International Journal of Communication 10(2016), 164–177 1932–8036/20160005

IJoC Digital Age

Managing Surveillance: Surveillant Individualism in an Era of Relentless Visibility

SHIV GANESH[1]
Massey University, New Zealand

Contemporary surveillance occurs in the context of communicative abundance, where visibility is not only easy but relentless: never ending, far reaching, and ceaseless. Managing surveillance therefore has considerable implications for democratic politics, workplace control, economic practices, cultural politics, and individual subjectivity. This article identifies surveillant individualism, or the pivotal role that individuals play in surveillance and countersurveillance, as a major feature of contemporary surveillance management. It seeks to clarify current research trajectories on digital surveillance management and to chart a course for organizational research on surveillant individualism.

Keywords: countersurveillance, relentless visibility, sousveillance, surveillant individualism

The rise of surveillance needs foremost to be contextualized with visibility as a major 21st century trope. It is not a stretch to claim that visibility is now a central concern of social and organizational theory, and scholars from multiple theoretical traditions and disciplines have traced how myriad forms of sociality and organizing have been modernized and rationalized, rendered knowable, and made transparent and accessible (Brighenti, 2007, 2010). Others have argued that the 21st century is characterized by a "new visibility," a powerful new force facilitated by digital media that is both intensively and extensively transforming our social and political fabric (Thompson, 2005).

A major form of managing visibility involves attending to issues of transparency, which, as Christensen and Cornelissen (2015) argue, is itself a central and mythical part of a contemporary world, a

Shiv Ganesh: S.N.Ganesh@massey.ac.nz
Date submitted: 2015–08–14

[1] This project was enabled by a grant on emerging forms of digital activism from the Royal Society of New Zealand's Marsden Foundation (MAU-1209). The author would like to thank the participants of a June 2013 workshop on transparency, communication, and organization at Copenhagen Business School as well as those of a November 2014 follow-up at the University of California, Santa Barbara, for their helpful engagement with the ideas in this article.

deep-seated way of knowing and acting in the present age. However, despite several multitheoretic critiques of transparency in organizational and communication studies (Christensen & Cheney, 2015), liberal conceptions of transparency continue to prevail in practice. This is especially true of many civil society organizing efforts around the world, in which demands for transparency as an explicit or meta-objective ideal now drive many efforts, especially in an era of digital ubiquity (Bimber, Flanagin, & Stohl, 2012).

Demands for transparency are certainly important in an era in which a considerable proportion of the world's population is still outside the information loop but nonetheless significantly impacted by it, and these demands from civil society groups all over the world have had important material and democratic social impacts. However, popular liberal discourse on transparency can ironically obscure issues of surveillance. Several scholars have proposed the idea that increased transparency implies increased surveillance, and the two are intimately connected. Indeed, surveillance might be regarded as the dark other of transparency: As Drucker and Gumpert (2007) have observed, transparency itself is a two-sided concept, involving both openness and surveillance, visibility and invisibility. In many respects, then, managing transparency *is* managing surveillance. John Keane's (2009) concept of monitory democracy is a perfect example of how processes of managing transparency require surveillance in the form of *monitoring*, as evidenced by the proliferation of agencies and organizations, including watchdogs, inquiries, commissions, international committees, old and new media, and think tanks that track, research, measure, or seek to render accountable the actions of governments.

Yet another factor complicating the relationship between transparency and surveillance is the fact that surveillance itself has changed quite remarkably in the last 30 years and now involves individuals watching organizations as much as it does organizations watching individuals. For much of the 20th century, surveillance was understood not only through a dystopian Orwellian metaphor but also as a manifestly organizational activity: It required management in the forms of organizational infrastructure, resources, technologies, and expertise and was hardly something individuals could do on their own. Indeed, our very notions of surveillance are undergirded by a notion of communication scarcity, a construct that assumes that secrecy is relatively easy, and that recording and transmitting communication are both difficult and expensive. Essentially, then, surveillance involved organizations watching individuals, whether those organizations were corporations, states, police forces, terrorist outfits, or intelligence agencies, or some combination thereof.

