Media and Communication
Open Access Journal | ISSN: 2183-2439
Volume 3, Issue 3 (2015)

Special Issue

Surveillance: Critical Analysis and Current Challenges (Part II)

Editors

James Schwoch, John Laprise and Ivory Mills

COGITATIO

Media and Communication, 2015, Volume 3, Issue 3
Special Issue: Surveillance: Critical Analysis and Current Challenges (Part II)

Published by Cogitatio Press
Rua Fialho de Almeida 14, 2º Esq.,
1070-129 Lisbon
Portugal

Available online at: www.cogitatiopress.com/mediaandcommunication

Table of Contents

COGITATIO

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 3, Pages 1-11
Doi: 10.17645/mac.v3i3.263

Article

Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance

Christopher Parsons

Citizen Lab, Munk School of Global Affairs, University of Toronto, Toronto, M6K 3R8, Canada;
E-Mail: christopher@christopher-Parsons.com

Submitted: 23 March 2015 | In Revised Form: 16 July 2015 | Accepted: 4 August 2015 |
Published: 20 October 2015

Abstract
This article begins by recounting a series of mass surveillance practices conducted by members of the "Five Eyes" spying alliance. While boundary- and intersubjectivity-based theories of privacy register some of the harms linked to such practices I demonstrate how neither are holistically capable of registering these harms. Given these theories' deficiencies I argue that critiques of signals intelligence surveillance practices can be better grounded on why the practices intrude on basic communicative rights, including those related to privacy. The crux of the argument is that pervasive mass surveillance erodes essential boundaries between public and private spheres by compromising populations' abilities to freely communicate with one another and, in the process, erodes the integrity of democratic processes and institutions. Such erosions are captured as privacy violations but, ultimately, are more destructive to the fabric of society than are registered by theories of privacy alone. After demonstrating the value of adopting a communicative rights approach to critique signals intelligence surveillance I conclude by arguing that this approach also lets us clarify the international normative implications of such surveillance, that it provides a novel way of conceptualizing legal harm linked to the surveillance, and that it showcases the overall value of focusing on the implications of interfering with communications first, and as such interferences constituting privacy violations second. Ultimately, by adopting this Habermasian inspired mode of analysis we can develop more holistic ways of conceptualizing harms associated with signals intelligence practices than are provided by either boundary- or intersubjective-based theories of privacy.

Keywords
critical theory; democracy; Habermas; intelligence; national security; privacy; surveillance; telecommunications

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

1. Introduction

The Snowden revelations have shown the extent to which American, Australian, British, Canadian, and New Zealand signals intelligence agencies operate across the Internet. These agencies, collectively known as the "Five Eyes" (FVEY), have placed deep packet inspection equipment throughout telecommunications networks around the world to collect metadata and content alike. They have engaged in sophisticated signals development operations by intruding into non-public commercial and government networks to access, exfiltrate, and modify data. Their operations are so deeply integrated with one another's that it is challenging, if not impossible, to analyze one member without analyzing them all a single group. The breadth of these signals intelligence agencies' activities has called into question whether they are intruding on the privacy of people all over the globe, including the privacy of their own citizens.

This article begins by recounting of a series of mass surveillance practices conducted by the FVEY agencies. These practices reveal the extent of the FVEY agencies' surveillance activities which, in aggregate, exceeds the

surveillance capabilities of any particular corporation or single state. Next, the article engages with how boundary- and intersubjectivity-based theories of privacy register harms associated with the FVEY members' signals intelligence activities. Whereas boundary-based theories can account for some of the harms experienced by targeted individuals they are less able to register harms associated with the surveillance of global populations. In contrast, theories focused on the intersubjective characteristics of privacy register how capturing the global population's electronic metadata weakens the bonds needed for populations to develop the requisite relationships for fostering collective growth and inclusive lawmaking. However, these intersubjective theories of privacy are less capable of responding to individual harms than liberal theories of privacy. Ultimately, neither of these approaches to privacy are holistically responsive to legally-authorized mass surveillance practices conducted by the FVEY nations.

