Surveillance & Society

Article

Criticising Surveillance and Surveillance Critique: Why privacy and humanism are necessary but insufficient

Sun-ha Hong

Massachusetts Institute of Technology, US.
sunha@mit.edu

Abstract

The current debate on surveillance, both academic and public, is constantly tempted towards a 'negative' criticism of present surveillance systems. In contrast, a 'positive' critique would be one which seeks to present *alternative* ways of thinking, evaluating, and even undertaking surveillance. Surveillance discourse today propagates a host of normative claims about what is admissible as true, probable, efficient—based upon which it cannot fail to justify its own expansion. A positive critique questions and *subverts* this epistemological foundation. It argues that surveillance must be held accountable by terms other than those of its own making. The objective is an open debate not only about 'surveillance or not', but the possibility of 'another surveillance'.

To demonstrate the necessity of this shift, I first examine two existing frames of criticism. *Privacy* and *humanism* (appeal to human rights, freedoms and decency) are necessary but insufficient tools for positive critique. They implicitly accept surveillance's bargain of trade-offs: the benefit of security measured against the cost of rights. To demonstrate paths towards positive critique, I analyse *risk* and *security*: two load-bearing concepts that hold up existing rationalisations of surveillance. They are the 'openings' for reforming those evaluative paradigms and rigged bargains on offer today.

Introduction

As the post-Snowden fallout continues, the debate on telecommunications surveillance[1]—academic and otherwise—is awash with criticism. The risks and harms of surveillance practices are flogged in open air each day. Yet this controversy should direct us towards an even more crucial problem: *what is an alternative to surveillance* (or: an alternative kind of surveillance)? How might we begin conceptualising a more beneficent surveillance? This essay is a normative assessment of the present state of surveillance criticism. Privacy and humanism—two presently dominant frames for criticism—are necessary but insufficient for thinking about 'another surveillance'. That debate must begin by redefining two concepts surveillance has co-opted for its own self-justification: risk and security.

[1] Surveillance today refers to an ever-growing panoply of practices. This essay focuses on electronic extraction of personal communications data by U.S. state agencies, and the controversy they have become subject to in the Snowden affair. I am concerned with how such surveillance is defined, defended, tested, justified; thus the analysis engages primarily with the discursive domain. It should become clear that I am addressing aspects of surveillance's rationality that are not unique to the NSA's activities, but widely applicable—in locally specific forms—to other national and technical contexts.

Hong, Sun-ha. 2017. Criticising Surveillance and Surveillance Critique: Why privacy and humanism are necessary but insufficient. *Surveillance & Society* 15(2): 187-203.
http://library.queensu.ca/ojs/index.php/surveillance-and-society/index | ISSN: 1477-7487

Surveillance's present notoriety makes this an opportune—and urgent—moment for such a debate. It has been argued that without Snowden, we would not have had such a public opportunity to influence what 'surveillance' means and entails (e.g. Drum 2014; Sargent 2014; Schulberg 2015). This is especially the case in the United States—yet the Snowden affair itself demonstrates the status of telecommunications surveillance, at least, as an object of international concern. Whatever the morality and legality of his actions, it is clear enough that the leaks have rendered the future of state surveillance a little less certain, a little more open for negotiation. For now.

Nevertheless, surveillance is equipped with its own kind of rationality, one which works to close up such windows of opportunity. These consistently insist on surveillance's *autonomy*—that is, its ability and right to internally justify its own scope, validity and efficiency. When the NSA implores the public that the sensible thing to do is simply trust the security experts and let the unknown lie undisturbed (Lizza 2013; Ackerman 2014), they are working towards a situation where surveillance justifies itself according to its self-created mechanisms of proof. This extends to surveillance systems' claim to their *strategic necessity*. Public Senate committee hearings are used to broadcast that the (Western) world has become more dangerous than ever before, requiring ever more expansive forms of surveillance (U.S. Senate Select Committee on Intelligence 2014). The Snowden leaks help attract proper scrutiny on exactly these schemas of justification, persuasion and validation.

But why 'another surveillance'? Alternatives matter because surveillance cannot simply be dismantled. As I elaborate below, surveillance fulfils many important functions for the modern state—and, no less importantly, provides us with affectively potent promises of safety and knowability. Identifying the present harms of surveillance is not enough: analysis must also consider how threats like terrorism should be addressed, and what different regimes of knowledge could be applied to evaluate surveillance more appropriately. For the sake of clarity, if at the cost of crudeness, this entails a movement from *negative criticism*, which focuses on the flaws and misdeeds of the status quo, to *positive critique*, which seeks to recolonise the discourse and values of surveillance—and thereby open the discussion towards thinking real alternatives.[2]

In what follows, I identify two major existing frameworks for surveillance commentary, *privacy* and *humanism*, and show why they are *necessary but insufficient*. Each offers an indispensable tool for criticising surveillance, but in doing so, enters into surveillance's own rationale, ultimately limiting their capacity for reform. Specifically, these values are too easily co-opted into surveillance's *bargain* of 'security or freedom': this renders criticism eligible for easy dismissal as part of the price we (must) pay for security. Next, I address *risk* and *security*—two concepts which help ground surveillance's self-justification—yet are themselves built on arbitrary foundations. I treat them as 'openings' towards an alternative surveillance. In other words, I explore ways in which they could be subverted, challenging the premises of surveillance's bargain and urging us towards a positive critique.

The Problem

But first, let us backtrack a little: is it true that we currently have no real alternative? And why is this even a problem, anyway?

[2] Of course, both terms emerge from the same root, κριτική, and are more or less synonymous in languages like French. Here, my usage is not intended to draw from a respectable heritage (such as Kant), but echo the present vernacular valence in English—where criticism in particular is often associated with, and itself criticised for, its destructive and negative tendencies. What I call positive critique, then, shares some (but not all) connotations with what we would typically call 'constructive criticism'.

While many scholarly, activist and other 'expert' voices have sought the dismantling or at least major reforms of surveillance, this project appears to face great difficulties. The system churns onwards, ever bigger and better, mouthing the words of Karl Rove: "when we act, we create our own reality. And while you're studying that reality, […] we'll act again, creating other new realities, which you can study too" (in Andrejevic 2013: 16-7). While the recent passage of the USA Freedom Act (a name well designed to trigger the conspiratorial reflex) took on the airs of significant reform, it is unlikely to make a fundamental difference in the state's ongoing surveillance activities.[3] Meanwhile, it is becoming more and more banal to write off values like 'privacy' as dead in the water; a newspaper column openly declares, "the war on privacy is already over" (Yaverbaum 2014). Certainly, such criticism and analysis are not wholly impotent, and remains an important part of public debate. Many studies (e.g. Turow, Feldman and Meltzer 2005; Turow 2012; Turow, Hennessey and Draper 2015) testify, for instance, to the American public's lack of specific knowledge about many surveillance practices and technologies. There is work to be done. But information is not a magic bullet. After all, Americans have been 'concerned' about surveillance and 'aware' of its problems for a very long time. Wiretapping was a consistent concern in the mid-20th century. Telegraph companies advertised their commitment to privacy (McMullan 2015). Benjamin Franklin suspected his mail was being opened in transit (Diffie and Landau 1998). As for digital surveillance, over 70 per cent of respondents in a 1991 *Time* survey reported they were 'somewhat' or 'very' concerned about personal information held in digital databases (Lacayo 1991; also see Poster 1995: 284). When the discourse in the Snowden debate recaptures, almost word for word, the warnings sounded a generation earlier, one wonders how much more effective it will be this time round.