Now, however, surveillance occurs in a context of communication abundance, where visibility is not only easy but also never ending, far reaching, and ceaseless—in other words, *relentless*. Communication itself moves quickly and easily through multiple media simultaneously (Blumler & Coleman, 2015; Blumler & Kavanagh, 1999), and this further complicates dystopian Orwellian visions of surveillance. Consequently, the surveillant relationship between organizations and individuals is inverted: Digital ubiquity has resulted in surveillance being operationalized as individuals watching organizations—or each other. Scholars have struggled to come to terms with such sharp shifts, coining terms such as *dataveillance* (Marx, 2003) and the *electronic superpanopticon* (Poster, 1990) to describe the shift from analog to digital forms of surveillance. Perhaps most profoundly, in an environment of communication

abundance and relentless visibility, the binary between surveillance and countersurveillance as management and resistance, respectively, begins to break down.

The management of surveillance is therefore of the utmost importance, not only because it is considerably more fraught in such a complex and volatile digital environment but also because of the implications that surveillance has for democratic politics, workplace control, economic practices, cultural politics, and individual subjectivity. As digital code continues to be programmed into the texture of our everyday lives, producing particular kinds of spaces, politics, and economies and moving us beyond digital/analogue or online/offline binaries, our understanding of surveillance practices and their dystopian implications will continue to shift and become more complex.

In particular, the notion of surveillant individualism, which emphasizes the increasingly pivotal role that individuals play in surveillance and countersurveillance, is central to understanding the ambiguities and contradictions of contemporary surveillance management. In the contemporary environment, organizations act much as individuals do in surveillance processes, even as a few key nodes such as the National Security Agency (NSA) in the United States become superorganizations. Thus, this article seeks to clarify current research trajectories on digital surveillance management while charting a course for research on surveillance management. It does so first by discussing shifts in the surveillant environment, attending in particular to the notions of relentless visibility and surveillant individualism. Then, it unpacks two prominent theoretical points of view in surveillance studies that have different implications for understanding surveillance management and resistance. Finally, it outlines three implications for research on surveillance management.

Relentless Visibility and Surveillant Individualism

The last 20 years have seen a sharp rise in studies of surveillance, particularly of digital forms of surveillance. This is hardly surprising, given the increasing relentlessness of visibility as a mode of organizing: Take, for instance, the profound acceleration of digital technologies, the transformation of systems of workplace control, the institutionalization of neoliberal regimes of governance, and the global war on terror. Recent years have seen some global public outrage at surveillance activities of superorganizations such as the NSA, following the revelations of a former systems administrator for the CIA, Edward Snowden. Snowden's whistle-blowing indexes and makes visible the extent to which the everyday lives of citizens in much of the world are digitally monitored, tracked, and relentlessly recorded in a manner that even Orwell's (1948) dystopian vision in *Nineteen Eighty-Four* could not predict. The Utah Data Center in Bluffdale, built by the NSA in 2013, for example, has a storage capacity of yotabytes, or *quadrillions* of gigabytes, many times the capacity of the entire digital world, that costs approximately 40 million dollars in annual energy charges (Bamford, 2012). The human imagination can scarcely contemplate such scale.

In Aotearoa, New Zealand, Snowden's revelations have thrown into relief some of the hitherto murky operations of the Government Communication Security Bureau (GCSB). The GCSB was integrated into the intelligence network ECHELON in the 1980s (Hager, 1996), and New Zealand's satellite interception facilities in Waihopai and Tangimoana were created as part of its agreement with the four

other countries—Australia, Canada, the United Kingdom, and the United States—that created ECHELON. In post–Cold War politics, the network was sometimes critically labeled Big Brother without a Cause (e.g., Asser, 2000), but its relevance to the digital universe only became apparent after Snowden's disclosures in 2013, when it reemerged in popular discourse as the Five Eyes Network. The GCSB also came into prominence for its role in spying on the German digital entrepreneur Kim Dotcom in a series of events that led to his arrest in 2012. The Kitteridge Report, which established the illegal nature of that spying, led to the passage of the GCSB and Related Intelligence Amendments bill, which now permits the GCSB to collect intelligence from foreign citizens and expand the scope of cybersecurity work to assist private corporations. The law was passed in early July 2013, a month after Snowden's revelations about interception of data from the transpacific Southern Cross cable became public, and there were protests across the country against the passage of the bill.