The concluding sections of this article argue that privacy ought not to be used as the primary critique of the FVEY agencies' mass surveillance practices given the deficiencies associated with liberal and intersubjective privacy theories. Instead, critiques of signals intelligence surveillance practices can be grounded on why these practices erode boundaries between the public and private spheres, to the effect of eroding the autonomy that underpins democratic processes and institutions. The erosion of these boundaries may be registered as privacy harms or—more broadly—as intrusions on communicative and association rights that are essential to democratic models of government. These intrusions are made worse by the secrecy of the laws and rulings authorizing the FVEY's surveillance practices. The paper ultimately argues that a Habermasian grounded critique can identify privacy harms, but as symptoms of broader harms. Moreover, in adopting a Habermasian approach to critiquing the FVEY agencies' practices we can readily identify how such surveillance has normative consequences beyond national boundaries, offers a more robust way of thinking about legal challenges to such surveillance, and clarifies how communications rights offer a way to critique and rebut unjust surveillance practices.

2. Mass Surveillance, Unmasked

The Snowden archives reveal the breadth of surveillance undertaken by members of the Five Eyes alliance, which is composed of the Signals Intelligence (SIGINT) agencies of the United States (NSA), United Kingdom (GCHQ), Canada (CSE), New Zealand (GCSB), and Australia (DSD). The FVEY members use their geographic positions and technical proficiencies to massively collect information about the global population's use of electronic communications, to target specific persons and communities, and to retain information about "non-targeted" persons for extensive amounts of time. The implications of such surveillance are taken up in subsequent sections, when analyzing the effectiveness of individual and collective theories of privacy to respond to these modes of surveillance, as well as when analyzing how a Habermasian critique of surveillance more holistically accounts for harms linked to the aforementioned surveillance practices.

The FVEY alliance collects communications data from around the world at "Special Source Operations", or SSOs. Some surveillance programs associated with SSOs temporarily store all communications traffic routed to these locations. These communications are also analyzed and filtered to pick out information that is expected to positively contribute to a SIGINT operation. A Canadian program, codenamed EONBLUE, operated at over 200 locations as of November 2010 and was responsible for such analyses. Other agencies, such as DSD, may also have used the EONBLUE program (CSE, 2010). Similarly, the United States runs deep packet inspection surveillance systems that parallel some of EONBLUE's capabilities (Gallagher, 2013a; Bamford, 2008). In the case of the United Kingdom, GCHQ's TEMPORA program monitors at least some data traffic passing into and out of the country (MacAskill, Borger, Hopkins, Davies, & Ball, 2013). All of these countries share data they derive from SSO-located surveillance programs in near-real time; no single alliance member can effectively detect and respond to all of the Internet-related threats that are directed towards any of these nations, nor can they comprehensively track the activities of individuals around the world as they use telecommunications systems without the FVEY agencies pooling and sharing their collated data. The very capacities of the "national" programs operated by each of these member nations are predicated on accessing information collected, processed, analyzed, and stored by other member nations' collection and analysis programs.

Content and metadata alike are stored in the FVEY nations' databases. Stored content includes, for example, the content of encrypted virtual private network communications (NSA, 2010), email messages (Risen & Lichtblau, 2009), and automatic transcriptions of telephone calls (Froomkin, 2015). In contrast, the metadata databases store cookie identifiers, email addresses, GPS coordinates, time and date and persons involved in telephony events, IP addresses used to request data from the Internet, and more (Ball, 2013; Geuss, 2013; CSE, 2012b). Data stored in the content and metadata databases can be used to target specific persons or systems or networks. Such targeting operations can either involve establishing new "selectors", or communications characteristics, that promote either the automatic attempt to compromise the communications device in question or a set of more active efforts by analysts to deliver exploits to devices using more manual techniques. In the case of the NSA, it may rely on the Tai-

lored Access Operations (TAO) unit to fire "shots" at targets. These shots are meant manipulate targets' internet activity to divert targets from the legitimate websites that they are trying access towards websites the NSA has compromised to install malware, or "implants", on the target's device (Parsons, 2015; Weaver, 2013, 2014). Targets can also be selected to receive implants using alternative methods depending on the technical proficiency and value of the target and security of their devices; equipment shipments can be interdicted in transit (Gallagher, 2014), USB drives deposited in places where the target individual or someone they are a digitally associated with may find them (Gallagher, 2013b), or network equipment that are used by contemporary or possible future targets are mapped for later infiltration or exploitation (Freeze & Dobby, 2015). In all of these cases, an individual's communications privacy is violated in order to mount a signals intelligence operation against the individual vis-à-vis their devices.

