International Journal of Communication 11(2017), 824-842 1932–8036/20170005

Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity

DAVID LYON
Queen's University, Canada

This article argues that to make sense of surveillance today, the concept of surveillance culture should be added to the conceptual tool kit. This goes beyond the important concerns of the *surveillance state* and *surveillance society* to examine how today's subjects make sense of, respond to, and—in some cases—initiate surveillance activities. Building conceptually on Charles Taylor's work, the concepts of surveillance imaginaries and surveillance practices are proposed as a means of analysis of how surveillance is engaged today. Previous studies have hinted at surveillance culture both explicitly and implicitly, but more is needed. This article explores further one illustrative dimension—that of online practices of *sharing*. These practices are seen, in turn, in relation to *visibility* and *exposure*. Finally, the concept of surveillance culture is shown to be relevant to current discussions ethics and of digital citizenship.

Keywords: surveillance, surveillance culture, online information, digital citizenship

An unprecedented surveillance culture is emerging. Its key feature is that people actively participate in an attempt to regulate their own surveillance and the surveillance of others. There is growing evidence of patterns of perspectives, outlooks, or *mentalités* on surveillance, along with some closely related modes of initiating, negotiating, or resisting surveillance. These I call *surveillance imaginaries* and *surveillance practices*, respectively. They are analytically distinguishable, but not separable. They shade into each other. This article discusses the reasons for focusing on the growth of surveillance culture as engagement; some of its key features, including, specifically, exposure; and how the surveillance culture concept enlarges previous debates about the surveillance state and surveillance society, and it facilitates the discussion of ethics and citizenship.

The term *surveillance culture* has appeared before, but it has yet to be treated as a broad phenomenon in its own right and theorized as a development distinct from others, such as *surveillance state* and *surveillance society*. William Staples (1998), for instance, used *surveillance culture* in a book title, exploring what he appropriately terms "postmodern" developments in our everyday interactions with surveillance. *Surveillance culture* also appears in John McGrath's subtitle to *Loving Big Brother* (2004), a study that helpfully indicates and discusses some of the performative dimensions of surveillance. Or think of Jonathan Finn'sinsights, with regard to camera surveillance in particular, about how, with the proliferation of public space cameras, surveillance has become a "way of seeing, a way of being" (2012, p. 78). Each provides a good springboard into surveillance culture.

David Lyon: lyond@queensu.ca
Date submitted: 2016–03–29

Take a current example of how surveillance culture relates to some pressing issues concerning surveillance in general. The kind of "suspicionless surveillance" carried out by intelligence agencies, such as the U.S. National Security Agency (NSA), to which Edward Snowden's disclosure of documents drew attention, cannot be understood simply in terms of older concepts such as surveillance state or surveillance society. They now have to be supplemented with a concept that focuses more on the active roles played by surveillance subjects, not least because those roles make a difference to the surveillance outcomes. I propose that surveillance culture is just such a concept and that focusing on what occurs within various aspects of surveillance culture helps to explain why the responses to Snowden—and to surveillance in general—have been so diverse: from outrage and political mobilization to buoyant reassurance or even complacency.

The culture of surveillance was becoming visible at the turn of the 21st century, especially after the 9/11 attacks on America and the advent of social media, and became even clearer after Snowden copied and released documents from the NSA in 2013. Historians may discern the first signs of surveillance culture in the later 20th century, but now it is present on a broad scale and its contours are becoming clear. What is meant by this term? It is the sense—as Raymond Williams (1958) might have said— that surveillance is becoming part of a whole way of life. Hence, my use of the word *culture*. It is no longer merely something external that impinges on our lives. It is something that everyday citizens comply with—willingly and wittingly, or not—negotiate, resist, engage with, and, in novel ways, even initiate and desire. From being an institutional aspect of modernity or a technologically enhanced mode of social discipline or control, it is now internalized and forms part of everyday reflections on how things are and of the repertoire of everyday practices.

The document disclosures of Snowden certainly brought some important debates into the foreground—questions of digital rights in relation to both corporations and government departments and agencies, and of who is responsible for flows of data across borders, flows that have clear consequences for life chances and freedoms (Kuner, 2014; Mosco, 2014). The disclosures also served to revitalize controversies over the role of online political activity that had surfaced widely a few years ago after the so-called Arab Spring. To what extent were the new media the means of fomenting popular and radical change, and to what extent were they the tools of repression and the denial of democratic aspirations?

These matters cannot properly be considered without first thinking more broadly about surveillance culture. That culture, in turn, must be seen in relation to the astonishing growth of what may fairly be called *digital modernity* in the 20th, but especially in the 21st century. Exploring the origins, carriers, and consequences of surveillance culture is a way of contextualizing more effectively the post-Snowden world. In what follows, I show that the presence of a surveillance culture raises fresh questions for everyday involvement with digital media, questions with ethical and political aspects that point to possibilities and challenges for digital citizenship. Both surveillance and citizenship are now mediated by the digital. What is the setting for this?

Surveillance Culture: The Context

Surveillance culture is a product of contemporary late-modern conditions or, simply, of digital modernity. From the later 20th century especially, corporate and state modes of surveillance, mediated by increasingly fast and powerful new technologies, tilted toward the incorporation of everyday life through information infrastructures and our increasing dependence on the digital in mundane relationships. Just as all cultural shifts relate in significant ways to social, economic, and political conditions, today's surveillance culture is formed through organizational dependence, political-economic power, security linkages, and social media engagement.

Let me contrast *surveillance culture* with previous terms and show why, on their own, they are now inadequate. *Surveillance state* worked well in the postwar Orwellian period and can still capture significant aspects of surveillance, such as the activities of intelligence agencies. But even there, the surveillance state is heavily dependent on commercial entities—Internet and telephone companies—to provide the desired data (Ball et al., 2015). Although such data have been used, via warrants, by police and security agencies for decades, the mass scale on which this now happens alters the dynamic. Today, no one is unaffected by this very post-Orwellian collusion of governmental and corporate forces. A second factor is that many of those data are themselves generated in the first place by the everyday online activities of millions of ordinary citizens. We collude as never before in our own surveillance by sharing—whether willingly or wittingly, or not—our personal information in the online public domain. Surveillance culture helps situate this. If this is state surveillance, it has a deeply different character from that which in popular terms is "Orwellian."