These developments are important, as they index just how deeply embedded surveillance is in our everyday lives. As Mathieson (2012) says, it is the "cardinal point" of the Internet (p. xviii). Relentless visibility is in some ways the ultimate affordance of a digitally ubiquitous environment. It is an issue that any scholar studying collective action around social justice issues now encounters in activist practice (e.g., Ganesh & Stohl, 2013). The quantity of surveillance has thus resulted in a paradox: On one hand, surveillance is mundane, every day, and constant, but at the same time, it is unnoticed and therefore unseen. Mathieson (2012) in particular warns of the dangers associated with the "suave, unnoticeable and undetected surveillance of groups, categories and populations, its unnoticeable character in turn silencing opposition" (p. xx).

Gary Marx (2003) refers to three broad qualitative shifts in the structure of contemporary digital surveillance that distinguish it from analog forms. First, in the contemporary system, the surveilled are not aware of being surveilled (in contrast to the mode of surveillance exemplified by, say, the Hawthorne experiments; see, e.g., Carey, 1967). Second, surveillance is better understood as *dataveillance*, or technical surveillance without a surveillor and based on binary data rather than visual images. And third, the transmission of the surveilling act is radically easier than in previous generations.

Thus, the enactment and management of surveillance have been rendered highly complex by the spread, speed, flow, and extent of contemporary digital surveillance. Further, just as the organizational character of collective action in general has become more complex as individuals acquire more agency, organizational boundaries become more porous, and organizations themselves become more informal and short-lived (Bimber et al., 2012); many forms of surveillance are themselves now individualized rather than collective and are less reliant on formal organizational resources than on individual technical expertise.

Just as it is possible to speak of networked individualism, in which individuals are connected to each other as individuals rather than as members of groups, communities, or organizations (Rainie & Wellman, 2012), so too is it possible to speak of *surveillant individualism* as a contemporary managerial and disciplinary practice, a product of a society characterized by mass individualism (Gates, 2011), in which individuals monitor and surveil each other as everyday practice *qua* individuals rather than as representatives of other organizations or groups. Three aspects of surveillant individualism are worth

mentioning. First, as Fuchs (2011) says, surveillant individualism entails *prosumption*—the production and consumption of surveillance by the very same subjects. As a construct, prosumption acknowledges the user's complicity in and sometimes their desire for the ability to surveil others (Hu, 2015) or even be surveilled. Second, it involves what Rainie and Wellman (2012) call *coveillance*, or peer-to-peer individual surveillance. Social networking is perhaps a quintessential example of coveillance. Third, surveillant individualism involves *sousveillance*, a neologism coined by scholar-activist Steve Mann to describe contemporary ways that individuals engage in surveillance to challenge authority. If coveillance is peer-to-peer surveillance, sousveillance might be characterized as bottom-up surveillance. Per Mann, Nolan, and Wellman:

> One way to challenge and problematize both surveillance and acquiescence to it is to resituate these technologies of control on individuals, offering panoptic technologies to help them observe those in authority. We call this inverse panopticon "sousveillance" from the French words for "sous" (below) and "veiller" to watch. (2003, p. 332)

Surveillant individualism thus works at the level of the individual, but it is important to note again that in the contemporary environment, individual and organizational levels of analysis are impossible to clearly demarcate, and organizations themselves often function as individuals do, using the same tools—running a Google search or scanning the social network feed of a potential employee are common recruiting practices, for instance.

Even as surveillance practices continue to expand and transform, accounts of resistance to it are manifold. Activists all over the world have developed myriad creative and sometimes surprisingly effective tactics to counter state, police, and corporate forms of surveillance. Scholars have, in turn, studied such resistant organizing practices to further animate conceptions of sousveillance and countersurveillance (Fernandez & Huey, 2005 Marx, 2003; Wilson & Serisier, 2010). The now (ironically) iconic group Anonymous, for example, is famous for developing a collaborative hacktivism in what is sometimes hailed as a 21st century form of direct action. Indeed, for activists in general, resistance to surveillance is a crucial issue in collective activist practice in the context of relentless visibility.

However—crucially—resistance to surveillance is often subject to the same dynamics of surveillant individualism as contemporary surveillance itself. For instance, resistance to digital surveillance is often not organized collectively. Instead, it spans the full gamut of resistance tactics and is often manifested in casual, unexpected, ironic, playful, and feeble ways. Speed cameras are an excellent and notorious site for such resistance. Several years ago, high school students in Maryland pranked a speed camera by reproducing car license plates and speeding past the camera to ensure that faulty tickets were issued to their "enemies." Bystanders have also been known to take pictures of speed cameras operating outside legally established parameters. In many parts of the world, motorists often flash their headlights at oncoming motorists to indicate a speed camera in the vicinity. The wide variety of resistant practices to contemporary digital surveillance has immense potential for insight into the kinds of political and cultural mobilizations that characterize our current era and, consequently, what kinds of practices and populations are occluded.

