Surveillance & Society

Article

The Snowden Stakes: Challenges for Understanding Surveillance Today

David Lyon

The Surveillance Studies Centre, Queen's University, Canada.
lyond@queensu.ca

Abstract

The drip-feed disclosures about state surveillance following Edward Snowden's dramatic departure from his NSA contractor, Booz Allen, carrying over one million revealing files, angered some and prompted some serious heart-searching in others. One of the challenges is to those who engage in Surveillance Studies. Three kinds of issues present themselves: One, research disregard: responses to the revelations show a surprising lack of understanding of the complex, large-scale, multi-faceted panoply of surveillance that has been constructed over the past 40 years or so that includes but is far from exhausted by state surveillance itself. Two, research deficits: we find that a number of crucial areas require much more research. These include the role of physical conduits including fibre-optic cables within circuits or power, of global networks of security and intelligence professionals, and of the minutiae of everyday social media practices. Three, research direction: the kinds of surveillance that have developed over several decades are heavily dependent on the digital—and, increasingly, on so-called Big Data—but also extend beyond it. However, if there is a key issue raised by the Snowden revelations, it is the future of the internet. Information and its central conduits have become an unprecedented arena of political struggle, centred on surveillance and privacy. And those concepts themselves require rethinking.

Introduction

> "*Nineteen-Eighty-Four* is an important book but we should not bind ourselves to the limits of the author's imagination. Time has shown that the world is much more unpredictable and dangerous than that."
>
> Edward Snowden, July 2014.[1]

The disclosures about mass surveillance, provided by Edward Snowden, offer extensive insights into the inner workings of National Security Agency (NSA). One of the first things that featured in news accounts was that so-called mass surveillance is carried out on 'US persons' as well as foreigners and that those 'foreigners' may include close allies. While some details are tantalizingly patchy, for the most part the sheer volume of files and the range of areas to which they refer are nothing short of mind boggling. And although the drip-feed disclosures began in June 2013, they continue to be released, with the result that any commentary is open to further modification.

Moreover, the impact of Snowden's whistleblowing leaks is now being felt more profoundly at a national policy level, in 2015, in more than one context. First, the US Freedom Act, passed on June 2, 2015, restored in modified form some aspects of the post-9/11 Patriot Act but crucially, restricts the bulk

[1] http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript/.

Lyon, D. 2015. The Snowden Stakes: Challenges for Understanding Surveillance Today. *Surveillance & Society* 13(2): 139-152. http://www.surveillance-and-society.org | ISSN: 1477-7487

collection of telephone metadata of American citizens. Second, on June 11, a major government-commissioned report on counter-terrorism measures, *A Question of Trust*, by David Anderson, called for curbs on the UK's GCHQ. In particular, it is highly critical of the existing system of oversight of intelligence agencies. Neither of these would have been possible without Snowden.

Both what may be learned from the disclosed documents and what may be seen of their direct impacts provide the basis for some serious re-thinking of some assumptions about surveillance in the 21st century. To take one prominent example, the very term 'surveillance' may require some new qualification. What is known about NSA practices raises questions about the supposed clear distinction between 'mass' and 'targeted' surveillance, and the wholesale use of 'metadata' foregrounds long-standing debates about how to define 'personal data' (or 'personally identifiable information'). What goes for the 'subject' of surveillance applies to 'privacy' as well. Each requires some serious rethinking.

On these questions, themselves seen as controversial by defenders of the NSA's practices, there is little settled opinion as yet. If data are sought on a 'mass' basis, from wide swathes of a given population, with a view to identifying algorithmically through correlations who might be a 'person of interest,' the point at which 'mass' becomes 'targeted' surveillance is at best an indeterminate threshold. And if the kind of data obtained in the first instance are in fact metadata—such as IP address, duration of call, which friends were contacted?—then they comprise just the kinds of information that a private detective might seek: who spoke to whom, when, and for how long? Despite protestations to the contrary, it is hard to deny that such metadata are highly 'personal,' especially now that the US Freedom Act explicitly limits such collection.

That the activities of the NSA and its sister agencies around the world are controversial is made abundantly clear by government efforts in more than one country to use the term 'bulk collection' of data rather than 'mass surveillance.'[2] In a case in 2000, the European Court of Human Rights concluded that even the storing of data relating to the "private life" of an individual falls within the application of Article 8.1 of the European Convention on Human Rights (Bowden cited by Greenwald 2015). But the debates over this are fierce in countries such as the UK and US. This article argues that gathering and analyzing metadata, including content of communications, is best thought of as 'mass' surveillance, even though, as noted above, locating 'suspects' is still the main aim.

Surveillance Studies, the multi-disciplinary field of research dedicated to understanding in context contemporary practices such as monitoring, tracking and identification, is well positioned to respond to the new challenges raised by the Snowden files. However, the case made here is that, while some challenges are direct ones, to our grasp of substantive aspects of surveillance processes, others are indirect. While no claim is made about the exhaustiveness of the analysis that follows, it does suggest that Surveillance Studies can make significant contributions to considering each kind of challenge.

Snowden's own comments about Orwell point in this direction, too. Given that, for many people, the spectre of Big Brother is still the one that fuels the imagination regarding mass surveillance, there is a need to place Orwell's dystopic and cautionary tale in context. For Snowden, this is primarily a technological matter; "quaint" microphones hidden in bushes and the telescreen that can observe us have given way to mobile webcams and network microphones in cell-phones. But while Orwell cannot be blamed for not foreseeing the consequences of the so-called information revolution, it is also worth recalling that, like Max Weber or Hannah Arendt,[3] Orwell saw surveillance as in part an outcome of a

[2] In May 2015 the US Court of Appeals ruled that the collection of bulk phone metadata by the NSA never was legal.