If the surveillance state is an inadequate concept, the equally commonplace idea of a surveillance society is also insufficient for the task. Although *surveillance society* helps to indicate the broader context within which the unsettling discoveries about the mass surveillance engaged by the NSA and the "Five Eyes" occur, it also falls short of explaining today's situation. Surveillance society is a concept originally used to indicate ways in which surveillance was spilling over the rims of its previous containers—government departments, policing agencies, workplaces—to affect many aspects of daily life. But the emphasis was still on how surveillance was carried out by certain agencies in ways that increasingly touched the routines of social life—from outside, as it were. This concept was often used in ways that paid scant attention to citizens', consumers', travelers', or employees' experience of and engagement with surveillance.

From the later 20th century onward, surveillance became a central organizing feature of societies that had developed information infrastructures, in which complexity was managed using categories (Bennett, Haggerty, Lyon, & Steeves, 2014; Ericson & Haggerty, 2000; Lyon, 2007). By the early 21st century, evidence was emerging of a "third phase" of computing, after the mainframe and personal computer phases, where computing machinery is embedded, more-or-less invisibly, in the environments of everyday life. Many refer to this as evidence for the "Internet of things," where the focus is on "smart" devices and objects capable of communicating with users and other devices. As we shall see, this extends in specific ways the reliance on surveillance as a mode of organization. Today's surveillance culture is informed by these developments.

Second, it is almost a truism to say that surveillance is also a major industry. Global corporations are involved, often with close links to government. The Snowden disclosures made this abundantly clear if there was any doubt previously. From the very start, in June 2013, the Snowden documents showed that the NSA has access to telephone company (Verizon) metadata and also mines the customer databases of Internet corporations such as Apple, Google, Microsoft, Amazon, and Facebook (often referred to as the "Big Five"). On the one hand, then, these corporations engage in large-scale surveillance of their customers. And on the other, they share these data with government agencies.

Moreover, the character of the corporation is also important for the relation between the political economy and the culture of surveillance. The Big Five corporations now dominate not only the Internet but also the economic mode of operation, which has moved beyond the managerial and financial modes of accumulation that characterized the later 20th and early 21st century. As understood by Shoshana Zuboff, the emerging phase is *surveillance capitalism,* now intimately involved with big data practices (Zuboff, 2015, 2016, Lyon 2014a). Its aim is to "predict and modify human behaviour to produce revenue and market control" (Zuboff, 2015, p. 75). Her analysis is based on Google's strategies that evidence a "formal indifference" toward its user base. For her, this has implications for what she calls "information civilization." These remarks are limited to the related idea of surveillance culture that seeks to grasp how users' responses to such attempted prediction and modification affects their success.

This means, in turn, that links with securitization are strong and pervasive. As David Garland observed, surveying the late 20th-century world of policing and governance, neoliberal governance flows naturally from this; what he called the "culture of control" is its leading motif (Garland, 2001). Risk management and security was already an important surveillance motif. But a formative opportunity for its expansion was offered by 9/11 and its aftermath, which, significantly, relied heavily on recently ailing technology companies to create a new industry of "homeland security" (Lyon, 2003). Thus, one of the key trends of recent surveillance has been securitization, applied in numerous and ever-growing and intensifying areas (Bennett et al., 2014). Such securitization demands greater amounts of information about risk and how to handle it, which both weakens traditional privacy requirements and increases surveillance of what are deemed risky behaviors. In terms of surveillance culture, this reinforces the sense that surveillance is warranted, "for our own good." In practice, of course, this is also understood ambivalently.

This sense of risk, and the need to take steps to reduce it, is not only evident on the grand scale of (inter)national policy but also penetrates daily life at home, where self-tracking for health, income, and time management is an increasing phenomenon. Only a few years ago, *The New York Times* still thought of this as something for geeks and keep-fit addicts (Wolf, 2010). Today, such self-monitoring is less unusual and often taken for granted. Wearable devices have become increasingly popular since the first decade of this century, and now, talk of the "quantified self" is much more commonplace (Crawford, Lingel, & Karppi, 2015). In this world, people seek a form of "self-knowledge" so that they can lead "better lives," even though only a small fragment of the data is seen by them, the vast majority of the data ending up in the databases of the wearable device corporations.

Finally, and perhaps best known, is the relation between social media and the surveillance

culture. I regard José van Dijck's work (2013, 2014) as exemplary here. Her book examines social media cultures, and the related article expands the argument to include questions of surveillance and privacy. It would seem that among the Snowden revelations, the realization by broad swaths of the public that what happens on social media is open to both corporation and government was one of the most striking. Van Dijck points out how this connects with "dataism," the secular belief—part of the surveillance imaginary, in my terms—that users can safely entrust their data to large corporations. Snowden put serious dents into dataism. Indeed, in the U.S. a recent study of Americans' main fears shows that being tracked by corporations or government is close to the top of the list (Bader, 2016). It would hardly be surprising if such findings do not have an impact in everyday uses of social media.