All this makes it critical for those scholars interested in surveillance management to chart a theoretical course on surveillance and countersurveillance. Although, as I will discuss later, definitions of countersurveillance vary, it is often understood as "intentional, tactical uses, or disruptions of surveillance technologies to challenge institutional power asymmetries" (Monahan, 2006, p. 516). It might be easy to conclude that some practices involving surveillant individualism, in particular sousveillance, are forms of countersurveillance. However, the relationship between countersurveillance and sousveillance is conceptually blurry and is predicated upon an underlying approach to defining and studying surveillance itself.

To clarify this, I outline two major approaches to the study of digital surveillance in the next section: one that draws significantly from a Weberian sociological tradition and an Orwellian cultural imaginary, and another that both draws from and attempts to move beyond Foucault's rendition of a panoptic society. I then move on to a consideration of how these two approaches have differently considered and conceptualized resistance to surveillance. In the final section, I conclude the article by presenting three productive directions for research on surveillant individualism.

Theoretical Perspectives on Surveillance

Scholars in surveillance studies have approached the subject from multiple theoretical points of view, and in relatively crude terms, these might be reduced to two perspectives, one structural and the other poststructural (see Table 1). Whereas some scholars who work in the structural tradition (e.g., Lyon, 2005) have occasionally drawn from Marx, saying that surveillance is an integral part of the struggle between labor and capital, others have either not drawn significantly from Marxist approaches or have ignored them altogether. Fuchs (2011) argues that at least some of this may have to do with Giddens' prominent take on surveillance and Marx in the 1980s. For Giddens (1985), Marxist points of view have not been able to adequately account for surveillance because surveillance is a part of modernity in a way that is not accounted for by class struggle or even capital itself.

Certainly, there are many reasons to object to this characterization. Harry Braverman, along with other labor process scholars, for example, has shown that worker surveillance is an integral part of Fordist modes of production (Mumby, 1988). Likewise, Gandy (2003) argues that consumer surveillance is a fundamental dynamic in capitalist societies. It is arguably impossible to separate out surveillance practice from the broader dynamics of capitalism; as Jodi Dean (2005) has argued in her thesis on communicative capitalism, even "communicative exchanges, rather than being fundamental to democratic politics, are the basic elements of capitalist production" (p. 56).

Despite the potentially productive grounds for Marxist-inspired studies of surveillance, most research in surveillance studies has tended to draw from Weberian or Foucauldian inspired theoretical frameworks. Weberian-oriented formulations in particular have provided the cornerstone for much work on surveillance. Scholars such as David Lyon (2005) have discussed surveillance as built into processes of rationalization, as exemplified by the bureaucratic form. Take Lyon's (2005) definition of surveillance: "Where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance" (p. 2).

In this sense, surveillance is a manifestly organizational activity, involving organizations watching over individuals and groups. As Lyon says, surveillance is purposeful, systematic, routine, and focused, and in this way it is quintessentially bureaucratic. There are three key features of a Weberian notion of surveillance. First, it is hierarchical and unidirectional, with a clear ontological distinction between a powerful but identifiable surveilling agent and a subordinate surveilled subject. Second, surveillance is understood in terms of repression and its potential to regulate and stamp out practices that are disruptive of social order. And finally, surveillance in a Weberian sense is focused on the management of production and behavioral technologies. The now notorious time and motion techniques of scientific management, which attempted to achieve bureaucratic and industrial efficiency by monitoring and measuring every movement of workers, exemplify such surveillance (Taylor, 1911).