[3] Weber and Arendt have much to say about what is now known as surveillance, in relation to maintaining bureaucratic records on individuals (Weber) or how power is generated in "spaces of appearance" (Arendt). See e.g. Dandeker 1990; Marquez 2012.

relentless rationality expressed in bureaucratic procedures. That constraining cultural condition undoubtedly helps to explain why surveillance is in one sense self-augmenting. But more than that is needed to indicate in particular what difference is made by the digital.

Snowden's conviction is that due to surveillance, today's "…world is much more unpredictable and dangerous" than Orwell could have guessed. This too represents a genuine challenge from Snowden, not only to upgrade our grasp of new technology, but also place any and all technological systems in their social, political-economic and cultural context. The use of metadata, for example, is no mere outcome of technological potential, such as the exponential expansion of storage power, but of specific approaches to risk management in security industries and of consumer clustering in marketing, each of which has risen to prominence in contexts where globalization—understood as neo-liberalism—holds sway.

In what follows, three kinds of challenge are identified and discussed. The first, 'research disregard,' is in a sense historical: why the shocked and outraged responses to Snowden's revelations as if this is the first we have heard of very large scale surveillance in the early 21st or even late 20th century? The second has more to do with substantive and current challenges emerging from the revelations themselves; I label it 'research deficit.' I indicate some areas that require some serious reappraisal in our understanding of surveillance today. The third, 'research direction,' points rather to the future, suggesting that the larger context of the Snowden revelations is the fate of the internet. Surveillance should never be thought of as a discrete dimension of the modern world. Today, it cannot be understood without investigating information and its current conduit, the internet. In a coda, I return to the issues of how to rethink 'surveillance' and 'privacy' for today.

These, then, are the Snowden stakes. The revelations have rightly remained buoyant in the headlines, just because so much is "at stake," not merely for Surveillance Studies or the future of the internet, but more significantly, for privacy, human rights, civil liberties, freedom and justice.

Research disregard

The Snowden revelations continue to make headline news and several major diplomatic events have been sparked by them. Angela Merkel, Germany's Chancellor and Dilma Roussef, the Brazilian president, for example, say they were shocked to discover that their cell-phone conversations had been monitored.[4] As well, individual populations outside the US have reacted negatively on finding that the NSA has been active in unexpected ways within their national territory. In Canada, for example, it was disclosed that the NSA had set up shop in the capital, Ottawa, in order to monitor the G8, G20 summit in June 2010 (Weston, Greenwald and Gallagher 2013).

Broadly speaking, at least three elements of surveillance practices became strikingly evident during 2013 and since. One, governments engage in mass surveillance on their own citizens. The NSA works closely with the 'Five Eyes' of Australia, Canada, New Zealand and the UK but their activities are also mirrored in many other countries. Two, corporations share their 'own' data supplies with government, to mutual benefit. This happens as internet companies in particular, knowingly or not, collude with government to provide personal data. Three, ordinary citizens also participate through their online interactions—especially in social media—and cell-phone use. Without necessarily being aware of it, we all feed data to the NSA and its cognate agencies, just by contacting others electronically (Lyon 2013).

[4] It is symptomatic of today's celebrity culture, of course, that surveillance of high-profile public figures garners much more mass media interest than the mass surveillance of ordinary—in this case German—citizens. At the same time, it is not only the NSA that spies on others' leaders: Germany has also kept tabs on prominent Americans such as John Kerry and Hillary Clinton. See http://www.theguardian.com/world/2014/aug/16/germany-spied-john-kerry-hillary-clinton-der-spiegel/.

However huge the revelations, though, it has to be said that there was little that was completely new about the three surveillance elements mentioned here. Granted, the massive import of the Snowden disclosures lay in the substantial store of clear evidence pointing to the present and ongoing reality of mass surveillance and this was undoubtedly new. When the news first broke in *The Guardian* on June 5 2013, several factors were startling. Verizon, the telecom giant, was required by the NSA to give information on all calls within the USA and between the USA and other countries between April and July that year. Secret domestic spying on an astounding scale was happening under President Obama (Greenwald 2013). But the international outcry against the realities of mass surveillance now revealed gave the impression that citizens were quite unaware and unprepared for what they now were hearing.

This suggests that surveillance was not really on the radar of most ordinary citizens. But still, to those engaged in examining surveillance and in proposing legal, technical and policy responses, the sense of unawareness may have come as something of a disappointment; it is easy to over-estimate the reception of our own work. Also, most responses worry about the assault on privacy, construed as a personal—understood as individual—matter, which shows little understanding of the ways that surveillance also operates as social sorting, targeting primarily population groups before individuals, or of how privacy speaks to these questions of human rights and social justice as well. The main exception to the individualizing focus on privacy is among those whose concern is that communications privacy has been egregiously violated, which prompts weighty questions about trust in particular.

The popular and media debate over Snowden has focused all-too-frequently on state surveillance primarily as a threat to individuals, except where the challenge to a free and open internet has been recognized. Yet the evidence shows that arbitrary power is used against all citizens when mass surveillance is practiced. As a number of advocates have argued for some time (Regan 1995; Bennett and Raab 2006; Steeves 2009), privacy is not only an individual matter. Surveillance and privacy can each be considered along a spectrum of relationships, from the monad to the multitude. By definition, mass surveillance means that anyone and everyone can be caught in the surveillance net and the larger the scale of surveillance, the more likely it is that false positives will emerge in the quest for 'persons of interest.' These questions are pursued below.

Despite two decades of growth in Surveillance Studies there seems to be little public understanding of surveillance as it is practiced today. The sorts of practices uncovered by Snowden are ones that have a long history, not only in the annals of intelligence gathering and national security agencies, but in spheres from policing to public administration to consumer marketing. This should be salutary for those engaged in the academic study of surveillance and indeed for any who care about freedom, democracy and justice in the 21st century (for a no-holds-barred critique see Giroux 2014). It is worth briefly reviewing that development.