It is an unintuitive problem: criticism finds it difficult to change the course of its object *even when it is recognised as sound*. But it is a familiar problem, as well. One directly relevant case is the history of technology as a discursive and ideological construct in the 20th century. In response to technology's rise to dominance as a master-trope of progress and prosperity, Jacques Ellul, Lewis Mumford, Herbert Marcuse and others produced widely influential tracts, inspiring a genre of technology criticism and skepticism that remains familiar today. Yet whether one looks at specific cases like reformist engineers in 1960s America (Wisnioski 2012), or more broadly at the rise of technical rationality in capitalist societies (Habermas 1970; Marcuse 1964), technology often continued to enjoy enormous authority as an autonomous force of progress. The case was made that the flaws of technology were part of the necessary price we pay, which ultimately cannot detract from its benefits. Further technological advances would, we were (are) assured, be able to address those problems with technology. All this sounds more than familiar. We are in a moment where criticism and debate regarding surveillance is perhaps louder than ever—without seriously threatening the claim that surveillance is necessary and *worth* its price. 'Negative' criticism has become *routine* to the continuing development of the surveillance society. Surveillance is used to the complainers: it's learned to live with it, and keeps plugging ahead.

Perhaps a more constructive way to say this is that negative criticism alone cannot respond to the alleged *benefits* of existing surveillance practices. Certainly, there is widespread acknowledgement that surveillance performs the critical function of social sorting (Bauman and Lyon 2013: 17; Gandy 1993), and that the subject today relies on surveillance for a sense of peace and to help mitigate the ontological insecurity of modernity (Bauman and Lyon 2013: 102; Giddens 1990). But such benefits are typically described by critics in couched and qualified terms. They are said to be promised but not actualised, and/or as not 'really' beneficial to the subjects. Surveillance criticism often adopts a false consciousness framework, and then seeks to explain why subjects accept surveillance in an act of 'voluntary servitude' (Pallitto 2013). It is

[3] Having prohibited one specific legal interpretation (Section 215) that had allowed bulk collection of telephone metadata from American sources, and enacted several other reforms, the Act left almost untouched vast areas of the state surveillance system created or expanded during the post-September 11 era. At an elementary level, the interception of 'foreign' internet communications which, due to the ways in which data infrastructure has been constructed over previous decades, continues to collect large volumes of domestic communications as well.

asked: how is it that subjects accept intrusions to privacy against their true interests? They must either be unaware of their exploitation, or tricked into a false approval of it. In contrast, what a positive critique attempts is to tackle surveillance's benefits head-on—sometimes by admitting them, sometimes by exposing them, sometimes by suggesting alternative means for their provision. This also means not making presumptions of subjects' political consciousness. Subjects may not always be 'fooled' by surveillance discourse, and they may not always choose privacy over surveillance when 'fully informed'. Surveillance's promises, its Reason, its worldview, cannot simply be 'exposed' for what they are, as if they will then disintegrate in the light of publicity. Whether metadata dragnets or phone tapping, its alleged benefits must be effectively addressed by critique.

We may now appreciate the gap between criticism and critique. A great deal of scholarly work on surveillance in the new century has tended to espouse and/or begin from a liberal, rights-oriented, anti-surveillance position. (This is also the case with much anti-NSA discourse in the media over the last two years.) The common analytical position is to gaze at surveillance with suspicion: 'what hidden misuses, what unintended evils, do you perpetuate behind your promises of safety?' The field has thus developed its own 'hermeneutics of suspicion' (see Leiter 2004). Certainly, the arguments of scholars like David Lyon are more complex than podium-thumping alarmism, and a work on surveillance is not any less intelligent or effective because it is against surveillance. What I am suggesting is that we must beware of a *default to criticism,* which risks preaching to the choir rather than reaching across to audiences who are more sympathetic to surveillance. Mark Andrejevic recalls that his students recommended to him the conspiracy documentary *Zeitgeist*—an intuition founded on the conspiratorial air he says they must have thought they detected in his arguments (Andrejevic 2013: 111). Yet when one seeks to speak to a matter of broad public concern, the position of the conspiracist is rarely the most effective one. Another symptom is Brian Massumi's gloves-off portrayal of George W. Bush and Karl Rove as surreal and aberrant manifestations of the New World Order. Where Al Gore "spoke in full sentences and read books", Bush knew instinctively that "facts are stupid things" (Massumi 2010). The key point is not even that Obama is as much part of the surveillance logic as Bush, but that the much-maligned Texan is made a frightening Other—an inherently *unreasonable* being who heralds a *Minority Report*-style future. Despite the quality of the analysis, one wonders how a Republican reader is to respond.

Žižek once argued that the Left today is paralysed in motion: an endless hamster's wheel of criticism. What the Left apparently forgot is that "the true triumph is not the victory over the enemy, [but] when the enemy itself starts to use your language, so that your ideas form the foundation of the entire field" (Žižek 2013). The subject of the Left aside, this is exactly the role that the surveillance regime plays today, and it is on this level that critique must operate if it is to properly audit its practices. A negatively critical opposition to surveillance can only offer a scattered, conspiratorial, cynical front, growing ever more biting and urgent, as if already dimly aware of its impending defeat. Positing the problem of an alternative to surveillance does not necessarily entail a presumption of surveillance as 'evil', or advocating the wholesale dismantling of surveillance systems. Rather, it involves an attempt to construct a more independent epistemic and moral position from which we can critique surveillance.

Limits

Here, I address two major perspectives in existing criticism: privacy and humanism. This is to demonstrate how such criticism is necessary, but *insufficient*, for a positive critique in their current form. This will allow us to then leverage relevant parts of those criticisms as we move forward.

Privacy

The concept of privacy remains a tried and true tool for effectively mobilising diverse resources and actors (Stalder 2011). Since its legal debut through Warren and Brandeis in the 1890s, privacy has been the default opposition to arguments for surveillance, security, transparency. Although the idea of privacy as an intrinsic good has developed in multiple directions since the Enlightenment, and has sometimes supported or at least

cohabited the rise of new surveillance practices (e.g. Rosen and Santosso 2013), this binary opposition is the most familiar one in surveillance debates today.

But even as we build up privacy as the great moral counterpart to surveillance, it is becoming apparent that we are making the privacy fight a battle it is no longer (or perhaps never was) equipped to win outright. It is increasingly clear that much of society, much of the time, has—tacitly or overtly—succumbed to the bargain offered by surveillance: personal information for promises of convenience and safety (see van Dijck 2013).[4] Felix Stalder (2002) has bluntly pointed out that although many will *report* (say, in surveys) that they value their privacy, they now concede its routine invasions knowingly. In cases like social media participation, many of us have determined the surrendering of personal information to be, by and large, *beneficial* to our interests. After all, within the present state of affairs, giving up some degree of privacy can provide *greater* individual autonomy and scope of action (Stalder 2011; also see Morozov 2011: 62). The loss of privacy is thus outweighed, in some contexts, by the fear of being isolated by the irrelevance of our secrets (see Bauman and Lyon 2013: 31). This is not to say that we have knowingly and happily jettisoned privacy; more often, privacy is slipping through our fingers unwillingly and unwittingly. Increasingly, the choice to 'opt out' of privacy-intrusive services becomes a non-option, the equivalent of social erasure (Hull 2015). A 'Faustian bargain' ties benefits and conveniences of a wired life inseparably to the loss of privacy (Zimmer 2008). Thus, a recent report shows that Americans do not voluntarily surrender privacy for corporate surveillance, but rather that they feel *resigned*: that is, they do not believe that privacy can reasonably be protected anymore, and grudgingly swallow the everyday proliferation of surveillance (Turow, Hennessey and Draper 2015). Both cases of happy concessions and resigned surrender reflect a wider problem. The information and arguments furnished by privacy are insufficient to mount effective resistance against both the coercions and temptations of surveillance.