SIGINT agencies also develop communications association graphs to identify groups and group relationships. Agencies may more closely monitor or disrupt a given group's communications if they are regarded as a hostile threat or target. Being associated with "hostile" groups can involve being just three "hops" away from a person of interest to one of the SIGINT agencies (Ackerman, 2013). Actions taken against groups can include targeting key communicating members with "dirty tricks" campaigns, revealing whether a person views pornography (and what kind), exposing groups to "false flag" operations, or preventing communications from routing properly (Greenwald, 2014; Greenwald, Grim, & Gallagher, 2013). Little is known about the specifics of such operations, though documents pertaining to the GCHQ and CSE and the NSA indicate a willingness to engage groups as well as individuals in the service of meeting the SIGINT agencies' goals. In all of these cases, a group's or population's communications are captured and mapped against one another's and thus the collective's communicative privacy interests are engaged. Notably, such association mapping can take place even if no specific member of the group is actively targeted by a FVEY member; the mapping can occur automatically as algorithms make associations between different communicating parties based on data collected at SSOs.

Information that is collected from SSO locations can become "useful" if a previously-untargeted person, kind of communication, or group(s) becomes noteworthy following a post-collection event. As examples, an individual's telecommunications-related activities may be analyzed in depth months or years after the activities have actually occurred. Such analyses may be triggered by accidentally communicating with a person who is targeted by a FVEY agency, by innocently using a communications method that is also used by persons targeted by the FVEY agencies, or simply by error. The result is that past activities can be queried to determine the relative hostility of a person, their intentions, or their past activities and communications partners, and without a person being able to rebut or contextualize their past behaviours. They are effectively always subject to secret evaluations without knowing what is being evaluated, why, or the consequences or outcomes of the evaluations undertaken by FVEY agencies' intelligence analysts.

In aggregate, the FVEY agencies are engaged in the mass collection of electronic communications data and can collect information from around the world because of their alliance. This data is collected regardless of whether any given person or group is of specific interest to any particular FVEY member, and can be used to target specific persons or to understand the communications habits of large collections of people. The content and metadata of communications, alike, are analyzed and often retained. Even if collected information is not immediately useful it can be drawn upon months or years later. The result of this surveillance is that the world population's communications are regularly collected, processed, stored, and analyzed without individuals or groups being aware of how that information could be used, by whom, or under what terms and conditions. As discussed in the next section, such surveillance raises privacy issues that neither boundary- nor intersubjective-based theories of privacy can holistically respond to.

3. Privacy Interests of the Subjects of SIGINT Surveillance

The targeted and generalized SIGINT surveillance undertaken by the FVEY agencies intrude upon individuals' reasonable expectations of privacy. Such intrusions occur regardless of whether a human analyst ever examines the captured data or deliberately intrudes into a person's communications devices. Theories of privacy based on concepts of boundaries or of intersubjectivity can be brought to bear to partially capture the unreasonableness or illegitimacy of targeted and generalized surveillance. As will become evident throughout this section, however, neither conceptual approach captures the full ramifications of such surveillance.

Privacy is perhaps most commonly thought of as a boundary concept, which rests on the conception that autonomous individuals enjoy a sphere within which they can conduct their private affairs separate from the public sphere of the government. This concept is rooted in liberal democratic theory where individuals are at least quasi-rational and need to be "free from" government interference to develop themselves as persons who can then take part in public and private life (Bennett & Raab, 2006, p. 4; Mill, 1859). This concept of privacy can be subdivided into a series of boundaries:

- spatial boundaries that see privacy "activated" when a space such as the home is viewed by an agent of government or unauthorized citizen (Austin, 2012; Warren & Brandeis, 1890)
- behavioural boundaries identify activities that are meant to be secured from unwanted attention, such as sexual behaviours or medical matters or other "intimate" activities including those of the mind (Allen, 1985; Mill, 1859)
- informational boundaries can identify kinds of information that are deserving differing levels of protection, such as information pertaining to one's sexuality, religion, and increasingly between the content of communications versus the metadata associated with that content (Millar, 2009; Strandburg, 2008; Rule, 2007)