In the 1980s those interested in the study of surveillance were concerned primarily with state surveillance on the one hand (e.g. Burnham 1983; Campbell and Connor 1986) and workplace surveillance on the other (e.g. Webster and Robins 1986; Zuboff 1988). More broadly, surveillance in the service of 'social control' was discussed in relation to policing and the management of offenders (e.g. Cohen 1985; Marx 1988), and this dimension was already merging, in part with questions of 'national security.' However, research on consumer surveillance—and its links with systems of public administration—were also available at this time (see the pioneering work of Rule 1974) but consumer surveillance would not be recognized as part of mainstream surveillance developments until the 1990s (see, prominently, Gandy 1993). Without exception, these authors stressed the impact of computerization on the ways that these existing forms of surveillance, including public video cameras, would develop.

By the 1990s, however, the term 'surveillance society' was in much more general use as a term that indicated the ways that what once seemed to be restricted to the activities of government, policing or employment was spilling over into everyday life (Lyon 2001). This term in no way minimized the importance of state surveillance but did indicate that systemic surveillance of many kinds could be expected simply as a result of conducting one's daily affairs. Increasingly, surveillance became visible through ubiquitous cameras in public streets and locations such as shopping malls, the use of credit cards and, progressively, loyalty cards, plus, in some rudimentary ways, through online interactions that expanded after the development of the World Wide Web in 1994 and the subsequent commercialization of the internet, from 1995.

During the early 2000s, two events occurred that were to shape the direction of surveillance decisively, although the potential connections between them were not made public until 2010. One was the attacks of September 2001 ('9/11'), and also the London bombings of '7/7', and the Madrid train attack, the aftermath of which hugely boosted security-related surveillance at least in the global north. Interestingly, the activities of the quickly-formed Department of Homeland Security took some cues from 'Customer Relationship Management' (CRM) in their quest for 'Total Information Awareness (TIA)' (Lyon 2003: 92f). The other was the definitive appearance of social media, symbolized by the invention of Facebook in 2004, that quickly established itself as a mainstream dimension of the internet, simultaneously facilitating new levels of consumer surveillance (not to mention social surveillance, Marwick 2012; Trottier 2012), now based on self-expressed preferences and tastes. By President Obama's inauguration in 2009 the DHS had developed a Social Networking Monitoring Center to check for 'items of interest' (Lynch 2010).

In a sense, then, the Snowden disclosures may be functioning as a wake-up call to publics still unaware that the day of mass surveillance of ordinary citizens had already dawned. If it was not already clear, after 9/11 the 'national security' rationale for intensified surveillance (Ball and Webster 2003) became prominent and with it the use of data analytics (now generally referred to as 'Big Data,' Lyon 2014a). The TIA was dependent on a very large-scale database using "new algorithms for mining, combining and refining data"[5] that included bank machine use, credit card trails, internet cookies, medical files—anything, indeed, that might produce interesting correlations that might indicate meaningful relationships between records. These, the Snowden files show, are among just the methods used by the NSA in its surveillance both domestic and foreign.

Without doubt, Snowden is right to raise issues of privacy, civil liberties—including freedom of expression, communication and assembly—and human rights in relation to what his findings have exposed about the NSA and its cognate agencies around the world. But what many studies of surveillance over the past two decades have shown is that deeper questions are raised that challenge many conventional assumptions about contemporary societies, their actual forms of power, their politics and their democratic institutions and processes. As the above analysis shows, this is not only a question of electronically-enhanced bureaucratic power bearing down upon hapless citizens. It also has to do with how those citizens engage with the everyday, in communication, interaction and exchange, much of which occurs using digital devices. Arguably, then, it is also a matter of a surveillance culture (Lyon 2014b) in which an increasing proportion of the world's population lives and to which, for a number of reasons, many have become inured.

As well as the more fundamental societal-cultural questions raised by the Snowden findings, the key issues of contemporary surveillance may also be discerned through considering some major trends that have become increasingly evident in the past decade or so (and in the following section, we explore how some of these intersect with three central Snowden-specific questions). In addition to the sheer

[5] www.darpa.mil/iao/TIAsystems.htm/.

exponential growth of surveillance, as it has increasingly become a basic mode of organizational practice, several other significant trends may be identified (for more on this, see Bennett et al. 2014; Brown 2010).

As mentioned earlier, security is becoming a key driver of surveillance, not only at the 'national' level but also in general types of policing, urban security and in workplaces, transit systems and schools (Taylor 2013). This is of course, a key issue and one fraught with basic problems of definition, which also relates to its status as a widely-used political rationale for a range of controversial measures. The kind of 'national security' that prompts increased surveillance arguably has little in common with the kinds of 'security'—from things like famine, fear, even freedom—that many might think would benefit their communities and families. Moreover, in practice, many current attempts to procure national security seem to jeopardize the civil liberties and human rights basic to democratic practice (see Zedner 2009).

At the same time, it must be acknowledged that not only 'security' but also some much more mundane motifs are significant in the development of surveillance today. One is 'efficiency,' that encourages the use of cost-cutting policies and technology-intensive solutions and the other is 'convenience' that dominates much of the appeal of marketers to consumers. Under such very ordinary and unremarkable motifs surveillance expands apace, as evidence-producing technologies (as Josh Lauer calls them) are adopted for reasons that are routine and everyday.

'Security,' on the other hand, is still supreme among these 'drivers.' For philosopher Giorgio Agamben, the security motif seen behind contemporary surveillance may be trumping not only democracy but politics itself (Agamben 2013) and this insight may at least serve as a theorem to be explored. At the same time, this trend must be seen alongside another, the intertwining—and in some respects integration—of public and private agencies. The governmental and the corporate have always worked closely together in modern times but the idea that they inhabit essentially different spheres, with different mandates, is currently unraveling. As Snowden revealed, telephone companies such as Verizon and internet companies such as Microsoft work in tandem with state agencies such as the NSA, in ways that have yet to be fully understood.