One major reason that privacy-based criticism ends up fighting an uphill battle is that surveillance can typically fall back to the felt sense of *security* (and its moral legitimacy), and in doing so, depict privacy as a disposable luxury. Kelly Gates (2011) relates one specific example: a public controversy over smart CCTV implementation in Tampa, Florida in 2001. Where the ACLU and members of the public drew on Orwellian imagery to protest the invasion of privacy, a letter to the editor by an elderly 'Miss Benson' made the point quite clear:

> Too bad that a person cannot visit the shops and restaurants anymore without fear of being carjacked, raped, or killed. And now we have a modern invention that will curtail that activity. But wait! It may infringe on our precious 'rights.' I have rights, too. I have the right to go where I please in public without worrying about being harmed. And the police have the right to utilise modern inventions that will secure that end. The framers of the Constitution would hide their heads in shame to know what we have come to, when the rights of criminals are more protected than the rights of honest citizens. (Gates 2011: 90)

The 'right to be let alone' appears a relatively indulgent, bourgeois quibble when placed into such stark conflict with the 'right to be free from death and violence'. Similarly, the irony of the ongoing war on terror is that it is difficult to feel a *substantial and immediate* loss of privacy in most cases (unless one is subject to an extraordinary intervention, such as police questioning based on profiling). Meanwhile, the threat of terrorist attack is relentlessly impressed upon our minds as tangible and significant (see Taylor 2014: 48). It is in these senses that privacy is "functionally quite weak as a counter to the growth of surveillance" (McGrath 2004: 56). In its current form, privacy too often appears as a knee-jerk, neo-Luddite response with unclear benefits: a value which even in its original legal expression by Warren and Brandeis resorted to

[4] Indeed, we might interpret all this to say that the *pure* definition of privacy as absolute control over and restriction of personal information no longer seems to align with concrete situations; teenagers who seemingly disclose all sorts of personal details on social media are not necessarily abandoning all sense of privacy.

'mystical' expressions about the human soul (Rosen and Santesso 2013: 109), and today still pines after an ideal and fictional figure of the autonomous liberal subject (Cohen 2013). Meanwhile, as I will show later, surveillance is able to draw on security as an authorising value for innumerable partial intrusions and violations of privacy. Setting up a debate of privacy vs. surveillance is to persist in the face of a slippery slope, the momentum already in favour of surveillance's justifications.

Not only is privacy increasingly *inefficient* for the purposes of surveillance criticism, it is losing its own historically accumulated footing. The traditional (that is, Habermasian and Arendtian) public / private divide is undergoing rapid deconstruction in the surveillance context. Biometric and affective surveillance technologies rupture traditional boundaries of body, self and the world around it (e.g. Aas 2006; Adey 2009; Amoore and Hall 2009; Cheney-Lippold 2011; Schick and Malmborg 2010), contesting common sense definitions of what parts of this individual, or rather, Deleuzian dividual (Deleuze 1992), is reasonably eligible for privacy. The history of privacy as concept and its current difficulties have been well accounted elsewhere (e.g. Coll 2014). In our case, what these developments render problematic is the (non-)*alignment* between privacy as connoting certain ways of life and ways of being in the world, and privacy as a particular *state* of being secret, autonomous and 'free'. This conceptual confusion further weakens privacy's position, should it seek to contest claims made in the name of security. Privacy retains a powerful affective charge, but one that is in danger of becoming a skeuomorph of itself. To be sure, numerous scholars are attempting to refurbish the concept. However, many proposed reforms—such as Helen Nissenbaum's (2009) introduction of more fine-grained contextual specificity, or more general calls for individuals to 'control' their own data—do not fundamentally change privacy's weakness to arguments of security, though they may do good in other ways. Some have called for a more thorough overhaul of privacy into a social and collective good (e.g. Hull 2015). But until such nascent efforts yield more concrete notions, privacy remains fragile and conflicted in the face of surveillance.

Privacy is used today to construct an *antagonist* (or protagonist, depending on your point of view) in the struggle against surveillance; an 'another value' which contests the logic of safety above all else. However, its uncertain definition and historical position, as well as its vulnerability to the security justification, means that privacy as we know it is *necessary but insufficient* for a critique of surveillance systems.

Humanism

But privacy is just one dominant aspect of a wider set: a panoply of distributed arguments more or less grounded in liberal, humanistic values. For the sake of simplicity, let us use the label *humanism*: the appeal to human agency, human rights, dignity and decency, individual choice. These arguments rebel against surveillance logic's default to suspicion, and insist that protecting individuals' freedom is the morally laudable alternative to a surveillance society.

Take Harvey Molotch's *Against Security* (2012)—a work which is a useful exhibition of many common humanist arguments. Molotch argues that the ontological uncertainty which 'security' (promises to) alleviates and perpetuates induces the feeling that we must always 'do something'. In what has been elsewhere called 'actionism' (Hannah 2010), surveillance's advocates consistently argue that doing *something*—CCTV installations, pat-downs, shoe-scanners—must be better than doing nothing.[5] Molotch's response is that many of these technologies and practices are not nearly as efficient or helpful as they might pretend. In fact, their claim to efficiency is *unfalsifiable*: if a New York subway CCTV system has not yet

[5] One of the best examples of this tendency is what I have elsewhere called *fabrication* (Hong 2016a)*:* the FBI's actively helping suspects acquire the weapons, money, contacts and mental resolve to plot violent attacks in the name of Muslim extremist causes. Journalist Trevor Aaronson and others have shown that an increasing number of youths are being coaxed into providing sufficient grounds for their own arrest. In the absence of sufficient evidence or clear solutions, such techniques allow something *to be done*—even as the certainty of suspects' guilt becomes ever more uncertain.

obviously 'stopped' a single terrorist attack since 2005, does it mean that it was unnecessary in the first place? Or does it mean that it *must have* already stopped terrorist attacks that *could have* taken place in their absence? Perhaps sometime in the indefinite future, it will have justified itself by stopping an attack. As the references of the claims stretch out into the realm of potentiality (see Massumi 2007), conventional forms of falsification become impossible, and the assertion—'surveillance keeps *you* safe (alive)'—hangs indefinitely over the political arena. A similarly 'subjunctive', what-if logic is also prevalent in the Snowden affair. Then-director of the NSA, Keith B. Alexander, testified to PRISM's effectiveness by citing 'over 50' potential terrorist attacks stopped by the program (Landau 2013: 59; Ledgett 2014). Yet the details of most of these attacks were never released to the public, prompting even Senator Dianne Feinstein, at the time the most vocal defender of the NSA, to lament: "the instances where [PRISM] has produced good—has disrupted plots, prevented terrorist attacks, is all classified, that's what's so hard about this" (Knowlton 2013). On this basis, Molotch argues that "when you don't know what you are doing," or when you don't know what works, "the best approach is the more directly humane one" (2012: 192). He insists that measures like cleaner subways, relaxed and humour-friendly airport personnel and less restrictions on human movement will encourage humanity to do its own self-organising and self-monitoring work. This 'default to decency' is encapsulated by Molotch's use of an image of firefighters racing up the stairs (possibly to their deaths) in a crumbling World Trade Centre tower, while occupant citizens descend calmly and help each other (2012: 13-4).

The humanist argument here can boast a noble goal, and many individually credible arguments in its arsenal. Recall, however, the liberal-humanist leanings of Surveillance Studies in general, and the difficulty these narratives have in persuading those sympathetic to surveillance and security. Too often, *the success of humanist arguments depends on severely downplaying the objective benefits of surveillance*. Only in this way can Molotch, for instance, show that letting humans be may still be more 'effective' than the embarrassing obstacle course that airports have become today. Indeed, one of his final recommendations is, quite simply, to 'accept loss': accept that we cannot always 'do something' (2012: 221). This conclusion starkly demonstrates humanism's difficulty in addressing both the empirical gains in safety and the felt sense of security that surveillance promises. This makes humanism a *constraining factor* within the surveillance system, a moderating voice, rather than a truly autonomous alternative. Humanism remains susceptible to the same response technology presented its sceptics: 'we shall take your objections into account as we move forward with our newer and better systems'. Just as technology fixed technology, surveillance will fix surveillance.