According to Pew Internet and American Life researchers, Snowden's disclosures have indeed had an impact on social media use (Rainie & Madden, 2015). For example, 34% (or 30% of all adults) of those aware of the government surveillance programs have taken at least one step to hide or shield their information from the government—changing privacy settings, using other communication media than social media, or avoiding certain applications. A slightly smaller proportion (25%) has changed their use of phones, e-mail, or search engines following Snowden. Knowing more about government surveillance produces more evidence of changed behavior**.**

Let me say one more thing about the contexts of the surveillance culture. Having noted its relation to organizational dependence, political-economic power, security linkages, and social media engagement, I should also observe that surveillance culture has many facets and varies according to region. The point of using the concept of surveillance culture is to distinguish it from notions such as surveillance state or surveillance society by focusing on participation and engagement of surveilled and surveilling subjects. But surveillance culture will, like any culture, develop differently and often morph unpredictably, especially in contexts of increasing social liquidity (Bauman & Lyon, 2013). It will, moreover, bud and blossom differently depending on historical and political circumstance. Most of what is said here refers primarily to North America and Western Europe, although readers in Asia, Latin America, Africa, or the Middle East will recognize many features of surveillance culture, necessarily inflected by local circumstances. With that said, let us consider the main features of surveillance culture and ask how these may be best analyzed.

Engagement: Imaginaries and Practices

Surveillance culture exhibits forms that are varied and constantly mutating, but they have some common features that we begin to explore. I refer to those common features in the singular as *surveillance culture,* which, despite the singular-sounding concept, is nonetheless multifaceted and complex. As an increasing proportion of our social relationships is digitally mediated, subjects are involved, not merely as the targets or bearers of surveillance, but as more-and-more knowledgeable and active participants. This occurs most obviously through social media and Internet use in general and has arguably intensified an everyday adoption of varied surveillance mentalities and practices.

There are two main aspects of this. One has to do with widespread compliance with surveillance. Although attempts to resist surveillance in certain settings are relatively commonplace, in most settings

and for most of the time, surveillance has become so pervasive that the majority comply without questioning it (Zureik, Stalker, & Smith, 2010). This general collusion with contemporary surveillance is something that puzzles those who have lived through the surveillance regimes of authoritarian governments (e.g., Bauman & Lyon, 2013). But as Lyon (2014) argues, such compliance may be explained by reference to three rather commonplace factors—familiarity, fear, and fun.

On the first, familiarity, surveillance has become a taken-for-granted aspect of life, from loyalty cards in the supermarket, to ubiquitous public and private space cameras, and to security routines in airports, sports arenas, and many other sites. This normalization and domestication of surveillance appears to account, in part, for the general level of compliance (Murakami Wood & Webster, 2009). As for fear, this has become more marked since 9/11, and it is apparent that the reported desire for surveillance measures relates to the ratcheting-up of uncertainty in a media-amplified exploitation of fear (Lyon, 2003). And at the opposite end of the emotional spectrum, fun also accounts for compliance, above all in the realm of social media and digital devices. Although they are integrated into "serious" life in many self-evident ways, for many users there are many leisure-time and "entertainment" aspects of the same systems. Anders Albrechtslund suggests that in these areas, surveillance may be "potentially empowering, subjectivity building and even playful" (Albrechtslund, 2008, p. 1). This underscores what Snowden said in a speech: "I *live* on the Internet" (2015, video).

The question of why certain populations would comply so readily with surveillance is important and has been rehearsed, but it does not tell the whole story by any means. The second and larger issue is why such populations might also participate in, actively engage with, and initiate surveillance themselves. The fact that the tools for such activities are increasingly available is part of the answer, but that can hardly be the whole story. After all, some tools are adopted and used while others are ignored and neglected. Additionally, the markets are volatile, especially in social media platforms, with some erstwhile leaders such as Facebook now losing customers to Instagram or Snapchat. As in other spheres, social engagement with new technologies cannot somehow be read off technological capacities or availability. These are sociotechnical phenomena.

Turning more specifically to the components of surveillance culture, I suggest that together the concepts of imaginaries and practices serve well to frame the discussion. Building on Charles Taylor's analysis of "social imaginaries" (Taylor, 2004, 2007) surveillance social imaginaries (or simply "surveillance *imaginaries*") have to do with shared understandings about certain aspects of visibility in daily life, and in social relationships, expectations, and normative commitments. They provide a capacity to act, to engage in, and to legitimate surveillance *practices*. In turn, surveillance practices help to carry surveillance imaginaries and to contribute to their reproduction.

Surveillance imaginaries are constructed through everyday involvement with surveillance as well as from news reports and popular media such as film and the Internet. They include the growing awareness that modern life is lived under surveillance, that this affects social relationships in many ways—for instance, Will my employer look at my antics on this Facebook page?—that the very idea of an expectation of privacy may be moot, and that everything from complacency to confrontation may be appropriate modes of responding to surveillance. Surveillance imaginaries offer not only a sense of what

goes on—the *dynamics* of surveillance—but also a sense of how to evaluate and engage with it—the *duties* of surveillance. Such imaginaries, in turn, inform and animate surveillance practices; the two belong together.

Surveillance practices may be both activities that relate to being surveilled (*responsive*) and also modes of engagement *with* surveillance (*initiatory*). Examples of the former, responsive practices, might include installing some form of encrypted protection from unwanted attention from national security agencies or marketing corporations, or wearing clothing that limits camera recognition in public places, or eschewing the use of loyalty cards. Examples of the latter, initiatory practices, on the other hand, might include installing a dash-cam to record the activities of other road users while one is driving, using social media to check up on personal details of others, including complete strangers, or indulging in self-surveillance through monitoring heart rates or calculating activity duration and intensity with devices such as Fitbits (often referred to as the "quantified self"; see above, p.4). As noted, these are analytical distinctions and some kinds of practices may include elements of each.

Exploring today's surveillance culture through the lenses of imaginaries and practices offers fresh ways of thinking about surveillance in general. It opens up a much more complex cultural landscape than can be captured with the concepts of surveillance state or surveillance society (though it does not supersede them) and simultaneously takes us beyond simple conceptual binaries such as power–participation, in/visibility, and privacy–publicness. As noted, for example, for many users of social media, despite popular perceptions to the contrary, privacy is still a valued condition, but so also is publicness (boyd, 2010).