Several other important trends also deserve mention, if only to flag their significance (they are discussed in Bennett et al. 2014). Mobile and location-based surveillance is expanding, which means that the time-and-space coordinates of our lives are increasingly monitored. Surveillance is more and more embedded in everyday environments such as buildings, vehicles and homes. Machines recognize individual owners and users through card-swiping or voice-activation. The human body is itself the source of surveillance data, with DNA records, fingerprinting, facial recognition coming to be viewed as reliable means of identification and verification. Moreover, all these trends are rapidly being globalized, which is in itself a surveillance trend of some import. As mentioned above, social surveillance via networking sites is rising, a topic we return to below. And in all this, it becomes steadily more difficult to know what exactly counts as 'personal data.' Vehicle licence plates, presence in group photos posted on social media and of course metadata make definition difficult.

All the above stand as challenges to Surveillance Studies in particular, and to any and all citizens of contemporary liberal democracies in general. There are, however, some more specific questions to which I now draw attention. These are areas in which, after Snowden, we are obliged to say that current surveillance research simply does not yet know enough.

Research deficit

If the historical problem is the apparent disregard of research about surveillance, permitting a sense of surprise rather than sober expectation, then the contemporary problem is that current research has yet to catch up with some vital surveillance developments. In each case—digital infrastructures, professional

networks and social media practices—the difficulty of identifying the object of research is compounded by misleading language, dubious assumptions and inadequate theory. There is no conspiracy here, just an analytic fog that has to clear before the contours of each situation can be seen more sharply.

The first issue is one that may be most dramatically seen in relation to cloud computing (fog again?) and the electronic transfer of data from place to place. The metaphor of the cloud originated in diagrams intended to demonstrate how information is moved around (Mosco 2014: 77). The impression given—and reinforced through cloud marketing—is that somehow data flits weightlessly through the ether when in fact the actual conduits are fibre-optic cables. There is a geographical and material element to the cloud that belies the benign, fluffy, floating image. That material-geographic element is crucial to power configurations. Part of this has to do with the leading role of the US, through the NSA. As Andrew Clement shows, data files sent from the University of Toronto to the Ontario government (a few city blocks away, also in Toronto) actually travel down fibre-optic cables in a "boomerang" pattern to US data-handling interchanges before reaching their destination back in Canada (Clement 2013). They thus travel though a quite different data regime than Canada's. But new power configurations are also generated by the capacity to tap into digital data, which depends on cooperation between participating countries in order to obtain general views of the operation of the internet.

NSA programs use such cables to collect (Upstream, Quantuminsert—see also commercial versions of such hacking programs[6]) and to intercept (Tempora) data. Interceptors are placed strategically along the cable routes, a practice undertaken by many countries, as Snowden's work shows, and through Global Crossing security agreements with private companies much of the world's fibre optic cable is accessible to the US (Timberg and Nakashima 2013). More targeted surveillance occurs using systems like XKeyscore, which is linked to the PRISM program. XKeyscore also stores material in data caches spread around the world in specific locations (see map in Bennett et al. 2014: 113). PRISM, in turn, depends on consumer data obtained from internet companies through social media and cloud platforms (such as Dropbox; see Bauman et al. 2014: 123).

The second issue is that it is hard to pin down exactly who is conducting surveillance. Although the term 'state' surveillance is common in everyday parlance, those who stand in for 'state' employees are many and varied, and this follows from the point above about the blurring between public and private sectors. Snowden's own position before his departure with the documents illustrates this. He worked for Booz Allen Hamilton, whose expertise was subcontracted to the NSA. Didier Bigo (e.g. 2008; see also Ball and Snider 2013; Bauman et al. 2014: 124-131; Lyon and Topak 2013) has for some time drawn attention to the ways in which "security professionals" now form an international network, operating in different countries but with extensive cooperation. These are intelligence agents, technical experts, police (both public and private), advisers and others whose immediate genesis lies in post-9/11 international anti-terrorism cooperation but has now expanded into a clearly discernible network of some considerable influence.

Importantly, older distinctions break down as this network of "unease managers" (as Bigo calls them) develops. They connect public and private agencies, internal and external security, national and international interests and so on. This development grows alongside the digitization of security and surveillance such that, paradoxically, 'national' security is no longer 'national' in "…its acquisition or even analysis, of data…" which helps to blur "…the lines of what is national as well as the boundaries between law enforcement and intelligence" (Bauman et al. 2014: 125). This issue is related to the one mentioned above, about the uncertainty of who actually carries out surveillance, although the further point here is that a loose affiliation of professional organizations can be identified. They work together, learning from each other and developing their own protocols, rationales and surveillance practices.

[6] https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text/.

As the examples from the US show, similar surveillance practices occur across the board, whether in the DHS, CIA, FBI or the NSA (or, for that matter, in the UK's GCHQ or Canada's CSEC). These 'acronym' policing and intelligence organizations also rely on similar subcontracting organizations that also display similar technical, statistical and political-economic activities (see Ball and Snider 2013). Both policing and intelligence agencies have military connections that also influence their practices and as well the traffic is two way: information handling is crucial to each, such that policing becomes more data-heavy (Haggerty and Ericson 1997) and also more inflected by military method (Brodeur 2010). In all cases it is also clear that such organizations do not just react to perceived threats to national security or to criminal acts. They actively construct the target populations and refine the rationales for so-doing. This is where the commercial connections with technology corporations also become centrally significant, in conjunction with government actors. Policy influences and is influenced by the corporate and technical approaches and practices. At an organizational and network level, then, relationships are manifold and complex.

The third 'research deficit' question has to do with the tissues connecting these organizational networks and their practices with the subjects of surveillance or, more properly, with target populations. The internet, and above all social media, are crucial here, although cell-phone use is another linked dimension of the same question. It is important to recall that social media is a 21st century phenomenon of only very recent provenance. Yet it has grown at an astonishing speed and with amazing global reach such that it is now one of the dominant aspects of internet use. While much significant social research has occurred in this area—particularly with the help of units such as the Oxford Internet Institute in the UK or the Pew 'Internet and American Life' program—understanding how social media users operate in relation to practices and concepts relating to surveillance and privacy is still very much an infant subfield and a vital research priority (see, e.g. Fuchs 2014; Marwick 2013; Trottier 2012).