A Foucauldian-inspired notion of surveillance, on the other hand, draws from his famous appropriation of Bentham's panopticon. Rather than involving an organization observing individuals, the panoptic metaphor draws our attention to one watching many. At the heart of Foucault's panoptic metaphor is the lack of awareness of the surveilled about the surveilling agent, and the possibility that a distinct surveillor might not even exist. Thus, the focus in Foucauldian formulation of surveillance is not so much on the management of production or work as it is upon the subjectivity of those surveilled, and surveillance itself is understood as a technology of the self, or the means by which individual subjectivity is itself produced. As Hansen and Flyberbom (2014) say:

> The multidirectional nature of surveillance means that its target is not only the "deviant," as frequently implied by the panoptic metaphor, but nearly everyone by default. That surveillance is made from multiple angles and social positions reflects the polycentric character of contemporary social formations in which *governing* subjects, like representatives of corporations and governments, are also *governed* subjects. (p. 5)

Consequently, surveillant acts are not seen as repressive, unlike the Weberian model; instead, they are understood as productive of particular subject positions. Scholars who have worked in this postpanoptic tradition thus reject the idea of a hierarchy of surveillance, seeing it instead as a formative social dynamic. Haggerty and Ericson (2000), for example, interpret surveillance in Deleuzian terms, as an emergent and unstable assemblage that constitutes social relations. In an era of relentless visibility, the idea of a surveillant assemblage is evocative indeed. For instance, in an era of big data, where consumer research is increasingly fuelled by digital information that provides comprehensive information about individual consumption preferences, "data doubles," or digital composites of individuals, are in many ways more objective than individual subjects themselves because they yield much more objective data about behavior than our own subjective impressions.

Table 1. Two Perspectives on Surveillance and Countersurveillance.

	Perspective I	**Perspective II**
Theoretical inspirations	Weber, Orwell, and sometimes Marx	Foucault, Deleuze, and beyond
Main metaphors for surveillance	Organizations watching individuals	Panoptic and postpanoptic metaphors: one watching many; or Synoptic metaphors (Mathieson, 1997): many watching a few
Structure of surveillance	Hierarchical and structural, with identifiable surveilling agents	Poststructural: Surveilling agents are invisible, and surveillance is an assemblage
Means of surveillance	Repressive: production and behavioral technologies	Productive: technologies of the self
Object of surveillance	Individuals (involves conceptual distinctions between individual and mass surveillance)	Populations; "mass individualization" (Gates, 2011)

Resisting Surveillance

These two perspectives have significant implications for how one understands how surveillance might be both managed and resisted. A structural point of view often understands surveillance as a managerial practice and resistance to it an intentional act designed to disrupt or interrupt the surveilling gaze. Because surveillance itself is seen as a process of monitoring and managing individuals rather than as a constitutive social dynamic, it is possible for researchers within this tradition to understand resistance to surveillance in terms of practices that are not surveillant in and of themselves. For instance, Gary Marx's (2003) resistance typology identifies countersurveillance as one of many means of resisting surveillance. For Marx, activists who resist surveillance tend to engage in one or a combination of many tactics. These include discovery moves, or identifying whether surveillance is occurring and through what technologies; avoiding places where surveillance exists; distorting surveillance, or manipulating data collection so that it seems or looks legitimate and valid when it is actually not; preventing the recording of information; breaking the surveillance device itself; rendering the surveillance device itself inoperable; and countersurveillance, or observing the observers.

Thus, while structural perspectives identify countersurveillance as a behavior that is conceptually distinct from other kinds of resistant practice, it is ironically not seen as fundamental to resistance itself. In a poststructural formulation, however, what counts as countersurveillance shifts quite dramatically. Instead of countersurveillance being understood as a direct and oppositional act, it is understood as a "highly mediated, contradictory and continually reconfigured activity" (Wilson & Serisier, 2010, p. 178). In

fact, the idea of *countering* surveillance itself is ontologically suspect. Instead, resistance is understood in terms of the features of surveillant individualism most oriented toward challenging authority: acts of sousveillance. Here, sousveillance is seen as an endless cycle of observation by individuals, breaking sharp distinctions between observer and observed. Table 2 provides distinctions between a structural countersurveillance-oriented view of resistance and a poststructural sousveillance-oriented view of resistance. As the table implies, each orientation interprets the other in quite different ways. In particular, a countersurveillance-oriented stance identifies sousveillance, understood as the many watching the one, as a synoptic practice that is one form of countersurveillance.

Table 2. Countersurveillance and Sousveillance.

Countersurveillance-oriented	Sousveillance-oriented
A direct looking back/returning of the gaze.	Highly mediated, contingent, contradictory, and continually reconfigured (Wilson & Serisier, 2010).
One of many ways of neutralizing surveillance.	Any neutralization of surveillance is countersurveillance.
Sousveillance is a form of countersurveillance.	Sousveillance is an endless cycle of observation, or liquid surveillance (Bauman & Lyon, 2013).