It is worth reemphasizing that the term *surveillance culture* does not for a moment signify any unified or all-embracing situation. It is merely an umbrella term for many different kinds of phenomena that points to the reality of a "whole way of life" that relates, positively and negatively, to surveillance. The emphasis on imaginaries and practices already indicates the variety of phenomena that exists in this context. On the other hand, one can discern patterns, just as Michel de Certeau (1984) shows in *The Practice of Everyday Life*, where the major strategies of, say, consumption, are reappropriated in everyday situations. Within surveillance culture, people both negotiate surveillance strategies—for instance, often seeing the giving of personal data as a trade-off for personal benefit (Rainie & Anderson, 2014)—and also adopt them as their own, modifying them for their circumstances and initiating forms of surveillance on themselves and others (e.g., Trottier, 2012).

Sharing as Exposure

A key aspect of today's nascent surveillance culture is the imperative to share. Social media is in some ways synonymous with such sharing, and the theme has also been picked up in films and novels such as, classically, Dave Eggers's *The Circle* (2013), where it takes the form of a corporate—but also a coded, post-Orwellian slogan—"Caring is sharing." The connection with the corporate sector is crucial because this links it with the user-generated-content of Web 2.0 and the more general phenomenon of *prosumption*. From a corporate perspective, such prosumption and sharing is the *fons et origio* of the flowing floods of data on preference, habits, opinions, and commitments of digital technology users that

can be used for advertising or, perhaps more properly, the construction of consuming subjects (Turow, 2011). In this section we discuss some recent analyses of "sharing" that comport with the surveillance culture argument.

As Deborah Lupton (2015) observes, this may be theorized, critically, as a means of perpetuating neoliberal principles and as a central way in which corporations monetize content sharing and circulation. Moreover, it may mask ways in which classic consequences of capitalist practice continue in contemporary forms, creating discrimination and disadvantage for certain populations. At the same time, Lupton points to the ways that—in a similar vein to Albrechtslund—social media users enjoy creating content of all kinds and benefit from the feedback of other users, a process that helps to keep the whole system in motion, or in current usage, "spreadable." As she says, "The sharing subject seeks to recirculate content as part of their identity and participation in social networks and communities," believing that it will "have an impact on their networks" (Lupton, 2015, p. 30).

Sharing may also be thought of as an aspect of exposure (Ball, 2009), in which persons are made more visible by others or—and this is the relevant sense—deliberately make themselves more visible. Kirstie Ball explores "exposure" in terms of the "political economy of interiority"—in which institutions associated with technology, media, employment, and consumption create a demand or mobilize resources to focus on psychological states, or intimate behaviors. This is discussed further by Bernard Harcourt in his book *Exposed* (2015), which explores the ways in which the willingness to self-expose online has become a defining feature of our times. The issue of exposure has become far more widely discussed in the intervening years since 2009, as social media in particular became so central to social life.

Ball's leading concern is that subjectivity tends to be underplayed in the surveillance literature, in which subjectivity is often seen primarily in terms of oppression, coercion, ambivalence, or ignorance. Against this, she proposes that—at least—reflexivity, performativity, embodiment, and the psychoanalytic be brought more clearly into the picture. The fact that people may not actively resist or even question surveillance does not necessarily mean that they do not care about it, suggests Ball. You may hate the biometric camera at airport security, but you have to hide your feelings if you want to travel. There are many reasons why surveillance may be tolerated or even sought after, or why surveillance, negatively construed, may be seen as less significant in some situations than what are taken to be its positive benefits. The obvious example is engaging with social media or using loyalty cards even though users are aware of the ways that both corporate and government bodies may be tracking their activities.

In particular, Ball draws on John McGrath's (2004) work on performativity to explore how certain psychoanalytic dimensions of surveillance may be illuminated. McGrath insists that subjects of surveillance still make choices, however fleetingly, when "hailed" by the system in question. Experiences relating to, for example, reality TV, talent shows, or pornography place "a generic high value on the capture of authentic embodied experiences in a range of settings" (Ball, 2009, p. 645). Thus, through employment situations, new media, and biometrics, the political economy of interiority helps to connect "inner" and "outer" lives in various interconnected ways. Considering what *exposure* means in such contexts is the burden of Ball's work. While it may have negative connotations, such as vulnerability or abandonment, exposure may also be actively sought for pleasure or satisfaction.

Exposure, in surveillance contexts, occurs for various possible reasons. The institutions involved, whether in call centers, reality shows, or media portrayals of international "crises," wish to shape the responses of those employed or depicted without resorting to tactics that might thwart the authenticity of the subjects in question. Clearly, the emphasis on "authenticity" plays a crucial role. Subjects may in some sense be required to comply, but their active involvement means that their knowledge, desires, and expectations will form part of the outcome. So how is personal exposure legitimated in such contexts?

Various responses to this challenge exist, some of them noted by Ball. Gary Marx, for example, proposes that in relatively unintrusive "soft surveillance" situations subjects may be more willing to give up body data, whereas Frank Furedi adds to this by noting that the "confessional mode" of today's "therapy cultures" encourages public displays of vulnerability. Jodi Dean (2002) goes beyond this, pointing out that simply in order to be informed one must reveal more about oneself in the public domain—for example, in seeking online answers to questions of personal health. The public's "right to know" places high value on such publicity. Indeed, this can be generalized further, according to Dean, to the point of arguing that "uncovering secrets" is the key to a healthy democracy.

To consider the mushrooming phenomenon of exposure as a deliberate tactic is to acknowledge that there is more to "data subjects" than the reductionistic and passive position in which they are often found. Blind or bland user compliance should not be assumed by commentators or analysts. The realities of the lived body, rather than merely thinking of bodies as "reduced to information," should be kept in sight. Travelers going through airport security, for instance, may feel demeaned by the sense that the data-on-the-screen substitutes for their own narratives, but their lack of complaint may relate not to the unreality or unimportance of the negative experience, but rather to the fact that they are at the airport to fly—not speaking out at that point may just reflect their existential priorities at that moment (Saulnier, 2016).