In a longer historical frame, it might seem strange that social media users would freely permit personal details to be widely and promiscuously circulated online, thus making them vulnerable to intense surveillance both by the corporations that seek their data for marketing purposes and by policing and intelligence agencies. Such willing compliance would surely have puzzled and bothered an Orwell, attuned as he was to the use of new technologies to procure popular subservience to the state. But there is a strong sense in which today's situation is decidedly post-Orwellian. Not merely that the technologies of surveillance have been hugely upgraded, but that surveillance practices are common to all organizations, which amounts to surveillance "regimes" (Giroux 2014: 7) and as I noted above, a surveillance culture. In such a culture, surveillance is not only a form of entertainment but also something encountered in everyday life and in which many knowingly and actively engage themselves. Lives are lived, in part, online.

The research question that presents itself here is what long-term impact the Snowden revelations and their aftermath will have in informing and perhaps reorienting the practices of social media users. This involves careful analysis of how users themselves perceive the situations in which they find themselves and the practices they pursue online. For instance, Pew researchers found that social media users are unwilling to discuss Snowden online—*and offline too*—preferring safer environments such as the dinner table for such conversations.[7] As well this is a challenge for policy and advocacy research that is willing to go beyond conventional understandings of surveillance and, especially, privacy (see e.g. Cohen 2012).

This also involves fresh investigations of the potential of internet communication for questioning and resistance to forms of surveillance deemed excessive, unnecessary, or illegal. One the one hand, numerous internet-related NGOs and lobby and pressure groups have formed a disparate social movement to demand

[7] http://techcrunch.com/2014/08/26/social-media-is-silencing-personal-opinion-even-in-the-offline-world/.

accountability for, and transparency about, the surveillance practices exposed by Snowden.[8] On the other, everyday engagement of users with social media may be reflexively informed by growing knowledge of how surveillance works in the world after Snowden. Concepts such as "exposure" (Ball 2009) find new critical import for understanding how, how much, and under what circumstances users reveal personal data to others.

These questions lead into a more general inquiry about the future of internet-related surveillance research, which, I argue in the next section, has risen in significance to stand today as a key area—in the sense that it informs many other areas—in surveillance research.

Research direction

> Internet freedom—the ability to use the network without institutional constraints, social or state control, and pervasive fear—is central to the fulfillment of [its] promise. Converting the internet into a system of surveillance thus guts it of its core potential.
>
> (Glenn Greenwald 2014: 6)

Any field of study, including that of surveillance, is obliged to review from time-to-time the main force-fields that shape the object of analysis. Today the internet is bound up with surveillance at many levels and thus deserves special attention. This section argues that the research direction for Surveillance Studies should be strongly inflected by issues of information and the internet. The kinds of surveillance that have developed over several decades are heavily dependent on the digital—and, increasingly, on what is now labelled Big Data—but also extend beyond it. As Greenwald indicates, the Snowden revelations raise as a key issue the future of the internet. While it is true that modern societies have been 'information societies'—and thus 'surveillance societies'—from their inception (Lyon 2005), today information and its central conduits have become an unprecedented arena of political struggle, centred on surveillance. This suggests that both analytically, in terms of research directions, and politically, in terms of practice and policy, the internet and surveillance are bound in a mutually-informing relation.

The use of internet for surveillance is not new but its scope has never been greater. For many, such as Greenwald and Snowden himself, this is a great betrayal of the initial wave of optimism about its democratic potential with which the internet was born. The hoped-for human benefit pre-dated the commercialization of the internet but versions of it were also woven-into many corporate aspirations in Silicon Valley and elsewhere from the 1990s onwards. Some popular and prescient writers such as Ithiel de Sola Pool (1983) foresaw the development of what we now call the internet, arguing that it was a key carrier of technological freedom. He insisted that free speech would become a vital issue. How regulation and access were organized would determine whether or not the new communications would enhance democracy as the political platform and the printing press had done before.

What happened to those utopian dreams of the 'information revolution' pundits of the 1980s? After all, they had correctly noted the emancipatory and democratizing possibilities offered by the new technologies. But Ithiel de Sola Pool and others of his ilk perhaps paid insufficient attention to the already-existing political economy *informing* information technologies—not to mention the over-arching cultural belief in the power of Technology. Together, they led to a failure to note that the new technologies might be deemed efficacious despite evidence to the contrary, and to see the flaws in the analysis that sees knowledge as a new and independent factor of production. Following Karl Polanyi

[8] Coalitions against mass surveillance have engaged in several concerted global events since Snowden's disclosures began. See e.g. https://blog.wikimedia.org/2014/06/05/global-action-against-mass-surveillance-snowden-revelations/. The 'transparency' question, however, is in tension with the legitimate but limited need for secrecy within intelligence agencies. Research could fruitfully be brought to bear on this vexed question.

(1944, 2001), one might think of informational knowledge as in fact a 'fictitious commodity' that has been cut off from its social origins in creative labour as an 'independent' form in expert systems or virtual services (Hayles 1999), integrated into an economic system of general commodification where profit is the bottom line, and is allocated through the market, where reciprocity or social justice have little or no say (Jessop 2007; also Schiller 1988). The commodification of the internet in 1995 was a critical moment in the more general development of information as a fictitious commodity.

However, De Sola Pool's thirty-year-old comments on freedom of speech came home dramatically as documents were released by Snowden. By this time matters had become polarized. Right on the heels of the news about the NSA's access to Verizon telephone subscriber data came the disclosures about the PRISM program that directly implicated major internet companies such as Microsoft, Yahoo*!*, Google and Facebook. Urgent exchanges occurred, some of which involved some puzzlement on the part of the companies: yes, they had parted with some data but the revelations seemed to suggest that far greater quantities were involved than they had themselves authorized. As it transpired, beyond the FISA-authorized access to data held by internet companies, the NSA had also found ways to intercept upstream in the data flow, using systems such as Muscular, developed by the NSA along with Five Eyes partner the UK GCHQ (Gellman and Soltani 2013).