Concepts of privacy boundaries underwrite data protection and information privacy laws, which are themselves meant to "allow individuals rights to control their information and impose obligations to treat that information appropriately" (Parsons, Bennett, & Molnar, 2015). However, for any of the boundary concepts to be "activated" and potentially register a privacy harm a specific individual must be affected by the surveillance: this means that evidence of an intrusion, or likely intrusion, is required to determine whether an individual's privacy has actually been violated. So, how might boundary concepts of privacy be squared against the FVEY agencies' massive collection of metadata identifiers and the same agencies' broad targeting of kinds of communications?

A central challenge of determining if a violation has occurred is whether "personal" information has been monitored or captured by a third-party. Defining "personal information" can be "a contradictory maze between what privacy regulators ascribe as personally identifiable, what individuals understand as identifiable, and what the companies operating themselves" (Parsons et al., 2015) perceive as requiring legal protection, to say nothing of how SIGINT agencies define it. In the latter case, as an example, the collection of data about the devices used by individuals is semantically and legally separated from the collection of, or targeting of, the individuals using those devices themselves (Plouffe, 2014) despite the same data being collected in both situations. While legal claims asserting a violation are often based on a demonstrable infringement or likely infringement it may be impossible for individuals to demonstrate a clear violation given the secrecy of the FVEY agencies' activities.

The massive collection of data at SSOs enables the FVEY agencies to subsequently retain huge amounts of metadata. Metadata is important because, "[w]hen there is metadata, there is no need for informers or tape recordings or confessions" (Maas, 2015). In other words, metadata itself can "out" the individual and their associates. However, despite metadata's capability to enable the surveillance of persons as well as populations, it is unclear whether the capture of such data types necessarily constitutes a violation of a person by way of collecting personal information on a per-metadata record basis: is it the case that the capture of metadata only registers a violation when a sufficient degree of information is captured? And, if so, how can that subjective evaluation based on competing interpretations of how much metadata is personal be arrived at, such that a common ruleset can be established to identify if a violation has occurred? These questions are routinely asked of corporations involved in the processing of metadata and gain increased weight when the data could be used to trace the activities of persons and their devices across their daily lives, around the world, to meet states' national security objectives.

Boundary concepts of privacy can be squared, to an extent, against the massive collection of metadata identifiers by clarifying the conditions under which personal privacy is intruded upon by the collection. Metadata databases are used to store cookie identifiers, IP addresses, email and social media logins, and other pieces of data that, when combined, can reveal that particular identification tokens were used to access services across the Internet. SIGINT analysts can run tests against stored data to ascertain whether they *can* correlate metadata information with that of individuals and, where they need additional information, can make requests for program enhancements or the broader collection of information to identify the individuals or their devices (Israel, 2015). Many of the tests are designed to abstractly ascertain how to answer questions—such as can the analyst identify specific kinds of phones using particular networks and, subsequently, link identifier information with those phones for more targeted analysis—and which may never be put into practice. However, the intent driving the collection—to potentially target individuals—means that even if a person does not actually become targeted the collection of data is designed to place them in a persistent state of prospectively-being targeted. The result is that metadata is not "less identifying" than the content of a communication, nor that absent specific targeting a person does not suffer a privacy violation. As a result of being always in a potentially-targeted category, individuals may alter their behaviours to try to secure their telecommunications from third-party monitoring. Such alterations may cause individuals to suppress their autonomy in order to appear unobtrusive (Cohen, 2000) to government monitors without ever knowing what constitutes *being* obtrusive.

Where a person's communications have been deliberated targeted by a SIGINT agency it is relatively easy to register an individual harm: their personal communications device, or communications environments, are compromised with the intent to influence

or affect the individual based on what is discovered. Though there may be gradients associated with the intrusion, insofar as some modes of targeting specific persons reveal more or less sensitive information, a "boundary" is crossed by merit of monitoring spaces, activities, or kinds of information that individuals or their communities are receiving and transmitting. Of course, such intrusions may be justified—a legitimate national security threat may justify the intrusion—but regardless of the terms of justification an intrusion is experienced.