It may also be that, in certain circumstances, the desire to be exposed could be seen as a mode of resistance. There are extreme cases of this, of course, one being the activities of Hasan Elahi, who informs the NSA—and anyone who goes to his website—of his movements, eating habits, and so on, 24/7. In the everyday world of exposure, however, surveilled subjects experience surveillance through a series of complex layers, each of which can be uncovered by surveillance. How institutions prompt different kinds of responses to surveillance is crucial—and complicated by the multifaceted character of the situations in which such surveillance is experienced. Not reducing the experience of surveillance to a one-dimensional or binary—"compliance or resistance"—format and acknowledging the variety and subtlety of responses helps us understand the lived realities of surveillance subjects.

"Desire" is also an important element inspiring exposure. As seen by Gilles Deleuze and Felix Guattari in *Anti-Oedipus* (1972, 2004), desire is not merely a response to lack but as a productive force. For Harcourt (2015), a social-media-saturated era—what he dubs a "digital frenzy"—encourages our knowing self-exposure or self-exhibition. He sees this as particularly true for younger people; the teens interviewed by danah boyd, for example, who believe that unless you're on social media "you don't exist" (boyd, 2014, p. 5). Today's situation, says Harcourt, is better described as the "expository society" than any of Debord's "society of the spectacle," Foucault's "disciplinary society" or Deleuze's "society of

control." However, he sees this as the outcome of our having become "numb to the risk of digital transparence" (Harcourt, 2015, p. 19). He emphasizes the ways that subjects have been "dulled" by things like self-centeredness, the illusion of free markets, militaristic homeland security, and overincarceration. Indeed, he writes that the "see-throughness of our digital live mirrors the all-seeingness of the penal sphere" (Harcourt, 2015, p. 21). Pleasure and punishment suffuse each other and work together.

Corporate surveillance, now working through social media, may be thought of as shaping current subjectivities. Harcourt also argues that this is a crucial new development, "replenished by our own curiosity and pleasure—retweeted, friended, shared and reposted (p. 50)," thus inserting surveillance capability into our everyday pleasures. Consumerism liberates the flows of desire, now seen in the digital. Whereas for Orwell, surveillance power was yoked to destroying desire and passion—"desire was thoughtcrime"—today these are the very enablers of digital exposure, the means of surveillance. Harcourt leans on Deleuze and Guatarri's dream of desire as a "machine" in which the unconscious is a productive factory. As assemblages of desire-producing machines, we are now linked with other machines—digital devices like iPhones, Facebook, and the Internet.

Such soft surveillance has today become commonplace and was at first seen as separate from harder, more coercive forms. However, during the first decade of the 21st century, the U.S. Department of Homeland Security (DHS) began to use social media for "harder" surveillance purposes, and by the second, "SOCMINT"—for "Social Media Intelligence"—had become a recognized part of security agencies' arsenal. Indeed, proposals were made by the DHS to demand social media information of travelers at border points (Gibbs, 2016). For Harcourt, desire is now in tandem with another mode of power, this time from Foucault's writing: not that of surveillance, but of security.

As in the theme park or the shopping mall, so now also with social media, sites of consumption are often the product of a private–public mix. They optimize the movement of consumers while minimizing labor and other costs (Andrejevic, 2007). Thus, for Harcourt, digital exposure becomes the "*wired* space of secure consumption" (Harcourt, 2015, p. 97). While biopower may be visible in some surveillance contexts, this postsecuritarian "expository power" focuses on all our little wants, desires, preferences, beliefs, ambitions, our individuality and differences, says Harcourt, to shape our digital selves.

Despite the focus on desire in Harcourt's work, one might be forgiven for thinking that in the end the chances for the development of active agency in the digital realm are downplayed if not remote. Exposure becomes once again something that appears to be primarily done *to* rather than *by* social media users. True, desire is in many ways directed powerfully by corporate–governmental alliances in the virtual realm. Nonetheless, in Harcourt's account, there exist forms of "leaderless resistance" that open up spaces for otherwise silenced voices within the digital realm. He is thinking of networked movements that gain strength from their communicating members rather than from strong central leadership. This, he asserts, requires of all a certain courage and conviction, an "ethics of the self" (Harcourt, 2015, p. 283).

The use of Foucault's work on the ethics of the self (in the *History of Sexuality*) is common to other writers in the field. Lupton points out that the ways in which people configure and represent

themselves on social media may be construed as ethical self-formation. As aspects of life are shared, so others express their approval or disapproval through "liking" or sharing the content more widely. This, arguably, is a self-reflective process in which many users participate and that may contribute not only to individual self-formation but also to the development of social norms and expectations (Lupton, 2015). To this we turn next.

Ethics: How to "Go On"

One aspect of a culture of surveillance is that it has an unavoidably evaluative dimension. Particularly the notion of surveillance imaginaries points toward the normative. Readers of Raymond Williams will recall that this, too, was a feature of his work; he lamented, for example, the reduction of ethical to technical concerns. The very idea of culture implies that questions of *how* to think, to behave, to act, to intervene are raised, within any given social imaginary. So if the particular slant of the imaginary is surveillant, then at least some hint of the ethics of surveillance will be present in the practices. Ordinary subjects need to know how to "go on" in the digital realm as awareness grows of the consequences of the widespread and multifarious uses of personal data within today's digital modernity. Everything from everyday rules of thumb, to more sophisticated shared responses, to surveillance tactics is emerging.

One way of considering this is to return to the notion of transparency, so central to novelist Eggers's plot in *The Circle*. The corporate campus of the Circle—the megacorporation that has swallowed up the Big Five into one gargantuan organization is itself dominated by glass buildings, all of which may be seen through. A new device has recently been issued to all employees; a "see-change" camera that hangs as a pendant from every neck. One of the corporate slogans is that "Everything that happens must be known," and the openness, the transparency of all that is going on is the means to that end. The novel prods and pokes at the transparency that has become a byword of the digital modernity's surveillance capitalism.