As Steven Levy noted in a *Wired* article (Levy 2014), the Snowden 'revelations' exposed a "…seemingly irresolvable conflict. While Silicon Valley must be transparent in many regards, spy agencies operate under a cloak of obfuscation."

Snowden's findings shone a spotlight on an issue of which internet companies had been all too aware for some years. Companies such as Google, Yahoo*!* and Twitter had struggled to hold off government attempts, through the Foreign Intelligence Surveillance Act (FISA) court, to oblige them to hand over customer data. To their credit, the companies seemed to have tried to ward off such efforts[9] but the combination of government power and the fact that the companies also have government contracts compromised the struggle somewhat. PRISM focused the fight, but the secrecy surrounding the NSA has made it very difficult to know exactly what is happening. They are fighting in a fog. This also presents problems for those trying to research corporate-government surveillance relations.

The details of the ongoing controversies and battles may be found on various sites[10] but the theme that unites them is surveillance and the future of the internet. This has several implications for analysis and action.

One important outcome is that those studying surveillance have come to realize that those researching communications have much to offer. From Oscar Gandy's or Joseph Turow's pioneering work in consumer surveillance to Mark Andrejevic's or Alice Marwick's explorations of online surveillance (Gandy 1993, 2012; Turow 2012; Andrejevic 2007, 2013; Marwick 2013), not to mention ongoing work on communications surveillance itself, the connections are clear. Those whose surveillance background is in criminology or public policy in particular may need to strengthen their analyses by examining more closely how the internet intersects with their understanding of surveillance. Equally, those grappling with questions about internet surveillance would do well to look at the literatures of surveillance—and of privacy—more broadly conceived (e.g. Raab and Goold 2011).

---

[9] Centre for Democracy and Technology, September 2014: 'Yahoo v. U.S. PRISM documents,' available at https://cdt.org/insight/yahoo-v-u-s-prism-documents/.

[10] See e.g. http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html/ or http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline/.

A second area is to explore further the analytical possibilities for considering information as a fictitious commodity. One could argue, for example, with the strong push towards so-called Big Data, that the severing of connections between information and its social roots is now even more pronounced. In N. Katherine Hayles' analysis, information "loses its body" dating from the time of the 1950s Macey Conferences on communication theory onward. But I would argue that now so-called personal data progressively loses its 'person' (Lyon 2014a). When data gathered for commercial (marketing) purposes—which already stretch the links between data and individuals—are then resignified for security goals, quite new social and legal problems appear (Amoore 2014). All too often, inappropriate talk of 'raw data' gives the impression that they are harmless technical means of connecting the dots through algorithms. The practices and politics of algorithms are profound but scarcely explored (but see e.g. Kitchin 2014; Morozov 2013).

A third area of concern has to do with the politics of the internet in the era of 'mass' surveillance. In an obvious sense, this has been a key aspect of the Snowden controversies from the outset. Governments, including the US Administration, have been obliged to respond to the continuing debates over state power and its entwinement with commercial networks, especially internet companies (see e.g. Clarke et al. 2014). But the politics of internet surveillance is also a strong current running through the internet companies themselves—they have had to distance themselves from the NSA while at the same time acknowledging that they do cooperate extensively with government. Alongside these areas of turbulence is the active resistance of numerous NGOs who are engaged with both the civil liberties and privacy dimensions of mass surveillance and, again, the future of the internet itself. The new coalitions that have formed since Snowden, between EPIC, EFF and ACLU in the US, for instance, or under the banner of OpenMedia in Canada, are making waves in fresh ways and building creatively towards consensus on each new Snowden revelation. Could this be the more concerted response to surveillance that Colin Bennett concluded was still lacking when he published his 2008 book, *The Privacy Advocates*?

The future of the internet still hangs in the balance as the revelations about mass surveillance continue. As Ron Deibert indicates in *Black Code* (2013), broad issues of enclosure, secrecy and the arms race are all implicated here. And as Jonathan Zittrain (2009) reminds us, from a different standpoint, the internet has never had a golden age. The problems as well as the potential were built-in from the outset. Analysis of the spread of surveillance has never been more significant, from the threats to individual people to the consequences for war and peace, wealth and poverty, on a global level.

Coda: Snowden, surveillance and privacy

This article has surveyed some of the most striking implications of what, thanks to Snowden, we now know about 'national security' surveillance in the early 21st century. The historical question is, why, when the surveillance society is already so well-developed, were Snowden's 'revelations' read in the media as a complete surprise? The current question asks what key aspects of today's surveillance require new forms of analysis, along with policy and political response? The future question considers what the internet has now come to signify, and how it might be reclaimed for its original promise, given that it is the key site for surveillance practices at several levels?

At the outset, however, we noted that the Snowden revelations raise questions about the very language commonly used to discuss the monitoring and tracking of daily life and responses to these practices: surveillance and privacy. Concepts are always contested, some more than others. And definitions are always difficult because they reveal the time, place and cultural assumptions of their origins. Again, these questions have been raised before, but perhaps never so sharply as in relation to the post-Snowden scene. Once, the distinction between targeted and mass surveillance seemed fairly clear. No more. The lines blur with traffic between the two; is the person or the profile being surveilled? Once, privacy was construed primarily as a matter relating to the interests, or rights, of a specific identifiable individual. No more.

When profiling is 'anticipatory' and hunches about a possible 'nexus' to terrorism are the basis of suspicion, how exactly does privacy address this?

