51-75). London: Constable.

de Vries, T. (2012). The 1967 Central Intelligence Agency scandal: Catalyst in a transforming relationship between state and people. *Journal of American History, 98*(4), 1075-1092.

Dee J. (1989). Legal confrontations between press, ex-CIA agents and the government. *Journalism & Mass Communication Quarterly*, *66*(2), 418-426.

Deleuze, G. (1992). Postscript on the societies of control. *October*, *59*, 3-7.

Deleuze, G. (1995). *Negotiations*. New York: Columbia University Press.

Director of National Intelligence. (2013). Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act. Retrieved from http://icontherecord.tumblr.com/tagged/fact sheet

Emmerson, B. (2014) *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* (UN Doc A/69/397). Retrieved from http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf

Epstein, J. (2014, May 9). Was Snowden's Heist a foreign espionage operation? *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB10001424052702304831304579542402390653932

European Committee on Civil Liberties, Justice and Home Affairs. (2014). *On the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*. (2013/2188(INI)). Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//EN#top

FAS. (2015). CRS Legal Sidebar. USA FREEDOM Act reinstates expired USA PATRIOT Act provisions but limits bulk collection. *FAS. Congressional Research Service Reports on Intelligence and Related Topics*. Retrieved from www.fas.org/sgp/crs/intel/usaf-rein.pdf

Fernandez, L. A., & Huey, L. (2009). Editorial. Is resistance futile? Thoughts on resisting surveillance. *Surveillance & Society*, *6*(3), 198-202.

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

GCHQ. (n.d.). How does an analyst catch a terrorist? *GCHQ*. Crown Copyright. Retrieved from http://www.gchq.gov.uk/what_we_do/how_does_an_analyst_catch_a_terrorist/Pages/index.aspx

Google. 2015. *Transparency report*. Retrieved from http://www.google.com/transparencyreport

Goss, B.M. (2015). The world is not enough. *Journalism Studies*, *16*(2), 243-258.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA and the US surveillance state*. New York: Metropolitan Books.

Greenwald, G. (2015). *Absolute control vs. the free press*. Paper presented at *Media Days*. Gothenburg, Sweden.

Grey, B. (2013, July 2). The US media and the case of Edward Snowden. *World Socialist Web Site.* Retrieved from http://www.wsws.org/en/articles/2013/07/02/snow-j02.html

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605-622.

Harding, L. (2014). *The Snowden files: The inside story of the world's most wanted man*. London: Guardian Books.

Hillebrand, C. (2012). The role of news media in intelligence oversight. *Intelligence and National Security*, *27*(5): 689-706.

ISC. (2013). Statement on GCHQ's alleged interception of communications under the US PRISM programme. (House of Commons). Retrieved from http://isc.independent.gov.uk

ISC. (2015). *Privacy and security: A modern and transparent legal framework*. (House of Commons). Retrieved from: http://isc.independent.gov.uk

Johnson, L. K. (2014). Intelligence shocks, media coverage, and congressional accountability, 1947–2012. *Journal of Intelligence History*, *13*(1), 1-21.

Klauser, F. R., & Albrechtslund, A. (2014). From self-tracking to smart urban infrastructures: Towards an interdisciplinary research agenda on Big Data. *Surveillance & Society*, *12*(2), 273-286.

Lashmar, P. (2013). Urinal or conduit? Institutional information flow between the UK intelligence ser-