Weber: The Ghost in the Surveillance Machine

It would be easy to conclude that in an era of relentless visibility, managing surveillance and paying attention to surveillant individualism involves drawing entirely from the poststructural perspective as outlined above and that Weberian-inspired critiques of surveillance are more historical than contemporary, applicable to a social milieu dominated by 20th-century-style formal bureaucratic organizations. However, as Haggerty and Ericson (2000) point out, "contemporary studies of surveillance continue to emphasize [the] hierarchical aspects of observation" (p. 617). More specifically, studies of digital surveillance that draw on Foucauldian views of surveillance already rely implicitly, if sometimes less than productively, on some structural (post) Weberian formulations.

As Brighenti (2007) says, for Foucault, power is only visible in its effects and invisible in its identity. Surveillance and the disciplinary gaze for Foucault are close to identical. The French title of Foucault's *Discipline and Punish* is, after all, *Surveiller et Punit*—it was on Foucault's suggestion that the English translation of the book substitute the word "surveil" with "discipline" (Miller, 1993). So in a purely Foucauldian formulation, surveillance and the disciplinary gaze are one and the same thing. Discipline/surveillance is a condition or feature of contemporary society: as a network, without hierarchy, and without an identifiable surveilling agent (Foucault, 1977). However, work in surveillance studies that draws from Foucault tends to reinscribe structural points of view by treating not only the surveilled object but also the surveilling object *as visible*. Even Haggerty and Ericson's (2000) treatment of the surveillant assemblage draws frequently from examples of the police and the FBI as actual surveillors.

Thus, empirical confusion sometimes results in poststructural perspectives taking on structural undertones, and in the process turning the figure of Weber himself into the ghost in the surveilling machine. At other times, Weber's presence is more subtle, inasmuch as there is a deeply pessimistic overtone to much of the postpanoptic literature. In some ways this elides the fact that Foucault had a vastly different notion of surveillance than liberal democratic or structural ideas of surveillance or its possibilities. None of this is to say that the structural sensibility of postpanoptic points of view on surveillance and countersurveillance are counterproductive. On the contrary, rather than sharply delineate structural and poststructural positions, we should recognize that the lines between them can blur, that practice, thought, and logic dance inexorably between and through these distinctions, and that there are productive ways of holding these perspectives in tension. How might we think through how such hybridization could be productive?

Further Research

Thus far, I have argued that in an era of relentless visibility, managing surveillance (and countersurveillance) involves attending to surveillant individualism writ large and paying attention to presumption, coveillance, and sousveillance. How might this happen? First, instead of seeing sousveillance as one form of countersurveillance, or conversely, seeing all sousveillance as an endless cycle of observation, we might invert the relationship between them and understand contemporary countersurveillance as one aspect of sousveillance. Assessing the potential of sousveillance and countersurveillance has important implications for how we understand surveillant individualism, which can, after all, can be a highly reactionary and even authoritarian practice: Consider the new digital possibilities for citizens reporting crime, reporting on fellow drivers who are speeding, or even the all too common flooding of comments to the media from people who may have witnessed or been part of tragic accidents.

More broadly, Jodi Dean's ideas about communicative capitalism come into play. For Dean (2005), individual communicative acts, including political ones, are commodities in digital capitalism. Self-expression, sharing, and other forms of online communication not only prop up the corporate Internet but also serve to commoditize communication itself. In this sense, questions about countersurveillance involve asking about the possibility for resistive communicative praxis in the contemporary era.

Others, such as Margetts, Hale, and Yasseri (2014), also argue that digital technologies facilitate microparticipation but do not easily foster more robust and enduring forms of collective action. Studying countersurveillance could go a long way toward elaborating and sharpening or, conversely, to qualifying and challenging such assertions. For instance, one of the main innovations to come out of the Bitcoin experiment from the last few years has been the popularization of Blockchain technologies. Activists who work on issues of electronic democracy have been quick to jump on the potential of Blockchain technologies to eliminate the pervasive astroturfing that characterizes many electronic or digital campaigns by harnessing the technology to authenticate and legitimize every expression of online support. What potential does this technology have as a form of countersurveillance in a society characterized by surveillant individualism? How can one understand Blockchain as part of an ongoing

dance between control and resistance or as the ongoing manipulation and assertion of public opinion? As Uldam (2014) argues in a study of BP's and Shell's digital surveillance of their critics:

> Mediated visibility grant(s) *both* power and vulnerability to *both* corporate and civil society actors, and raises questions about the ways in which this tension is played out. At the same time, the dynamics of visibility encompass a double capacity of discipline: mediated visibility simultaneously works to instil self-discipline (as activists are conscious of security issues, and, for example, avoid providing their real names when registering a blog) and actual discipline. (p. 15)

Second, whereas many scholars of digital surveillance have talked about the synopticon (e.g., Mathieson, 1997, many contemporary studies continue to identify surveillance in practice as a set of exchanges between two agents: surveillor and surveilled. However, surveillant individualism invariably involve multiple individual coveillant agents. Indymedia, the iconic alternative media platform for global justice activists, is a case in point. Our own study of Wellington-based activists several years ago (Ganesh & Stohl, 2010) showed how the Aotearoa Indymedia website was not just a way for activists to communicate among themselves but was also a way for the policemen in the area to monitor ongoing activist effort. Additionally, it was also a way for local Neo-Nazis to monitor the activists and potentially stage counterevents. Some digitally savvy activists even began to monitor who was accessing the Indymedia site and from where, in the process deriving remarkably useful information about who was watching them. Looking at contemporary digital collective action, therefore, invariably involves an analysis of coveillance and sousveillance so explicit identification of multiple surveilling agents can yield sophisticated insight into moves, countermoves, internal tensions, and even unlikely alliances between surveillors and surveilled.

Third, a hybrid point of view helps to go beyond the focus on neutralization in studies of activist practice. Neutralization, as outlined earlier, is typically understood as a goal of resistance to surveillance. But if we take seriously the idea that neutralization is "a dynamic, adversarial social dance involving moves and countermoves. It has the quality of an endless chess game" (Marx, 2003, p. 388), then we need to consider it as a circular, ongoing process and to look at counterneutralization and counter-counterneutralization. Nowhere are these dynamics more apparent than in contemporary maneuvering around cryptography and decryptography. The field of action around cryptography is complex. On one hand, open-source activists, programmers, and hackers have been at the vanguard of developing robust standards of data security. Pretty Good Privacy (PGP), for instance, is integral to the history of the Internet as we know it. Its developer, Phil Zimmerman, released it in 1991 to Peacenet, a global service provider for peace organizations. He was then targeted by the U.S. government for a munitions crime and retaliated by publishing all the source code for PGP, creating an entire movement in the process. On the other hand, security agencies have been prolific in countering activist moves and hacker activity. Consider the Ethical Hacking certificate (a program that counts Edward Snowden among its graduates), which is a form of digital security training. Snowden's revelations from 2013 included the existence of Bullring, a decryption initiative run by the Five Eyes Network.

In short, we need to get into the field. A close study of the everyday and mundane ways in which surveillance is constructed in activist practice could provide crucial insight into what specific constructions allow it to emerge as a political issue, as a moment for mobilization, or as a security concern. Conversely, studying how surveillance is enacted by individuals in all its forms will help us to better understand when exactly it ceases to be an issue, fades into the background, and becomes transparent as an unremarkable or irrelevant phenomenon, an implicit or explicit risk, or embedded as part of the trusting apathy of the public toward widespread surveillance. This in turn could help shed further light onto the constitutive role that surveillance practices play in our everyday lives, producing some forms of political and cultural mobilization and disabling others.

References

Asser, M. (2000). Echelon: Big brother without a cause? *BBC News Online.* Retrieved from http://news.bbc.co.uk/2/hi/europe/820758.stm

Bamford, J. (2012, March 15). The NSA is building the country's biggest spy center (watch what you say). *Wired*. Retrieved from http://www.wired.com/2012/03/ff_nsadatacenter/

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance*. Cambridge, UK: Polity Press.

Bimber, B., Flanagin, A., & Stohl, C. (2012). *Collective action in organizations: Interaction and engagement in an era of technological change*. Cambridge, UK: Cambridge University Press.Blumler, J. G, & Coleman, S. (2015). Democracy and the media—revisited*. Javnost, 22*, 111–128.

Blumler, J. G., & Kavanagh, D. (1999). The third age of political communication: Influences and features. *Political Communication, 16*, 209–230.