It has been argued here that the kinds of surveillance highlighted by the Snowden revelations are on the one hand information-intensive, often relating to the internet and on the other, 'national security'-oriented. The concept of 'security' also requires problematizing in this context, which is yet another task for the multi-disciplinary research that today is patently urgent. As with surveillance or privacy, defining security is difficult especially under present conditions, where 'national' security has been elevated to a top priority by many governments. It is a highly contested concept (Zedner 2009) often erroneously supposed to be in conflict[11] with claims to a right to privacy or to civil liberties. Much more nuanced understandings of security are required if the term is to retain any connection with the desires, aspirations and indeed well-being of everyday citizens. And these must be considered in relation to the other concepts—surveillance and privacy—affected by the 'Snowden stakes' and discussed here (see Raab 2014; Bigo [2008] 2012; Lyon 2015).

The Snowden stakes are many and varied and differ from country to country. But this complexity should not be allowed to obscure the fact that in all cases those stakes are high. The disclosures challenge some taken-for-granted assumptions and expose the real gaps in current knowledge. But this is not only a matter for those engaged in surveillance research—from whatever discipline; this is a multi-disciplinary enterprise involving not only the social sciences but investigative journalists and computer professionals as well.[12] At stake, in particular, is the future of the internet and of digital communications in general. This article tries to stress the magnitude of this challenge and hints at some ways in which this can at least be described and analyzed that do not conform to some of the dangerously dominant assumptions currently available. But the stakes are even larger and they include the very character and possibilities for politics, democracy and social justice in a time of post-Orwellian big data surveillance.

References

Agamben, Giorgio. 2013. For a theory of destituent power. *Chronos.* Available at: http://www.chronosmag.eu/index.php/g-agamben-for-a-theory-of-destituent-power.html/.

Amoore, Louise. 2014. Security and the claim to privacy. *International Political Sociology* 8(1) 108-112.

Andrejevic, Mark. 2013. *Infoglut: How too much information is changing the way we think and know*. London: Routledge.

Andrejevic, Mark. 2007. *iSpy: Surveillance and Power in the Interactive Era.* Lawrence: University of Kansas Press.

Ball, Kirstie S. and Laureen Snider, eds. 2013. *The Surveillance-Industrial Complex: A Political Economy of Surveillance*. London and New York: Routledge.

Ball, Kirstie S. 2009. Exposure: exploring the subject of surveillance. *Information, Communication & Society* 12 (5): 639-657.

Ball, Kirstie S. and Frank Webster, eds. 2003. *The Intensification of Surveillance.* London: Pluto Press.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon and R.B. Walker. 2014. After Snowden: Rethinking the impact of surveillance. *International Political Sociology* 8 (2): 121-144.

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

Bennett, Colin J. and Charles D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA: MIT Press.

Bennett, Colin J., Kevin D. Haggerty, David Lyon and Valerie Steeves, eds. 2014. *Transparent Lives: Surveillance in Canada.* Edmonton AB: Athabasca University Press. Also available at: www.surveillanceinacanada.org/.

Bigo, Didier. 2008. Globalized (in)security: The field and the banopticon. In Didier Bigo and Aanastassia Tsouskala, eds. *Terror, Insecurity and Liberty*. London and New York: Routledge.

Bigo, Didier. 2012 [2008]. International Political Sociology. In *Security Studies: An Introduction*, ed. P. Williams, 116-128. Abingdon: Routledge.

Brodeur, Jean-Paul. 2010. *The Policing Web*. Oxford and New York: Oxford University Press.

Brown, Ian. 2010. *The challenges to European data protection laws and principles*. Woking paper #1 of the Directorate General Justice Freedom and Security. Available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_1_en.pdf/

[11] The phrase "…finding a balance between privacy and security" is routinely intoned by governments and media alike but it is at best vacuous and at worst a cloak for undermining the one to bolster the other.

[12] See e.g. the call from political scientist Charles D. Raab (2013).