Humanism seeks to produce an *'external'* critique of surveillance—that is, a set of values which subject surveillance to its own standards. But while humanism can mount an effective criticism of surveillance's current performance, it cannot adequately address surveillance's affective force, and the benefits it promises.

***

All this takes us back to the difficulties surveillance criticism faces today. The default to criticism strikes out at surveillance both present and future, actual and potential. On one hand, surveillance today is attacked for its misbehaviour, its undesirable side effects. On the other hand, the surveillance of tomorrow is feared for the excesses of its *primary* effects. Surveillance is thus condemned for both its successes and failures. But this is also precisely how analysis becomes limited to negative criticism. Not only does this encourage a blasé and resigned attitude, criticism becomes co-opted into surveillance's own frame of a 'bargain'. The insufficiency shared by privacy and humanism is that *they become articulable as costs, as the 'price' we pay for security*. Instead of undermining the equation itself (and its epistemological premises), criticism sustains it, and asks—where is the line? Shouldn't we give privacy or humanism more of the share? Yet this equation always presents surveillance with a winning hand. It simply needs to convince the public that new threats are just around the corner. It just needs a few more Miss Bensons, listing the litany of terrorist and criminal threats. After all, threats, as unrealised potential, are inexhaustible by definition. In this way we

arrive at Obama's initial defence of PRISM: "the modest encroachments on privacy […] was worth us doing" (*Wall Street Journal* 2013).

In a society which *knowingly* submits to surveillance's bargain of (apparent) security, it is no longer sufficient to merely inform the public or to repeatedly list its harms. We cannot merely assume that if only the public knew the 'truth', it would come to the conclusion that surveillance is not worth it or that it requires vigilant reform. A positive critique must begin by seeking ways in which surveillance's logic of self-justification may be broken down and subverted.

Openings

Logically, such reform could happen in two ways: external and internal. The first option is to introduce an external set of values and frames, and demand that surveillance systems not only fulfil their own standards for validity and efficiency, but tick all the boxes on this external end as well. Make profit all you like, but abide by environmental codes—and of course, the latter could not care less about the exigencies of the former (and vice versa). We have already seen the limitations of this approach in the case of humanism. Not only that, external frames, thanks to their very independence, constantly remain at risk of becoming irrelevant. The second option is to overhaul the very values and standards by which surveillance justifies itself; that is, the terms by which it depicts a world that always needs more surveillance. Here, I would like to pick out two load-bearing concepts which support the many rationalisations of surveillance. These are the stray threads, the points of contradiction, the 'openings', from which we might start the task of critique.

Risk

Risk is a concept of unparalleled importance to the reason of surveillance. It serves to legitimise surveillance practices of astonishing variety. It calculates their results and benefits into concrete figures. It furnishes the rhetorical bedrock on which almost every discursive defence of surveillance relies on. Surveillance thus invokes risk vis-à-vis urban design (Halpern et al. 2012); anti-terrorist measures (Andrejevic 2007); drone warfare (Gregory 2011); CCTV in public spaces (Molotch 2012); and even, via social media and users' mutual surveillance, the realm of human bonds (Bauman and Lyon 2013: 41). But what exactly does risk mean for the surveillance regime? Most concisely, it involves the *formalisation of uncertainty.* That which exists outside knowledge (uncertainty, indeterminacy) is crystallised into an ordered and manipulable form. In a similar sense, risk has elsewhere been described as a cultural 'translation' of danger (Douglas and Wildavsky 1982; Vaz and Bruno 2003: 282). The fundamental translation activity modern risk performs is a quantification of uncertainty, which produces risk as something that can be known, mitigated, increased and decreased, calculated (e.g. Porter 1995). Risk seeks to eliminate uncertainty by making it 'certain' in this way. At the same time, it is ontologically *dependent on* the existence of uncertainty, which it cannot help but reproduce (for more on the relation of surveillance and uncertainty, see Hong 2016b).

This double relationship yields the ontological irony of risk vis-à-vis security: despite my current state of safety, disaster is not only possible (in the sense of future occurrence), but in abeyance (Beck 1992: 51-3). My native city of Wellington, New Zealand, lies directly on the faultline of two massive tectonic plates. Popular belief goes that not only is a major earthquake likely to happen, it *should have happened already*. (And in 2016, two years after this passage was written, it did, hitting a 7.8 on the Richter scale.) The barely perceptible tremors which visit the city at frequent intervals are taken as reminders that the inhabitants live on borrowed time. A similar sense of ontological insecurity and existential anxiety (also see Giddens 1990: 92-100) pervades Miss Benson's earlier fear of 'being carjacked, raped or killed' at a restaurant, or even an individual who fears he/she is being watched by the NSA after learning of the Snowden leaks. In each case, a Damocles' sword over our heads. The difference is that most of us have filed away the first risk as "really existing but ignorable", while with the second (and perhaps the third), we have chosen to stay worried. So the belief in disaster-in-abeyance is constitutive of both anxieties we would normally consider 'reasonable' and those many might call paranoid. Yet the lines that divide the two are constantly under recalibration. Since the seminal publication of *Risikogesellschaft* in 1986, theorists like François Ewald (1993), and Beck

himself (2009), have described a rise in catastrophic risks: dangers which lie outside orthodox risk calculability, or even a society's ability to know in general (O'Malley 2004). As Dean (1998) and others point out, of course, there is no firm proof of any quantitative or qualitative change in the dangerousness of our world in realist terms. What is new is the way the unknown is resolved into (apparently) calculable forms.

In terms of surveillance and terrorism, we might call this emerging form *zero-degree risk*: a mode where the appearance of numerical risk is retained even as probabilities plunge to the point of negligibility, conflating calculation with speculation. Consider: in the wake of the Snowden leaks, some voices cautioned that all this might have been blown a little out of proportion; after all, the actual chance of dying from a terrorist attack in America was 1 in 20 million between 2007 and 2011 (Barrett 2013). Barack Obama was known for assuring both the public and his own staff that "the odds of people dying in a terrorist attack, obviously, are still a lot lower in a car accident" (Vickers and Leno 2013), or even falls in bathtubs (Goldberg 2016). But it is now common sense that the comparative rarity of a terrorist attack fails to correspond to its significance in the discourse of security. Even if there is only a 0.0002 per cent (insert as many zeros as you like) chance of stopping a terrorist, even if a surveillance program inconveniences or violates the rights of several million citizens to catch one terrorist, even if that program has not yet been found to 'stop' a terrorist… even then, it is all 'worth it' within surveillance's bargain, because of the sheer enormity of the risk-in-abeyance. When the 'what if' side of the equation is as catastrophic as September 11, the 'value' that each rights violation holds on the opposite side of the equation doesn't just decrease: it becomes unquantifiable. Actuarial reason might declare a certain individual 'worth' a certain monetary premium, but despite efforts to insure against terror (Aradau and van Munster 2007), the public debate in general can no longer balance such equations. Hence the 'zero-degree': the 'value' of a risk, and other factors in the risk equation, reaches the zero degree of mathematical indeterminacy.