To discuss transparency, however, is to raise a deeper question of visibility. While transparency does provoke discussions of its limits—as *The Circle* makes plain—the more properly ethical questions arise over how we are made visible and how we make ourselves visible, or cloak our visibility. This becomes clear in Andrea Brighenti's pioneering work on visibility as a social process (Brighenti, 2007, 2010). Brighenti rightly argues that visibility is always relational: seeing and being seen are connected; asymmetries and distortions are common. Western thought privileges vision, but Brighenti observes that there is no "visible" without *ways* of seeing that are socially and even internationally crafted (Brighenti, 2007). Visibility, in this view, is associated with recognition, its struggles, and politics. Some disappear, are excluded; others become supervisible. Most of the time, our experiences come somewhere between the two. Visibility makes identification possible and breeds a culture of identification. But nothing can be taken for granted. Visibility does not correlate automatically with recognition or oppression.

Following Brighenti, Eric Stoddart explores visibility as a more illuminating way of considering surveillance than conventional "privacy"-based critique. His concerns with the latter are that privacy tends to emphasize individualistic aspects of visibility and rest on an inadequate notion of information. Instead, he proposes that "in/visibility" captures the dynamic of managing and negotiating visibility in social space.

As he discusses it, in/visibility is the attempt to control one's relative position within social space. In/visibility is active and is not predicated on withdrawal. It is engagement driven rather than defensive (Stoddart, 2011). In/visibility is cognizant of the social conditions on which it depends and in which we exercise skills that include evaluating those conditions. It is also aware of the resources at our disposal for making ourselves more and less visible for strategic purposes. At a small-scale level, this approach enables people to deal with multiple or fluid identities, while on a larger canvas, it challenges monopolistic power bases, foregrounding the question of which data should be available to whom, in which contexts and for how long.

Stoddart's aim is to find ways forward for an adequate ethics of surveillance, but it depends on a sophisticated analysis of what I am calling surveillance culture. The practices of in/visibility are a crucial part of what Stoddart calls a critical ethics of care and of self-transcendence. In this view, surveillance ought not merely to be *of* people (technologized risk; isolating privacy) so much as *for* people—and thus should be practiced carefully and held to account. This conclusion emerges from a critical account of rights-based privacy orientations and an embrace of a more discursive–"disclosive" approach that aims analytically to show what surveillance does or how it is practiced and offers possibilities for alternative actions. Privacy and rights are not so much abandoned, in this view, as seen as one—limited—way of considering the possibility of ethics for surveillance. His complementary approach "has the potential to disrupt fatalistic or protected models of surveillance that foreclose possibilities for critical response" (Stoddart, 2012, p. 376).

One readily acknowledges that there are many technological, political, and legal responses to surveillance, and the debates cannot be summarized easily. But it is safe to say that one thing largely—and regrettably—missing from many mainstream surveillance studies is any serious attention to ethics, or, it must be said, to the analysis of the implicit ethics of different strands of surveillance culture. Starting there, the pregnant possibilities of ethics—normative, contextual, disclosive, and relational—may be probed for fresh approaches that go beyond the technological determinist, the privacy preoccupied, or the complacent. In an era of apparently unbounded surveillance, in which the appetite for more data seems insatiable and the types of linked data seem unending, there are vital questions awaiting imaginative and contextually relevant ethical responses.

Such ethics, like morals, should not be seen as something abstract or disengaged, but rather something that prompts political agendas and action. The ethics of surveillance flow naturally into the politics of surveillance, in tune with today's technosocial and globalized conditions, informing and challenging current developments. The ethics and politics of complex surveillance situations present new challenges. Important though they are, regulation and law—even when based on some sound "rights" criteria—struggle in vain to keep up with the pace of change. Today, the need for both disclosive and normative ethics is greater than ever. Like Stoddart, I urge a kind of ethics that explores the actual consequences of surveillance cultures in everyday life, not just one that worries about specific harms, important though the latter still are from a legal point of view. Our sense of how institutional surveillance might be confronted, technologically, politically, legally and above all ethically is due for overhaul. Cultures of surveillance, whether critical or complacent, are socially constructed and can thus be challenged and reconstructed. But how?

Surveillance Culture and Beyond

It cannot be stressed enough that the issues discussed are not minor, transient, or contingent. Surveillance culture is one dimension of a highly significant social, technological, and political-economic transformation that is unavoidably imbricated with digital modernity. If surveillance culture can be understood as a matter of surveillance imaginaries and practices, then inevitably it prompts normative and ethical questions. As I argued earlier, these relate not just to matters of law and limits but also to what is appropriate in each context and what might enhance human life or enable human flourishing. The discussion is limited to one area of consideration of what is "beyond" surveillance culture—digital citizenship. It is indicative rather than systematic or comprehensive.

This article argues for a careful, critical, and *cultural* analysis of surveillance situations. It suggests that we go beyond common designations such as surveillance state and surveillance society. But it is also worth picking up a strand from the start of the article, that the Snowden disclosures are better understood if considerations concerning surveillance culture are drawn into the mix. More than one response to Snowden has insisted that we try to understand better the actual practices of the users of smart phones and the Internet to seek a practical ethics appropriate to today's situation (e.g., Bauman et al., 2014). Such are more likely to find traction in the complex liquid world of surveillance today.

The point of analyzing surveillance culture is to uncover not only the various kinds of imaginaries and practices of surveillance but also to understand how those lived Ies connect with ethical challenges—how to go on in daily, digital life. This is not to say that the analysis of surveillance culture is not worthwhile in its own right. It is—for a number of reasons, mentioned earlier. But such analysis may also contribute to other kinds of debates, especially those relating to privacy and data protection, and to those about social responsibility and citizenship in the time of digital modernity. Such debates are often marred by a failure to acknowledge how the very terms of debate have altered in the 21st century.