Burnham, David. 1983. *The Rise of the Computer State*. New York: Vintage.
Campbell, Duncan and Steve Connor. 1986. *On the Record: Surveillance, Computers and Privacy*. London: Michael Joseph.
Clarke, Richard, Michael Morrell, Geoffrey Stone, Cass Sunstein and Peter Swire. 2014. *The NSA Report: Liberty and Security in a Changing World*. Princeton, NJ and Oxford: Princeton University Press.
Clement, Andrew. 2013. IXmaps – Tracking your personal data through the NSA's warrantless wiretapping sites. *IEEE International Symposium on Technology and Society*. (IEEE Explore Digital Library: 216-223, doi: 10.1109/ISTAS.2013.661661322).
Cohen, Julie. 2012. *Configuring the Networked Self*. New Haven, CN: Yale University Press.
Cohen, Stanley. 1985. *Visions of Social Control*. Cambridge: Polity Press.
Dandeker, Christopher. 1990. *Surveillance Power and Modernity*. Cambridge: Polity.
De Sola Pool, Ithiel. 1983. *Technologies of Freedom: On Free Speech in an Electronic Age*. Cambridge, MA: The Belknap Press.
Deibert, Ronald. J. 2013. *Black Code: Surveillance, Privacy and the Dark Side of the Internet*. Toronto: Signal (McClelland & Stewart).
Fuchs, Christian. 2014. *Social Media: A Critical Introduction*. London: Sage.
Gandy, Oscar. 2012. *Coming the Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage.* London: Ashgate.
Gandy, Oscar. 1993. *The Panoptic Sort: A Political Economy of Personal Information.* Boulder, CO: Westview Press.
Gellman, Barton, and Ashkan Soltani. 2013. NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. October 30. Available at: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html/.
Giroux, Henry. 2014. Totalitarian paranoia in the post-Orwellian surveillance state. *Cultural Studies*. Online May 14. Available at: http://dx.doi.org/10.1080/09502386.2014.917118
Greenwald, Glenn. 2015. The Orwellian re-branding of mass surveillance as merely 'bulk collection.' *The Intercept* March 13. At https://firstlook.org/theintercept/2015/03/13/orwellian-re-branding-mass-surveillance-merely-bulk-collection/.
Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. New York: Metropolitan Books,Toronto: McClelland and Stewart.
Greenwald, Glenn. 2013. NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. June 5. At http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order/
Haggerty, Kevin D. and Richard V. Ericson. 1997. *Policing the Risk Society*. Toronto: University of Toronto Press.
Hayles, N. Katherine. 1999. *How we became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics.* Chicago: University of Chicago Press.
Jessop, Bob. 2007. Knowledge as a fictitious commodity: insights and limits of a Polanyian analysis. In *Reading Karl Polanyi for the 21st Century: Market Economy as a Political Project*, eds A. Bugra and K. Agartan, 115-134. Basingstoke: Palgrave.
Kitchin, Rob. 2014. *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences*. London: Sage.
Lauer, Josh. 2012. Surveillance history and the history of new media: evidence-producing technologies. *New Media and Society* 14 (4) 566-582.
Levy, Steven. 2014. How the NSA almost killed the internet. *Wired*. July 1. Available at: http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/all/.
Lynch, Jennifer. 2010. New FOIA documents reveal DHS social media monitoring during Obama inauguration. Available at: https://www.eff.org/deeplinks/2010/10/new-foia-documents-reveal-dhs-social-media/.
Lyon, David. 2015 (forthcoming). *Surveillance after Snowden*. Cambridge: Polity.
Lyon, David. 2014a. Surveillance, Snowden and Big Data: Capacities, Consequences, Critique. *Big Data & Society* 1 (1). Available at: http://bds.sagepub.com/content/1/2/2053951714541861.abstract/.
Lyon, David. 2014b. The emerging surveillance culture. In *Media, Surveillance and Identity*, eds André Jansson and Miyase Christensen. New York: Peter Lang.
Lyon, David. 2013. Can citizens roll back silent army of watchers? *The Toronto Star*. September 23. Available at: http://www.thestar.com/opinion/commentary/2013/09/23/can_citizens_roll_back_silent_army_of_watchers.html/.
Lyon, David and Özgün Topak. 2013. Promoting global identification: corporations, IGOs and ID card systems. In *The Surveillance-Industrial Complex: A Political Economy of Surveillance*, eds Kirstie S. Ball and Laureen Snider, 27-43. London and New York: Routledge.
Lyon, David. 2005. A sociology of information. In *The Sage Handbook of Sociology*, eds Craig Calhoun, Chris Rojek and Bryan Turner. London and New York: Sage.
Lyon, David. 2003. *Surveillance after September 11*. Cambridge: Polity.
Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.
Morozov, Evgeny. 2013. The real privacy problem. *MIT Technology Review*. October 22. Available at: http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/.
Marquez, Xavier. 2012. Spaces of appearance and spaces of surveillance. *Polity* 44: 6-31.
Marwick, Alice. 2013. *Status Update: Celebrity, Publicity and Branding in the Social Media Age*. New Haven, CT: Yale University Press.
Marwick, Alice. 2012. The public domain: Surveillance in everyday life. *Surveillance & Society* 9 (4): 378-393.
Marx, Gary. 1988. *Undercover: Police Surveillance in America.* Berkeley, CA: University of California Press.

Mosco, Vincent. 2014. *To the Cloud: Big Data in a Turbulent World*. Boulder, CO and London: Paradigm Publishers.
Polanyi, Karl. 2001. *The Great Transformation: The Political and Economic Origins of Our Time*, 2nd ed. Foreword by Joseph E. Stiglitz. Boston: Beacon Press.
Polanyi, Karl. 1944. *The Great Transformation.* New York: Farrar and Rinehart.
Raab, Charles. 2014. Privacy as a Security Value. In *Jon Bing: En Hyllest / A Tribute*, eds Dag Wiese Schartum, Lee Bygrave and Anne Gunn Berge Bekken, 39-58. Oslo: Gyldendal.
Raab, Charles. 2013. Studying surveillance: the contribution of political science? *Political Insight*. October 29. Available at: http://www.psa.ac.uk/insight-plus/blog/studying-surveillance-contribution-political-science/.
Raab, Charles and Benjamin Goold. 2011. *Protecting Information Privacy*. Equality and Human Rights Commission Research Report 69. Available at: http://www.equalityhumanrights.com/sites/default/files/documents/research/rr69.pdf/.
Regan, Priscilla. 2009 (1995). *Legislating Privacy: Technology, Social Values and Public Policy*. Durham, NC: University of North Carolina Press.
Rule, James. 1974. *Private Lives, Public Surveillance: Social Control in the Computer Age*. New York: Schocken Books.
Schiller, Dan. 1988. How to Think about Information. In *The Political Economy of Information*, eds V. Mosco and J. Wasko, 27-44. Madison: University of Wisconsin Press.
Steeves, Valerie. 2009. Reclaiming the social value of privacy. In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Age*, eds Ian Kerr, Carol Lucock and Valerie Steeves. New York: Oxford University Press.
Taylor, Emmeline. 2013. *Surveillance Schools: Security, Discipline and Control in Contemporary Education*. London: Macmillan.
Timberg, Craig and Ellen Nakashima. 2013. Agreements with private companies protect access to cables' data for surveillance. *The Washington Post*, July 6. Available at: http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html/.
Trottier, Daniel. 2012. *Social Media as Surveillance*. London: Ashgate.
Turow, Joseph. 2012. *The Daily You: How the New Advertising Industry is Defining your Identity and your Worth*. New Haven, CT: Yale University Press.
Webster, Frank, and Kevin Robins. 1986. *Information Technology: A Luddite Analysis*. NJ: Ablex.
Weston, Paul, Glenn Greenwald and Ryan Gallagher 2013. New Snowden docs show US spied during G20 in Toronto. CBC News, Nov 27. Available at: http://www.cbc.ca/m/touch/news/story/1.2442448/.
Zedner, Lucia. 2009. *Security.* New York and London: Routledge.
Zittrain, Jonathan. 2009. *The Future of the Internet*. New Haven, CT: Yale University Press.
Zuboff, Shoshana. 1988. *In the Age of the Smart Machine: The Future of Work and Power*. New York: Basic Books.