Ironically, this means that when counterarguments to surveillance (such as privacy) are attributed a certain value or importance, this attribution becomes precisely the means by which they are fed into the zero-degree equation and rendered negligible. Surveillance practices are often justified on the bargain-claim that a certain amount of invasion of privacy, for instance, is 'worth it' for a certain amount of safety gained: we might recall Obama's aforementioned defence of PRISM. This implies lines in the sand, at least, where we could say surveillance *isn't* worth it. Yet this is not the case in the post-9/11 climate, where there is a constant emphasis on the calamitous enormity of even a single terrorist attack. When even a single error, a single oversight, could cause apocalyptic harm, surveillance becomes an emergency measure that can never be repealed. In this broken equation, surveillance has neither a proper 'fail-state' (where it is proven to be inappropriate) nor 'success-state' (where it can prove it has done the job). Its failure is always *provisional*, and its success can always be positioned as *just around the corner* (for an analogous case, see Halpern et al. 2012: 294). Surveillance's obsession with potential futures means its calculation of 'worth' and 'success' increasingly become indifferent to actualised cases of danger (Amoore 2011; Massumi 2007, 2010).

Still, even as the calculability of risk evaporates, and the term 'acceptable levels' becomes an oxymoron, surveillance continues to leverage the affective force invested in the language of risk. After all, 'acceptable levels', as we see in insurance industries, is always to some degree a 'symbolic tranquilizer pill' (Beck 1992: 64-9). Risk's mathematical veneer becomes indistinguishable from pure uncertainty, and instead of the refrain 'the risk is *too great*', we say instead, 'you never know for sure'. One great irony of the Snowden affair has been that this appeal to uncertainty has been made, in almost identical ways, by both sides of the debate. Edward Snowden cries, *J'accuse*: NSA surveillance programs trample upon people's rights. When asked why people who had 'done nothing wrong' should be concerned, he answers: "you're giving up your rights. Your rights matter because you never know when you'll need them" (Rowan 2014). Just a month earlier, James Clapper, Director of National Intelligence, had offered a parallel argument with paternalistic confidence: "I buy fire insurance ever since I retired, the wife and I bought a house out here and we buy fire insurance every year. Never had a fire. But I am not gonna quit buying my fire insurance, same kind of

thing" (Lake 2014). Zero-degree risk foregrounds the question of *belief* that is always constitutive of our comprehending risk. It exposes calculation as directed squarely at the incalculable (also see Amoore 2014). Yet this redundant exercise is nevertheless crucial in protecting and justifying surveillance practices. It also gives off the appearance of knowledge, enjoining us to *do something about it*. This is what Massumi (2010) identified in Bush's decisionism, and which we previously discussed as actionism. One does not dither and contemplate the specifics of danger, which cannot be clarified anyway; what is important is to do something about it with certainty,[6] and today, that 'something' defaults to surveillance.

What this approach exposes is the self-legitimating loop between risk and surveillance. Surveillance evacuates itself from external scrutiny. (This epistemological move has practical parallels, as well: the NSA's post-2003 strategy to create a closed and secret loop of legal affirmation, where it tells the FISA Court it has 'reasonable' suspicion and is thus cleared by law to pursue 'reasonably suspicious' cases.) The important question is how to not only criticise, but subvert this logic. Extending Molotch's humanist proposals, we might begin with a counterfactual: *isn't 'doing something' also a form of 'doing nothing'*, and vice versa? Given the collapse of comparative equations and calculative rationality, there is no necessary reason that new surveillance mechanisms will deliver any benefit above the status quo, or that the *dismantling* of existing systems will cause irreparable harm. 'Doing something' cannot be assumed to produce any consistent improvement in the chances of a socially desirable outcome. It is also worth remembering that the dominance of the 'doing something' argument in debates over surveillance and terrorism are contrasted elsewhere by the rising popularity of the precautionary principle in, say, issues of environmental sustainability. This all goes to show that the weight invested in the idea of 'doing something' is nothing more than word-play, a fraud upon our reason. Surveillance often entails a Herculean expense of resources and rights for a profoundly indeterminable difference. (The difference is indeterminable because the *object* that it makes a difference to—the risk equation—has itself become indeterminate.) A sprawling CCTV system certainly does *something* in response to a terrorist attack, but whether it does something *about* the terrorist attack is fundamentally unclear. Meanwhile, we have already mentioned the humanist argument that 'doing nothing' can actually enable latent resources like human goodwill and attention to act as instruments of surveillance and security. Doing something can sometimes stop other things being done, and it can certainly lead to harm and wastage.

Here is the irony. The humanist proposal is essentially that we should have subjects voluntarily aid the institutional goals of security, rather than institutions coercing unwilling subjects. In other words, biopower. In his genealogy of liberalism, Foucault defines its initial form as a minimal, frugal reason of government, where certain 'natural laws' (in this case, of the market) yield the 'truth' of governance (Foucault 2008: 28-32). Here, liberalism is built on the realisation that understanding subjects' interests and then letting them play out is the most *efficient* way to achieve government's own aims. It is this same logic which enacts the long historical passage from disciplinary power to societies of control (Deleuze 1992), and the rise of biopower. From this perspective, is not traditional surveillance—centralised, overburdened, data-obsessive, and caught in a furious archive fever of dubious utility—a primitive wastage of biopower? Is it not *inefficient* for surveillance's stakeholders—the government, the corporation, and even the public? The crudeness of the needle-in-a-haystack approach is well illustrated by the surveillance agencies' own rhetoric. Internal NSA memos refer to 'analysis paralysis', and the problem of drowning in data (Maas 2015). A decade earlier, the Information Awareness Office—the forerunner to the NSA surveillance programs that Snowden exposed—would produce what it literally called *big ass graphs* (BAG): a cacophonic overlay of surveilled communication networks that represented the enormity of their task (Harris 2010). Surveillance today may not be panoptic, but it certainly retains the most critical aspects of Foucaultian discipline (Foucault 1995): documentation, examination, gradation… all techniques by which an *external apparatus* works upon

[6] The American neo-conservative predilection for 'doing something' was replicated in their faithful ally, the UK Prime Minister Tony Blair. Faced with persistent criticism over his support of the United States in the Iraq War, he would argue: "would you prefer us to act, even if it turns out to be wrong? Or not to act and hope it's OK?" (see for example Blair 2004).

recalcitrant and uncooperative subjects to generate knowledge. Wasn't the whole point of control societies that we could divest of such behemoths? The alternative to 'doing something' is not to simply 'accept loss' or to become exposed to danger. It is about doing surveillance's job more effectively, and with less painful side effects.

In short, humanist aims should not be mutually exclusive with a sophisticated and powerful surveillance system. Instead of negotiating the surveillance regime's bargain, and its linear 'trade-off' between privacy / humanism and control / efficiency, it is a question of *improving* surveillance systems such that they might serve masters other than themselves, serve values other than the frenzied actionism of risk and security. Efficiency does not boil down to just catching the most terrorists; it also means a surveillance system that can identify danger *without* secretly undermining the nation's own constitutional values behind the public's back.

It is critical to distinguish this approach from what we typically associate with biopower forms of surveillance—that is, the *unwilling and unaware* exploitation of subject labour. Many such 'manipulative' applications are already commonplace. Some are perfunctory to the point of irrelevance; today, forlorn calls of 'look up, speak up' echo in the dismal underground subway stations of Philadelphia. Others, like the disclosure of personal information to third party trackers online, involve highly sophisticated systems of incentivisation. But such techniques typically eschew the subjects' consent or active participation, when they are not downright pernicious to the subjects' own interests. A superior long-term solution is a properly 'participatory' surveillance, wherein the benefits as well as harms of surveillance can be openly negotiated and audited.

Security

If risk denotes a specific 'input' (= translation of reality into the surveillance regime), security is the output. It is the concept through which surveillance's efficiency seeks to be assessed, and the discursive means by which it is justified. And this function, corresponding to the logic of zero-degree risk, exceeds the boundaries of concrete evidence. Even though we usually do not experience NSA wiretapping or third-party tracking directly, we understand it to be *probably already happening*, and on this basis 'feel' secure (and/or paranoid)—a 'what if' mentality I have elsewhere called *subjunctive* (Hong 2015).[7] All this renders security particularly resistant to challenge. If one should attack surveillance's claim to objective improvement in security, there remains the widespread sentiment that it is still better to 'do something'. If one challenges instead security as a good (for instance, with appeals to human rights and decency), the 'trade-off' discourse enters into play. The question here is how the notion of security can be divested of this self-legitimising loop, and subject to social scrutiny and evaluation that is not a game rigged in its favour.