The practices that have emerged, for instance in the world of social media, are *social* practices, and the imaginaries that they inform and that shape them are equally *social*. For Taylor, social imaginaries incorporate "a sense of normal expectations we have of each other, the kind of common understanding that enables us to carry out the collective practices that make up our social life" (2004, p. 24). They are thus simultaneously factual and normative—people know how things go, but it is never disconnected from a sense of how things *ought* to go. That this is also true of what I call surveillance imaginaries is clear from the contexts within which, for instance, camera surveillance may be thought of as acceptable, or otherwise. Bathrooms are off limits, while cameras at traffic signals are often seen as legitimate. Helen Nissenbaum's work on contextual integrity, which stresses the malleability of privacy according to its setting, underscores this importance of context. Julie Cohen insists that academic and legal treatments often reduce privacy to technical and abstract matters whereas in fact our handling of information is always an embodied experience. Such lived experiences are vital, today, for the ways in which the self—also a key concern of Taylor's—is "configured" within digital networks (Cohen, 2012; Nissenbaum, 2009).

By the same token, they also have some unavoidably political aspects that implies some notion of citizenship. Debates over citizenship classically refer to membership and responsibilities within the nation-

state. But they may equally be thought of in terms of rights claims, or in terms of the kinds of responsibilities that are incumbent on those who are connected, in this case, digitally. Now, debates over digital citizenship have sometimes been rather limited—not to say idealistic—but as much of life is increasingly lived online, there is an urgent need to consider digital citizenship more broadly.

One recent study of digital citizenship that resonates well with the discussion of surveillance culture is Engin Isin and Evelyn Ruppert's *Being Digital Citizens* (2015), and this can be commended as a study that opens up emerging issues relating to participants' actual online behavior. The book is a unique collaboration that intermingles citizenship studies and digital studies. Its starting point is Foucault's insight that becoming citizens means being constituted as subjects of power—only now they enact themselves through the Internet both submissively and subversively. In the end, Isin and Ruppert ask the same kinds of questions that I have asked; in their words, "How do we conduct ourselves through the Internet?" (2015, p. 13).

This question cuts to the chase—or chases—of what digital citizenship might look like. On the one hand, there may be some urgent questions that have to do with teens interacting online: They often have clear ideas about what is and is not appropriate in their own communications with peers and in their relationships with parents and teachers (Steeves, 2006). On the other hand, other equally urgent issues concern how our online interactions should be handled in a post-Snowden environment. Bauman and others ask whether Internet users "will continue to participate in their own surveillance through self-exposure or develop new forms of subjectivity that are more reflexive about the consequences of their own actions?" (Bauman et al., 2014, p. 124). Much hangs, at very different levels, on how these issues are addressed.

Isin and Ruppert conclude that digital citizenship connects especially with what they call digital acts—legal, performative, and imaginary—and with rights to expression, access, and privacy—plus now, openness and innovation. They write of the many individuals and groups who are exemplars of digital rights activists and campaigners. But they also point to a much wider swath of persons who "live on the Internet" who engage in "dissensus" as well as promoting positive values online. They drive no wedge between those who make digital rights claims as they act on the Internet and those who work toward "bills, charters, declarations and manifestos" (Isin & Ruppert, 2015, p. 179), seeing the two in complementary fashion, much as was argued earlier, do practices and imaginaries. And while there may be important regional variations, the emerging figures who are digital citizens not only represent tradition but also a politics of a citizen to come.

Conclusion

This article argues that the concept of surveillance culture should be developed to understand more clearly the relations between contemporary surveillance and the everyday lives of those who might be described as its subjects. Using the work of Charles Taylor on "modern social imaginaries" as a springboard, it is suggested that two interrelated terms, *surveillance imaginary* and *surveillance practice* may be used to marshal analyses of how those immersed in the digital world (and beyond, of course; the focus here is on the communicational dimension of surveillance) conceive of and act in surveillance

contexts. Different experiences, for example, of fear, familiarity, and fun, may produce different outcomes in terms of compliance with institutional surveillance, whether governmental or corporate.

Taking this further, it is suggested that to grasp the ethical and political challenges of digital modernity, a concept such as surveillance culture is vital. Why? Because the dominant public and academic discourses about surveillance are couched in terms of the surveillance state or surveillance society. Neither of these is adequate today, not least because they tend to accent the viewpoint of the surveill*or*, the agent of surveillance, and often fail to give place to the ways that (what are called here) surveillance imaginaries and practices produce complacency, compliance, negotiation, or resistance.

This strategy of deliberately analyzing the surveillance imaginaries and practices of surveillance subjects is intellectually appropriate in that it attempts to grapple more realistically with contemporary digital realities as well as other, residual surveillance situations not directly mediated by the digital. But it also helps to connect with other significant debates about how to respond, for example, to the disclosures made by Edward Snowden about global, intensive, suspicionless surveillance. Legal and political approaches, seen for some time as sorely inadequate to the task of confronting contemporary surveillance, will benefit tremendously from trying to get to grips with the diverse lived experiences of those often lumped together as "users," as, for instance, the work of Julie Cohen, on the legal side, or Engin Isin and Evelyn Ruppert, on the political, clearly show.

Considering the significance of surveillance culture is a fruitful way of going beyond earlier analyses of the surveillance state or the surveillance society. Those concepts retain their salience for many situations, but are of limited value in providing a full-orbed understanding of today's surveillance—especially in the mainly online contexts discussed. Much more work will be needed to fill out this work satisfactorily, but I hope that this brief article will stimulate such endeavors.