In contrast to boundary theories of privacy, intersubjective theories of privacy focus on how privacy is principally needed to strengthen community and facilitate intersubjective bonds. Privacy, on an intersubjective account, is about enabling social interaction. Regan argues that privacy is "less an attribute of individuals and records and more an attribute of social relationships and information systems or communications systems" (Regan, 1995, p. 230) on the basis that privacy holds: a common value, something that we all have an interest in; a public value, as essential to a democratic system of government; and a collective value, or a non-divisible good that cannot be allocated using market mechanisms. In effect, Regan situates privacy as something that cannot be exchanged or given up in the market on the basis that privacy is a common inalienable right or good. Valerie Steeves shares Regan's position and demonstrates this when arguing that privacy must be "understood as a social construction through which "privacy states" are negotiated" (Parsons et al., 2015; Steeves, 2009). As a negotiated good, privacy is never any one person's but instead possessed by the parties implicitly and explicitly involved in the social construction. Steeves' work echoes Schoeman's, who argued in part that protecting autonomy should not be bound up in boundary concepts of privacy because autonomy is about being able to develop new, deeper, and enhanced relationships (Schoeman, 1992). So for these theorists, efforts to individualize privacy or empower individuals to protect their privacy are the results of misinterpreting the concept of privacy and its social purpose.

So, on the one hand, intersubjective theories of privacy are concerned with how privacy is a common value that is needed to enable the actions of individuals situated in communities. On the other, scholars such as Nissenbaum focus on privacy as constituting "a right to live in a world in which our expectations about the flow of personal information are, for the most part, met; expectations that are shaped not only by force of habit and convention but a general confidence in the mutual support these flows accord a key organization principles to social life, including moral and political ones" (Nissenbaum, 2009, p. 231). Here social norms derived from the communities individuals find themselves within are used to determine what is an inappropriate intrusion into personal activities. Nissenbaum uses her term, "contextual integrity", to parse out whether an intrusion has occurred. Integrity is preserved when informational norms are respected and violated when the norms are breached. Where parties experience discomfort or resistance to how information is collected, shared, or analyzed the discomfort is predicated on a violation of context-relative information norms; thus contextual integrity operates as a benchmark for privacy (Nissenbaum, 2009, p. 140). The norms that can be violated are themselves developed based on force of habit amongst persons and their communities, their conventions, as well as a "general confidence in the mutual support" of information flows that "accord to key organizing principles of social life, including moral and political ones" (Nissenbaum, 2009, p. 231). However, Nissembaum tends to veer towards norms built into law when contested norms arise. She does so based on an argument that legally-established norms are more likely to be widely accepted in a given society because judges are ultimately responsible for determining whether the contextual integrity linked with a given informational norm or practice infringes on an individual's reasonable expectation of privacy within a broader social context (Nissenbaum, 2009, pp. 233-237).

Nissenbaum's mode of settling contestations between norms is problematic for several reasons. First, new technologies routinely bring norms of privacy into flux. The consequence is that individuals are often challenged in negotiating norms amongst themselves (Turkle, 2012) and judges are not necessarily aware of how new technologies are, or may be, shaping norms of information control. Second, the groups within a nation-state may hold differing normative accounts of what should constitute a reasonable expectation of privacy based on their lived experiences or cultural backgrounds; thus, while a law may hold that disclosing information to a third-party immediately reduces a person's privacy interest in the disclosure, the same position may not be held by members of society who possess different understandings of privacy (Timm, 2014). There is no guarantee that a judge's or judiciary's normative stance on any given privacy issue is necessarily representative of the social norms adopted by the parties involved in the disclosures in question. Third, there is the issue that signals intelligence-based surveillance transcends national boundaries: which norms should be appealed to when vast segments of the entire world's communications are potentially being aggressively monitored? It seems unlikely that judges of national legal systems will enjoy a sufficiently expansive mandate, let alone capability, to settle infringements on contextual integrity that involve all the world's populations which are under the FVEY agencies' surveillance. Forth, when it comes to national security issues, judges may be reluctant to scrutinize these issues or oppose state positions for fear of the judgement ultimately facilitating a subsequent violent

event against citizens of the nation-state (Chandler, 2009). Combined, these problematics can impose conservative or nationalistic understandings of social norms of privacy that are out of character with the actual norms maintained by significant proportions of national and global populations.