One crucial articulation of security for the historical development of the state surveillance systems has been the term 'national security'. This term is neither as old nor venerable as it now appears, having emerged into prominence during Cold War America. James R. Schlesinger, U.S. Secretary of Defense in the 1970s, could already identify its 'incantatory power'—a term which seemed to defy precise definition as well as challenges to its moral authority (Mattelart 2010: 49). In the 1960s and 1970s, it was strategically redefined through public political discourse in order to admit drug trafficking (Diffie and Landau 1998: 78). Today, the specific definition of 'national security', especially when deployed in surveillance and privacy debates, remains unclear (see Taylor 2014). Even as the operative scope and political stakes of surveillance are more globally distributed and intertwined than ever, a mystification of the 'national' produces a distinctly patriotic articulation of security and freedom (Kaplan 2006: 694). Meanwhile, the term lives on in both the U.S.

[7] This does not imply a manipulated, ignorant or otherwise 'abnormally' crippled subject. Such belief is fundamental to *trust* in modern institutions, surveillance systems among them. After all, trust is *deciding to trust* in the absence of concrete certainty that I will not be betrayed (Weckert 2011). Or, in Luhmann's terms, trust is the mode in which one decides to *accept* a certain type and degree of uncertainty (in Giddens 1990: 32-6).

government's defence of its surveillance activities and its own bureaucratic language—from the NSL ('national security letter', issued by the FBI to force cooperation in its data collection) to, indeed, the National Security Administration. This is more than just a skeuomorphic retention of vocabulary. It reflects the expansion and legitimation of national security in juridico-legal processes. The U.S. Patriot Act is a classic case of the ratchet effect—"a unidirectional change in some legal variable that can become entrenched over time, setting in motion a process that can then repeat itself indefinitely" in legal interpretation (Givens 2013). Having been created as a response to a specific threat (of Al-Qaeda), the Act is now able to plead usefulness against a number of different purposes. Meanwhile, the law's very existence contributes to a public sense of crisis, encouraging an escalation that ultimately sediments as a 'new normal'. In effect, the law—and 'national security'—authorises itself on its own terms. This self-confirming tendency is at the heart of surveillance's reliance on security.

How to escape the loop? One way is to reformulate the grand bargain not as a trade-off between security and humanism, life versus rights, but two values that are incommensurable: the *security of way of life* on one hand, and the *security of life itself* on the other. These are not mutually exclusive, and it is certainly not a zero-sum game. The clunky terminology accentuates the crucial point that both 'sides' of the debate advocate some important form of security for our society. The security of way of life asks: how will you protect your ability to live a 'free' life, with minimal restrictions and scrutiny? How will you ensure your rights and privacy, but also the classical liberal values of freedom of expression and individual property (including one's own body and its information)? The security of life itself asks: how will you protect your body and property from physical harm and theft? One might suggest that little has changed, and the latter will invariably triumph over the former when push comes to shove. However, we know from the discussion of risk that security of life can never be completely achieved. Thus, it is impossible to absolutely privilege it—unless we literally prioritise it above every other good in our society at all times, and consign ourselves to permanent martial law in the face of danger and unrest. It is patently clear that our societies are not happy and willing to simply have one security trump the other.

This, it might be said, is mere discourse, fighting battles at the surface of phenomena. But just as the 'incantatory power' of national security helped effect a certain moral and ideological paradigm, a discursive intervention helps show that surveillance's one-sided fixation with crime and terrorism is already, in Agamben's language, normalising the exception (1995). The original formulation of the exception was reserved for the sovereign, who alone has the power to take *exception* to the law, and through this power guarantees the rule of law. When this exception becomes a regular and common state of affairs, it creates a space in which *anything* may be legitimised in the name of the now hollow law. Surveillance's dogged pursuit of the security of life legitimises the exception *for the cause* of life itself, but because it can never fully guarantee this security, it is pushed into its own kind of the ratchet effect: the securitised society, the 'banopticon' (e.g. Bauman and Lyon 2013), where surveillance becomes the new normal. Because physical survival becomes something to be defended at any cost, its defence becomes precisely the most powerful tool by which civil society and democracy can be undermined. The articulation of 'two securities' therefore begins by prising apart the conflation between surveillance activities and the protection of life itself. Its end is not simply to expose the socially constructed nature of security, but to arrange an explicit discussion of what kind of 'security' we *want to* construct.

***

These critiques of risk and security seek to problematise the epistemological basis of surveillance's reason, and direct that problem towards alternative formations and standards. They do so by prising apart surveillance's claims to *efficiency*, and by pushing surveillance to confront a broader definition of 'success'. There is little new in the suggestion that efficiency is a contextually specific construction with self-legitimating capacity. Every technological system builds its own localised definition of efficiency, which requires a political struggle to connect material technologies with particular pieces of scientific knowledge

(see Haggerty and Ericson in Gates 2011: 7). The history of surveillance is full of episodes in which locally specific notions of 'accuracy' and 'precision', as well as discursive and visual(ly spectacular) means for 'proving' them, had to be constructed (e.g. Gates 2011, 2013; Kaplan 2006). To take surveillance systems' presentation of their own efficiency at face value is to pass over its fundamentally ambiguous basis upon the zero-degree risk schema, and its one-dimensional standard of 'security'.

In short, efficiency is something that always can and should be disputed on an explicitly normative basis. Obama defended NSA practices by stating that "we will not apologise simply because our [intelligence] services may be more effective" (*New York Times* 2014). But what exactly does it mean for surveillance to be 'effective'? Are values like privacy and human rights external factors which impinge on and detract from surveillance's efficiency, or is their fulfilment also part of the 'efficiency' to which surveillance should aspire? A debate is necessary not only about whether surveillance is good or evil, whether it should be 'privacy or surveillance', but *what kind of surveillance*, assessed by what standard of efficiency, should be called 'good surveillance' in the first place.

Another Surveillance

I have not attempted to provide a full-fledged model for a concrete 'alternative' to surveillance. The 'openings' are intended to orient us towards that horizon and begin the conversation. Nevertheless, I should at least briefly address some potential objections, if only to justify the necessity of critique. First, is not a vision of truly 'participatory' surveillance simply helping fulfil surveillance in even more insidious ways? Certainly, my argument could be taken as an argument in favour of greater surveillance. But if a surveillance system could hypothetically address all the major humanist criticisms, then that would be a worthwhile thing to support. There is no moral high ground to be had in a blanket opposition to surveillance in the name of an amorphous freedom, just as national security should never be a trump card for authorising every kind of surveillance. It is true that any talk of 'better' or 'harmonious' surveillance has dangerous proximity to biometrics and other exploitative methods of self- / lateral surveillance. But the current period of heightened public concern over surveillance and state power offers an opportunity—one that perhaps will not come again for years—for a different paradigm of participatory surveillance to take root. There is a marked difference between a surveillance subject who is always-potentially criminal (and a body to be mined for data regardless of consent), and a subject who is most useful and least dangerous when he/she can be voluntarily mobilised for their own safety. We should make the attempt to theorise the conditions for *happy subjects* of a surveillance that actually serves their interests. The current dynamic, in which citizens are funnelled into a rigged bargain while surveillance is justified through secret and indeterminate proofs, risks becoming particularly dangerous in times when government fails to safeguard its own institutional and moral standards.