References

Albrechtslund, A. (2008). Online networking as participatory surveillance. *First Monday, 13*(3). Retrieved from http://firstmonday.org/article/view/2142/1949/

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

Bader, C. (2016). America's top fears 2015. *The Chapham University Survey on American Fears*. Retrieved from https://blogs.chapman.edu/wilkinson/2015/10/13/americas-top-fears-2015/

Ball, K. (2009). Exposure: Exploring the subject of surveillance. *Information, Communication and Society, 12*(5), 639–-657

Ball, K., Canhoto, A., Daniel, E., Dibb, S., Meadows, M., & Spiller, K. (2015). *The privacy security state: Surveillance, consumer data and the war on terror*. Copenhagen, Denmark: Copenhagen

Business School Press.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology, 8*(2), 121–144.

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

Bennett, C., Haggerty, K., Lyon, D., & Steeves, V. (Eds.). (2014). *Transparent lives: Surveillance in Canada*. Edmonton, Canada: Athabasca University Press.

boyd, d. (2010, March 31). *Making sense of privacy and publicity*. Paper presented at SXSW conference, Austin, Texas. Retrieved from http://www.danah.org/papers/talks/2010/SXSW2010.html

boyd, d. (2014). *It's complicated: The social lives of networked teens*. New Haven, CT: Yale University Press.

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*. London, UK: Palgrave Macmillan.

Cohen, J. (2012). *Configuring the networked self: Code law and the play of everyday practice*. New Haven, CT: Yale University Press.

Crawford, K., Lingel, J., & Karppi, T. (2015). Our metrics, ourselves: One hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies, 18*(4/5), 479–496.

De Certeau, M. (1984). *The practice of everyday life*. Berkeley: University of California Press.

Dean, J. (2002). *Publicity's secret: How technoculture capitalizes on democracy*. Ithaca, NY: Cornell University Press.

Deleuze, G., & Guattari, F. (1972, ET 2004). *Anti-Oedipus: Capitalism and schizophrenia*. New York, NY: Continuum.

Dijck, J. van. (2013). *The culture of connectivity*. New York, NY: Oxford University Press.

Dijck, J. van. (2014). Datafictaion, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208.

Eggers, D. 2013. *The circle.* San Francisco, CA: McSweeney's.

Epstein, C. (2016). Surveillance, privacy and the making of the modern subject. *Body & Society*, *22*(2),

28–57.

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

Finn, J. (2012). Seeing surveillantly: Surveillance as social practice. In A. Doyle, R. Lippert, & D. Lyon (Eds.), *Eyes everywhere: The global growth of camera surveillance* (pp. 67–80). London, UK: Routledge.

Garland, D. (2001). *The culture of control: Crime and social order in conteporary society*. Chicago, IL: University of Chicago Press.

Gibbs, S. (2016, June 28). U.S. border control could start asking for your social media accounts. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/jun/28/us-customs-border-protection-social-media-accounts-facebook-twitter

Harcourt, B. (2015). *Exposed: Desire and disobedience in the digital age*. Cambridge, MA: Harvard University Press.

Isin, E., & Ruppert, E. (2015). *Being digital citizens*. London, UK: Rowman and Littlefield.

Kuner, C. (2014). *Transborder data flow regulation and data privacy law*. Oxford, UK: Oxford University Press.

Lupton, D. (2015). *Digital sociology*. London, UK: Routledge.

Lyon, D. (2003). *Surveillance after September 11*. Cambridge, UK: Polity Press.

Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge, UK: Polity Press.

Lyon, D. (2014). The emerging culture of surveillance. In A. Janssen & M. Christensen (Eds.), *Media, surveillance and identity* (pp. 71–90). New York, NY: Peter Lang.

Lyon, D. (2014a). Surveillance, Snowden and Big Data: Capacities, Consequences, Critique, *Big Data & Society* 1(1), 1-13.

McGrath, J. (2004). *Loving big brother: Surveillance culture and performance space*. London, UK: Routledge.

Mosco, V. (2014). *To the cloud: Big data in a turbulent world*. London, UK: Routledge.

Murakami Wood, D., & Webster, W. (2009). Living in surveillance societies: The normalisation of surveillance in Europe and the threat of Britain's bad example. *Journal of Contemporary European*

Research, 5(2), 259–273.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy and the integrity of social life*. Stanford, CA: Stanford University Press.

Rainie, L., & Anderson, J. (2014). The future of privacy. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2014/12/18/future-of-privacy/

Rainie, L., & Madden, M. (2015). America's privacy strategies post Snowden. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/

Saulnier, A. (2016). *Surveillance studies and the surveilled subject* (Doctoral thesis). Queen's University, Kingston, Canada.

Staples, W. G. (1998). *The culture of surveillance: Discipline and social control in the United States*. New York, NY: St Martin's Press.

Steeves, V. (2006). It's not child's play: The online invasion of children's privacy. *University of Ottawa Law and Technology Journal, 3*(1), 171–187.

Stoddart, E. (2011). *Theological perspectives on a surveillance society: Watching and being watched*. London, UK: Routledge.

Stoddart, E. (2012). A surveillance of care: Evaluating surveillance ethically. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *The Routledge handbook of surveillance studies* (pp. 669–676). London, UK: Routledge.

Taylor, C. (2004). *Modern social imaginaries*. Durham, NC: Duke University Press.

Taylor, C. (2007). *A secular age*. Cambridge, MA: Harvard University Press.

Trottier, D. (2012). *Social media as surveillance*. London, UK: Ashgate.

Turow, J. (2011). *The daily you: How the new advertising industry is defining your identity and your worth*. New Haven, CT: Yale University Press.

Williams, R. (1958). *Culture and society: 1780–1950*. London, UK: Chatto and Windus.

Wolf, G. (2010, April 27). The data-driven life. *The New York Times*. Retrieved from http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization.

Journal of Information Technology, *30*, 75–89.

Zuboff, S. (2016, March 5). The secrets of surveillance capitalism. *FAZ Feuilleton*. Retrieved from http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html/

Zureik, E., Stalker, L. H., & Smith, E. (2010). *Surveillance, privacy and globalization of personal information*. Montreal, Canada: McGill–Queen's University Press.