Brighenti, A. (2007). Visibility: A category for the social sciences. *Current Sociology, 55*(3), 323–342.

Brighenti, A. (2010). *Visibility in social theory and social research*. New York, NY: Palgrave.

Carey, A. (1967). The Hawthorne studies: A radical criticism. *American Sociological Review, 32*, 403–416.

Christensen, L. T., & Cheney, G. (2015). Peering into transparency: Challenging ideals, proxies, and organizational practices. *Communication Theory*, *25*, 70–90.

Christensen, L. T., & Cornelissen, J. P. (2015). Organizational transparency as myth and metaphor. *European Journal of Social Theory*, *18*(2), 132–149.

Dean, J. (2005). Communicative capitalism: Circulation and the foreclosure of politics. *Cultural Politics, 1*, 51–74.

Drucker, S., & Gumpert, G. (2007). Through the looking glass: Illusions of transparency and the cult of information. *Journal of Management Development, 26*(5), 493–495.

Fernandez, L. A., & Huey, L. (2005). Is resistance futile? Thoughts on resisting surveillance. *Surveillance & Society, 6*(3), 198–202.

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

Fuchs, C. (2011). Web 2.0, presumption, and surveillance. *Surveillance & Society, 8*(3), 288–309.

Gandy, O. H. (2003). Data mining and surveillance in the post-9/11 environment. In K. Ball & F. Webster (Eds.), *The intensification of surveillance* (pp. 26–42). London, UK: Pluto Press.

Ganesh, S., & Stohl, C. (2010). Qualifying engagement: A study of information and communication technology and the global social justice movement in Aotearoa, New Zealand. *Communication Monographs, 77*(1), 51–75.

Ganesh, S., & Stohl, C. (2013). From Wall Street to Wellington: Protests in an era of digital ubiquity. *Communication Monographs*, *80*(4), 425–451.

Giddens, A. (1985). *The nation-state and violence*. Cambridge, UK: Polity Press.

Hager, N. (1996). *Secret power: New Zealand's role in the international spy network*. Nelson, NZ: Craig Potton.

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

Hansen, H. K., & Flyverbom, M. (2014). The politics of transparency and the calibration of knowledge in the digital age. *Organization.* (Published online first.) doi:10.1177/1350508414522315

Hu, T.-H. (2015). *A prehistory of the cloud*. Cambridge, MA: MIT Press.

Keane, J. (2009). *The life and death of democracy.* New York, NY: Simon & Schuster.

Lyon, D. (2005). *Surveillance society: Monitoring everyday life*. Philadelphia, PA: Open University Press.

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.

Margetts, H., Hale, S. A., & Yasseri, T. (2014). Big data and collective action. In M. Graham & W. H. Dutton (Eds.), *Society and the Internet: How information and social networks are changing our*

lives. Oxford, UK: Oxford University Press.

Marx, G. T. (2003). A tack in the show: Neutralizing and resisting the new surveillance. *Journal of Social Issues, 59*(2), 369–390.

Mathieson, T. (1997). The viewer society: Michel Foucault's `Panopticon' revisited. *Theoretical Criminology, 1*(2), 215–234.

Mathieson, T. (2012). Introduction. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media.* New York, NY: Routledge.

Miller, J. (1993). *The passion of Michel Foucault*. New York, NY: Simon & Schuster.

Monahan, T. (2006). Counter-surveillance as political intervention? *Social Semiotics, 16*(4), 515–534.

Orwell, G. (1948). *Nineteen eighty-four*. London, UK: Penguin.

Poster, M. (1990). *The mode of information: Poststructuralism and social context*. Chicago, IL: University of Chicago Press.

Rainie, L., & Wellman, B. (2012). *Networked individualism: The new social operating system*. Cambridge, MA: MIT Press.

Taylor, F. W. (1911). *The principles of scientific management*. New York, NY: Harper & Row.

Thompson, J. B. (2005). The new visibility. *Theory, Culture & Society, 22*(6), 31–51.

Uldam, J. (2014). Corporate management of visibility and the fantasy of the post-political: Social media and surveillance. *New Media & Society*, 1–19. doi:10.1177/1461444814541526

Wilson, D., & Serisier, T. (2010). Video activism and the ambiguities of counter-surveillance. *Surveillance & Society, 8*(2), 166–180.