In the same vein, one might argue that the discourse of 'two securities' simply dresses up existing humanist criticism in different clothes. More fundamentally, it is clear that the two openings, as discussed here, are firmly ensconced within liberal humanist values writ large. My analysis can be accused of reproducing the narrow focus on the autonomy and freedom of surveilled citizens. In this essay at least, my goal was not to call for a different conception of personhood altogether, or of truly nonliberal frameworks—though such analysis will, too, become increasingly salient. It was rather to work with as much of the existing paradigm as possible, while still steering the discourse towards more positive forms of critique. Hence, the reorientation towards 'two securities' sought to specifically demonstrate, and embed into collective discourse, the point that opposition to surveillance also involves a form of security. The current surveillance regime should not be permitted to monopolise the meaning of the word. This pressures the surveillance regime to more concretely define what kind of security it provides, and to prove that it actually fulfils its promises. It is critical to find a way beyond the perennial justification, 'without surveillance, people will die', and the highway banditry of 'your life or your rights?' Losing security of life means vulnerability to physical death, which no scholar will ever have the moral right to belittle. But it is also true that without our

security of way of life, we would *merely live*: a bare life, helpless to the erosion of its political rights and to abuse by those in power.

Andrew Feenberg (1991) argued that the critical question is not 'technology or not', but 'what technology'; that it is necessary to think of 'another technology' which reaches across both the benefits of present technology and the possibilities it left behind in its historical development. In a world where surveillance seems increasingly ubiquitous, we must pursue the possibilities of 'another surveillance'.

Acknowledgements

The author would like to thank Carolyn Marvin, Lisa Parks, and the editors and reviewers of *Surveillance & Society*. An earlier version of this essay was also presented at the International Communication Association conference, 2015, San Juan, Puerto Rico.

References

Aas, Katja Franko. 2006. "'The Body Does Not Lie': Identity, Risk and Trust in Technoculture." *Crime, Media, Culture* 2 (August): 143–58.

Ackerman, Spencer. 2014. "Outgoing NSA Chief Keith Alexander Signals Openness to Surveillance Reform." *The Guardian,* February 27. http://www.theguardian.com/world/2014/feb/27/nsa-chief-keith-alexander-surveillance-reform.

Adey, Peter. 2009. "Facing Airport Security: Affect, Biopolitics, and the Preemptive Securitisation of the Mobile Body." *Environment and Planning D: Society and Space* 27 (2): 274–95.

Agamben, Giorgio. 1995. *Homo Sacer: Sovereign Power and Bare Life*. Stanford, CA: Stanford University Press.

Amoore, Louise. 2014. "Security and the Incalculable." *Security Dialogue* 45 (5): 423–39.

Amoore, Louise. 2011. "Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times." *Theory, Culture & Society* 28 (6): 24–43.

Amoore, Louise, and Alexandra Hall. 2009. "Taking People Apart: Digitised Dissection and the Body at the Border." *Environment and Planning D: Society and Space* 27 (3): 444–64.

Andrejevic, Mark. 2013. *InfoGlut: How Too Much Information Is Changing the Way We Think and Know*. New York: Routledge.

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

Aradau, Claudia, and Rens van Munster. 2007. "Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future." *European Journal of International Relations* 13 (1): 89–115.

Barrett, Richard. 2013. "Don't Turn Security into Theater." *CNN*, May 6. http://globalpublicsquare.blogs.cnn.com/2013/05/06/dont-turn-security-into-theater/

Bauman, Zygmunt, and David Lyon. 2013. *Liquid Surveillance: A Conversation*. Cambridge: Polity.

Beck, Ulrich. 2009. *World at Risk*. Malden: Polity Press.

Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity*. London: SAGE.

Blair, Tony. 2004. "Full Text: Tony Blair's Speech." *The Guardian*, March 5. http://www.theguardian.com/politics/2004/mar/05/iraq.iraq

Cheney-Lippold, John. 2011. "A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control." *Theory, Culture & Society* 28 (6): 164–81.

Cohen, Julie E. 2013. "What Privacy Is For." *Harvard Law Review* 126: 1904–33.

Coll, Sami. 2014. "Power, Knowledge, and the Subjects of Privacy: Understanding Privacy as the Ally of Surveillance." *Information, Communication & Society* 17 (10): 1250–63.

Dean, Mitchell. 1998. "Risk, Calculable and Incalculable." *Soziale Welt* 49: 25–42.

Deleuze, Gilles. 1992. "Postscript on the Societies of Control." *October* 59: 3–7.

Diffie, Whitfield, and Susan Landau. 1998. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press.

Douglas, Mary, and Aaron Wildavsky. 1982. *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. Berkeley: University of California Press.

Drum, Kevin. 2014. "If You Think the NSA Debate Has Been Valuable, You Have Edward Snowden to Thank." *MotherJones,* January 2. http://www.motherjones.com/kevin-drum/2014/01/if-you-think-nsa-debate-has-been-valuable-you-have-edward-snowden-thank

Ewald, Francois. 1993. "Two Infinities of Risk." In *The Politics of Everyday Fear*, edited by Brian Massumi, 221–28. Minneapolis, MN: University of Minnesota Press.

Feenberg, Andrew. 1991. *Critical Theory of Technology*. Oxford: Oxford University Press.

Foucault, Michel. 2008. *The Birth of Biopolitics: Lectures at the Collége de France, 1978-79*. Edited by Michel Senellart. Translated by Graham Burchell. Basingstoke: Palgrave Macmillan.

Foucault, Michel. 1995. *Discipline and Punish: The Birth of the Prison*. Translated by Alan Sheridan. New York: Vintage Books.

Gandy, Oscar. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press.