At their core, intersubjective theories of privacy are attentive to the bonds that are responsible for forming and maintaining the communities in which individuals develop and act within: these theories take seriously the nature of humans as community-based creatures and the theories acknowledge the conditions needed for community and (by extension) individual flourishing. In other words, these theories prioritize the bonds needed to create community whereas boundary theories of privacy prioritize spatial, behavioural, or informational boundaries to carve out private spheres for autonomous individual action. Intersubjective theories of privacy prioritize interpersonal bonds on the basis that intersubjective and social conditions of human life precede the emergence of an individual's subjectivity. This prioritization follows Mead, who argued that humans become aware of themselves as individuals only through their social interaction with others (Mead, 1934). Moreover, having developed subjectivity, humans rely on intersubjectivity-based modes of communications to arrive at commonly held normative, ethical, and political positions (Warren, 1995). Social life then plays a significant role in shaping and informing how individuals unfold as a result of relationships they are situated in throughout their lives.

An approach to privacy based on intersubjective concepts ably registers the "harm" associated with mass collection of telecommunications metadata, insofar as such data are used to map communities of communication, associations between different parties, and mechanisms through which persons communicate with one another. An intersubjective-based privacy model registers that aggregated metadata can be deeply harmful to a given person's or community's interests and even provoke individuals to retreat based on fears of potential discrimination. Thus, the collection of metadata infringes upon the privacy needed for communities of people to develop, communicate, and share with one another. The effects of metadata collection stand in contrast to the routine—if mistaken—assertions that metadata are less revealing of individuals than the content of their communications and thus less likely to infringe upon privacy interests.

For intersubjective models of privacy to register individual harms, however, they must appeal to how affecting individuals has a corresponding impact on the communities in which they are embedded and on how those community-shared norms are responsible for identifying an individual's harm. Consequently, individual harms resulting from targeted surveillance are registered as a secondary-level of harm, where the first-level harm is registered in how the community is affected by the retreat of the given individuals. This stands in contrast to a boundary model, where harms to the individual are what trigger a first-order harm. Intersubjective theories of privacy effectively shift the lens of harm: the focus is placed on how a community or group is affected by surveillance, first and foremost, and how such surveillance has a derivative effect on public engagement, the development of intersubjective bonds, and the actions undertaken by specific individuals included in the targeted community or group.

Both individual- and intersubjective-based conceptions of privacy retain value in an era of pervasive mass surveillance. But by turning to deliberative democratic theory a more robust line of critique towards mass surveillance can be mounted: such surveillance practices are not just problematic because they violate privacy rights or reasonable expectations of privacy but because the practices threaten to compromise the very conditions of democracy itself. As such, mass surveillance endangers democratic governance domestically as well as abroad.

4. Rebalancing Critique on the Grounds of Autonomy

The FVEY agencies monitor groups and individuals to justify or support kinetic operations, such as those against militants or terrorists or foreign military agencies. The agencies also conduct surveillance to inform economic policy advice, understandings of international organizations political leanings, as well as to support domestic agencies' operations (Fung, 2013; Robinson, 2013). Given the scope of potential targets, combined with the mass-collection techniques adopted by Western agencies, the central critiques of the agencies' operations should not exclusively revolve around how these operations raise or generate privacy violations. Instead, a central line of critique should focus on analyzing the core of what the agencies engage in: the disruption, or surveillance, of communications through which citizens engage in deliberation, exercise their autonomy, and conduct public and private discourse. While the FVEY agencies' surveillance engages privacy rights the surveillance also engages more basic freedoms such as rights to speech and association. A Habermasian deliberative democratic model offers a fertile ground to address these deeper democratic problems based on an articulation of human autonomy and deliberation while simultaneously accounting for the privacy harms associated with the FVEY agencies' surveillance activities.