vices and the news media. *Journalism*, *14*(8), 1-17.
Latour, B. (2005). *Reassembling the social. An introduction to actor-network-theory*. Oxford: OUP.
Lyon, D. (2003). *Surveillance after September 11*. Cambridge: Polity.
Lyon, D. (2014). Surveillance, Snowden, and big data: capacities, consequences, critique. *Big Data & Society*, *July–December*, 1-13.
Lyon, D. (2015). The Snowden stakes: challenges for understanding surveillance today. *Surveillance & Society*, *13*(2), 139-152.
Mann, S. (2004). "Sousveillance": Inverse surveillance in multimedia imaging. In *International Multimedia Conference: Proceedings of the 12th annual ACM international conference on Multimedia*, (pp. 620-627). ACM Press, New York. Retrieved from http://idtrail.org/content/view/135/42
Mann, S. (2013). *Veillance and reciprocal transparency: Surveillance versus sousveillance, AR Glass, Lifeglogging, and wearable computing*. Retrieved from http://wearcam.org/veillance/veillance.pdf
Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society*, *1*(3), 331-355.
Mann, S., & Ferenbok, J. (2013). New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society, 11*(1/2), 18-34.
Mathiesen, T. (1997). The viewer society: Michel Foucault's "panoptican" revisited. *Theoretical Criminology*, *1*(2), 215-234.
May, A. (2015). *Report of the interception of communications commissioner*. Interception of Communications Commissioner's Office. (HC 1113. SG/ 2015/28). OGL. Retrieved from http://www.iocco-uk.info/sections.asp?sectionID=1&type=top
McStay, A. (2014). *Privacy and philosophy: New media and affective protocol*. New York: Peter Lang.
Moore, M. (2014). RIP RIPA? Snowden, surveillance, and the inadequacies of our existing legal framework. *The Political Quarterly*, *85*(2), 125-132.
Murakami Wood, D., & Wright, S. (2015). Editorial: Before and after Snowden. *Surveillance & Society*, *13*(2), 132-138.
National Academies of Sciences. (2015). *Bulk collection of signals intelligence: Technical options*. Retrieved from http://www.nap.edu/download.php?record id=19414#
Newsnight. (2013, October 3). Glenn Greenwald trashes GCHQ/NSA apologists Kirsty Wark, Pauline Neville-Jones. *Newsnight* [Originally broadcast BBC2]. Retrieved from https://www.youtube.com/watch?v=-moGtQFvsVU
Olmsted, K. S. (2011). The truth is out there: Citizen sleuths from the Kennedy Assassination to the 9/11 truth movement. *Diplomatic History*, *35*(4), 671-693.
Papandrea, M. R. (2014). Leaker traitor whistleblower spy: National security leaks and the first amendment. *Boston University Law Review*, *94*(2), 449-544.
Parton, H. D. (2014, November 10). Mark Udall's perfect farewell. *Salon*. Retrieved from http://www.salon.com/2014/11/10/markudallsperfectfarewellhowhecangooutinablazeofglory
Pavone, V., Esposti, S. D., & Santiago, E. (2013). D2.2. *Draft report on key factors. Surprise.* Retrieved from http://surprise-project.eu
Pavone, V., Esposti, S. D., & Santiago, E. (2015). *D2.4—Key factors affecting public acceptance and acceptability of SOSTs. Surprise.* Retrieved from http://surprise-project.eu
Pew Internet Research Centre. (2014). Social networking fact sheet. *Pew Internet*. Retrieved from www.pewinternet.org/fact-sheets/social-networking-fact-sheet/
Poitras, L. (2006). *My Country, My Country*. Zeitgeist Films.
Poitras, L. (2010). *The Oath*. Zeitgeist Films.
Poitras, L. (2014). *Citizenfour*. Praxis Films, Participant Media, HBO Films.
Poster, M. (1997). *The second media age*. Cambridge: Polity Press
Privacy International. (2015). GCHQ-NSA intelligence sharing unlawful, says UK surveillance tribunal. *Privacy International*. Retrieved from https://www.privacyinternational.org/?q=node/482
Purvis, S. (2014). What are they so anxious to hide? *British Journalism Review*, *25*(2), 46-51.
Reform Government Surveillance coalition. (2014). *Global government surveillance reform*. Retrieved from https://www.reformgovernmentsurveillance.com
Rusbridger, A. (2013, November 21). The Snowden leaks and the public. *The New York Review of Books*. Retrieved from http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public
RUSI. (2015). *A Democratic licence to operate: Report of the independent surveillance review*. London: Royal United Services Institute for Defence and Security Studies.
Simcox, R. (2015). *Surveillance after Snowden: Effective espionage in an age of transparency*. London: The Henry Jackson Society.
Snowden, E. (2013a). Snowden: A manifesto for the truth. *Information Clearing House*. Retrieved from www.informationclearinghouse.info/article36733.htm
Snowden, E. (2013b, June 13). NSA whistleblower Edward Snowden. *The Guardian*. Retrieved from http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

TechNet. (2013). *Submission to the Privacy and Civil Liberties Oversight Board (PCLOB) notice. Hearings: Surveillance programs*. (Docket Number: PCLOB 2013-0005. October 24). Retrieved from http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0067

TPCLOB. (2014a). *Report on the Telephone records program conducted under section 215 of the USA PATRIOT ACT and on the operations of the foreign intelligence surveillance court*. (23 January). Retrieved from https://www.pclob.gov/events/2014/january23.html

TPCLOB. (2014b). *Report on the surveillance program operated pursuant to section 702 of the Foreign Intelligence Surveillance Act.* (2 July). Retrieved from https://www.pclob.gov/events/2014/july02.html

The President's Review Group on Intelligence and Communications Technologies. (2013). *Liberty and security in a changing world*. (12 December). Retrieved from http://icontherecord.tumblr.com/ppd-28/2015/seeking-independent-advice

Twitter. (2014). Guidelines for law enforcement. *Twitter.* Retrieved from https://support.twitter.com/articles/41949-guidelines-for-law-enforcement#10

Twitter. (2015). Transparency report. *Twitter.* Retrieved from https://transparency.twitter.com

United Nations. (2014). *The right to privacy in the digital age.* United Nations. Retrieved from http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

USA Freedom Act [2015] H.R.3361. Retrieved from https://www.congress.gov/bill/113th-congress/house-bill/3361

Yahoo. (2015). Transparency report. *Yahoo*. Retrieved from https://transparency.yahoo.com

Yin, R. K. (2013). *Case study research: Design and methods*. London: Sage.

About the Author

Dr. Vian Bakir

Vian Bakir is Reader in Journalism and Media at Bangor University, Wales, UK. She is author of *Torture, Intelligence and Sousveillance in the War on Terror: Agenda-Building Struggles* (2013) and *Sousveillance, Media and Strategic Political Communication: Iraq, USA, UK* (2010). She is Principal Investigator on Economic and Social Research Council Seminar Series (2014−16), *DATA - PSST! Debating & Assessing Transparency Arrangements: Privacy, Security, Surveillance, Trust.*