Gates, Kelly A. 2013. "The Cultural Labor of Surveillance: Video Forensics, Computational Objectivity, and the Production of Visual Evidence." *Social Semiotics* 23 (2): 242–60.
Gates, Kelly A. 2011. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: New York University Press.
Giddens, Anthony. 1990. *The Consequences of Modernity*. Cambridge: Polity Press.
Givens, Austen D. 2013. "The NSA Surveillance Controversy: How the Ratchet Effect Can Impact Anti-Terrorism Laws." *Harvard National Security Journal*. http://harvardnsj.org/2013/07/the-nsa-surveillance-controversy-how-the-ratchet-effect-can-impact-anti-terrorism-laws/ .
Goldberg, Jeffrey. 2016. "The Obama Doctrine." *The Atlantic*, March 10. http://www.theatlantic.com/magazine/archive/2016/04/the-obama-doctrine/471525/#article-comments.
Gregory, Derek. 2011. "From a View to a Kill: Drones and Late Modern War." *Theory, Culture & Society* 28 (7-8): 188–215.
Habermas, Jurgen. 1970. *Toward a Rational Society: Student Protest, Science, and Politics*. Boston: Beacon Press.
Halpern, Orit, Jesse Lecavalier, Nerea Calvillo, and Wolfgang Pietsch. 2012. "Test-Bed Urbanism." *Public Culture* 25 (2): 273–306.
Hannah, Matthew G. 2010. "(Mis)adventures in Rumsfeld Space." *GeoJournal* 75 (4): 397–406.
Harris, Shane. 2010. *The Watchers: The Rise of America's Surveillance State*. New York: The Penguin Press.
Hong, Sun-ha. 2016a. "What If / Fabrications." *Sunhahong.org*. https://sunhahong.wordpress.com/2016/08/07/what-if-fabrications/.
Hong, Sun-ha. 2016b. "Data Epistemologies / Surveillance and Uncertainty" (PhD diss., University of Pennsylvania, 2016). http://repository.upenn.edu/edissertations/1766/.
Hong, Sun-ha. 2015. "Subjunctive and Interpassive Knowing in the Surveillance Society." *Media and Communication* 3(2): 63-76. DOI: 10.17645/mac.v3i2.279.
Hull, Gordon. 2015. "Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data." *Ethics and Information Technology* 17(2): 89–101.
Kaplan, Caren. 2006. "Precision Targets: GPS and the Militarization of U.S. Consumer Identity." *American Quarterly* 58 (3): 693–714.
Knowlton, Brian. 2013. "Feinstein 'Open' to Hearings on Surveillance Programs." *New York Times,* June 9. http://thecaucus.blogs.nytimes.com/2013/06/09/lawmaker-calls-for-renewed-debate-over-patriot-act/?_php=true&_type=blogs&_r=0.
Lacayo, Richard. 1991. "Assaulting Our Privacy: Nowhere to Hide." *TIME,* November 11. http://content.time.com/time/subscriber/article/0,33009,974234,00.html.
Lake, Eli. 2014. "Spy Chief: We Should've Told You We Track Your Calls." *The Daily Beast*, February 17. http://www.thedailybeast.com/articles/2014/02/17/spy-chief-we-should-ve-told-you-we-track-your-calls.html.
Landau, Susan. 2013. "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations." *Spotlight* (July/August): 54–63.
Ledgett, Richard. 2014. "The NSA Responds to Edward Snowden's TED Talk." *TED 2014*, March 20. http://www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk.
Leiter, Brian. 2004. "The Hermeneutics of Suspicion: Recovering Marx, Nietzsche, and Freud." In *The Future for Philosophy*, edited by Brian Leiter, 74–105. Oxford: Clarendon Press.
Lizza, Ryan. 2013. "State of Deception." *New Yorker*, December 16. http://www.newyorker.com/magazine/2013/12/16/state-of-deception.
Maas, Peter. 2015. "INSIDE NSA, OFFICIALS PRIVATELY CRITICIZE 'COLLECT IT ALL' SURVEILLANCE." *The Intercept*, May 29. https://firstlook.org/theintercept/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/.
Marcuse, Herbert. 1964. *One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society*. Boston: Beacon Press.
Massumi, Brian. 2010. "The Future Birth of the Affective Fact: The Political Ontology of Threat." In *The Affect Theory Reader*, edited by Melissa Gregg and Gregory J Seigworth, 52–70. Durham: Duke University Press.
Massumi, Brian. 2007. "Potential Politics and the Primacy of Preemption." *Theory & Event* 10 (2) https://muse.jhu.edu/article/218091. DOI: 10.1353/tae.2007.0066.
Mattelart, Armand. 2010. *The Globalization of Surveillance: The Origin of the Securitarian Order*. Cambridge: Polity Press.
McGrath, John E. 2004. *Loving Big Brother: Performance, Privacy and Surveillance Space*. London: Routledge.
McMullan, Thomas. 2015. "The World's First Hack: The Telegraph and the Invention of Privacy." *The Guardian*, July 15. http://www.theguardian.com/technology/2015/jul/15/first-hack-telegraph-invention-privacy-gchq-nsa?CMP=ema_565.
Molotch, Harvey Luskin. 2012. *Against Security: How We Go Wrong at Airports, Subways, and Other Sites of Ambiguous Danger*. Princeton, NJ: Princeton University Press.
Morozov, Evgeny. 2011. "Whither Internet Control?" *Journal of Democracy* 22 (2): 62–74.
New York Times. 2014. "Obama's Speech on N.S.A. Phone Surveillance." January 17. http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html?_r=0.
Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.
O'Malley, Pat. 2004. *Risk, Uncertainty and Government*. London: Glasshouse Press.

Pallitto, Robert M. 2013. "Bargaining With The Machine: A Framework For Describing Encounters With Surveillance Technologies." *Surveillance & Society* 11 (1/2): 4–17.

Porter, Theodore M. 1995. *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton, NJ: Princeton University Press.

Poster, Mark. 1995. "Databases as Discourse, or Electronic Interpellations." In *The Second Media Age*, 78–94. Cambridge: Polity Press.

Rosen, David, and Aaron Santesso. 2013. *The Watchman in Pieces - Surveillance, Literature, and Liberal Personhood*. New Haven, CT: Yale University Press.

Rowan, David. 2014. "Snowden: Big Revelations to Come, Reporting Them Is Not a Crime." *Wired*, March 18. http://www.wired.co.uk/news/archive/2014-03/18/snowden-ted.

Sargent, Greg. 2014. "Yes, We Have Snowden to Thank for NSA Surveillance Debate." *The Washington Post*, January 2. https://www.washingtonpost.com/blogs/plum-line/wp/2014/01/02/yes-we-have-snowden-to-thank-for-nsa-surveillance-debate/.

Schick, Lea, and Lone Malmborg. 2010. "Bodies, Embodiment and Ubiquitous Computing." *Digital Creativity* 21 (1): 63–69.

Schulberg, Jessica. 2015. "The Elephant In The Room: Senators Finally Credit Edward Snowden For Role In Patriot Act Reforms." *The Huffington Post*, June 1. http://www.huffingtonpost.com/2015/06/01/snowden-nsa-patriot-act_n_7485702.html.

Stalder, Felix. 2011. "Autonomy beyond Privacy? A Rejoinder to Bennett." *Surveillance & Society* 8 (4): 508–12.

Stalder, Felix. 2002. "Opinion. Privacy Is Not the Antidote to Surveillance." *Surveillance & Society* 1 (1): 120–24.

Taylor, Nick. 2014. "To Find the Needle Do You Need the Whole Haystack? Global Surveillance and Principled Regulation." *The International Journal of Human Rights* 18 (1): 45–67.

Turow, Joe, Michael Hennessy, and Nora Draper. 2015. "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up To Exploitation." Philadelphia. https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

Turow, Joseph. 2012. "The Disconnect Between What People Say and Do About Privacy." *Journal of Law The Post* 2 (1): 479–82.

Turow, Joseph, Lauren Feldman, and Kimberly Meltzer. 2005. "Open to Exploitation: America's Shoppers Online and Offline." A Report from the Annenberg Public Policy Center of the University of Pennsylvania, Philadelphia. http://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers.

U.S. Senate Select Committee on Intelligence. 2014."Current and Projected National Security Threats Against the United States." Washington D.C. http://www.intelligence.senate.gov/hearings/open-hearing-current-and-projected-national-security-threats-against-united-states#.

van Dijck, José. 2013. *The Culture of Connectivity: A Critical History of Social Media*. New York: Oxford University Press.

Vaz, Paulo, and Fernanda Bruno. 2003. "Types of Self-Surveillance: From Abnormality to Individuals 'at Risk'." *Surveillance & Society* 1 (3): 272–91.

Vickers, Debbie, and Jay Leno. 2013. "The Tonight Show with Jay Leno." USA: NBC. https://www.youtube.com/watch?v=jOW0Z2Czgzk.

Wall Street Journal. 2013. "Transcript: Obama's Remarks on NSA Controversy." March 14. http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/.

Weckert, John. 2011. "Trusting Software Agents." In: *Trust and Virtual Worlds: Contemporary Perspectives*, edited by Charles Ess and May Thorseth, 89–102. New York: Peter Lang.

Wisnioski, Matthew H. 2012. *Engineers for Change: Competing Visions of Technology in 1960s America*. Cambridge, MA: MIT Press.

Yaverbaum, Eric. 2014. "The War on Privacy Is Over." *The Huffington Post*, March 13. http://www.huffingtonpost.com/eric-yaverbaum/the-war-on-privacy-is-ove_b_4949429.html.

Zimmer, Michael. 2008. "The Externalities of Search 2.0: The Emerging Privacy Threats When the Drive for the Perfect Search Engine Meets Web 2.0." *First Monday* 13 (3). http://firstmonday.org/ojs/index.php/fm/article/view/2136/1944.

Žižek, Slavoj. 2013. "The Simple Courage of Decision: A Leftist Tribute to Thatcher." *New Statesman*, April 17. http://www.newstatesman.com/politics/politics/2013/04/simple-courage-decision-leftist-tribute-thatcher.