Habermas' deliberative democratic model considers the co-original nature of what he calls private and public autonomy. Both of these are intrinsically linked with speech acts which, today, routinely are made using the telecommunications systems monitored by the FVEY agencies. Per Habermas, these forms of autonomy are

equally needed to establish the basic laws of a nation-state, which themselves secure individual and group freedoms. Specifically, individuals must be able to exercise their private autonomy as members of a collaborative political process when first establishing constitutions, charters, or first principles of law making. Public autonomy is made possible by engaging with others to create the terms for collaborative law making and assignment of political power, but doing so presupposes that individuals self-regard themselves as autonomous and thus capable of shaping their personal freedom vis-a-vis their group, or public, autonomy (Habermas, 1998a). In short, it must be possible for individuals to recognize themselves as independently autonomous and, simultaneously, within social relationships in order to establish basic laws protecting personal and group rights while acting within the context of shared political dialogue and negotiations.

Neither the private autonomy of the individual or the autonomy expressed in engaging in public action precede one another; instead, they are co-original (Chambers, 2003). As a result, all law emergent from these essential concepts must shield the legally secured capacities to enjoy and express public and private autonomy or else laws would risk infringing upon the very essential principles needed to take part in politics. This means that activities which infringe on either the private or public expression of autonomy can be critiqued on the basis of the legitimacy of the activities, as well as based on how infringing upon a person's private autonomy affects their public autonomy and vice versa.

As noted previously, under a Habermasian political theory model, communications are central to a person's development and expression of their autonomy. Habermas explicitly asserts the importance of communications as shaping core aspects of individuals' relations with themselves and one another, writing:

> The social character of natural persons is such that they develop into individuals in the context of intersubjectively shared forms of life and stabilize their identities through relations of reciprocal recognition. Hence, also from a legal point of view, individual persons can be protected only by *simultaneously* protecting the context in which their formation processes unfold, that is, only by assuring themselves access to supportive interpersonal relations, social networks, and cultural forms of life. (Habermas, 1998b, p. 139)

Such supportive relations, networks, and forms of life are denied to persons and populations subject to persistent and pervasive surveillance; the collection and retention of personal information can cause people to become prisoners of their recorded pasts and lead to deliberate attempts to shape how their pasts will be remembered (Solove, 2008; Steeves, 2009). Such attempts can include avoiding deviant behaviour, refusing to associate with groups at the margins of acceptable society, or otherwise attempting to be "normal" and thus avoid developing or engaging with "abnormal" social characteristics (Cohen, 2000; DeCew, 1997, p. 74). The stunting of communication, and the associated stunting of personal and social development, run counter to the development possibilities possible absent mass, untargeted, surveillance. In conditions of non-mass surveillance, persons may engage in "direct frank communications to those people they trust and who will not cause harm because of what they say. Communication essential for democratic participation does not occur only at public rallies or on nationwide television broadcasts, but often takes place between two people or in small groups" (Solove, 2008, p. 143). While the monitoring of such communications will not end all conversations it will alter what individuals and groups are willing to say. Such surveillance, then, negatively affects communicative processes and can be critiqued on its capacity to stunt or inappropriately limit expressions of private or public autonomy (Cohen, 2000).

Habermas does not argue that all government surveillance is necessarily illegitimate or unjust. Rather, citizens must have knowingly legitimated surveillance laws that could potentially intrude upon their lives. The FVEY agencies' surveillance practices, however, are arguably illegitimate on the basis that these agencies apply secret interpretations to public law, while preventing the public from reading or gaining access to those interpretations (Office of the Communications Security Establishment Commissioner, 2006; Robinson, 2015; Sensenbrenner, 2013). Given the secrecy with which FVEY agencies conduct their operations there is little to no way for citizens to know whether such basic rights have been, or are being, set to one side by the FVEY agencies in their service to their respective executive branches of government. The consequence is that citizens cannot perceive themselves as potential authors and authorizers of law that infringes legal protections designed to secure each citizen's public and private autonomy. Citizens cannot, in effect, legitimate laws that result in the mass and pervasive surveillance of the population based on the potential that one person may be a danger; such surveillance practices would stunt the individuals' development and the development of the communities that individuals find themselves within, as people limit what they say to avoid experiencing the (unknown) consequences of their speech.

Habermas' emphasis on the role of speech in orienting political activity, combined with his theory's critical nature, provide us with a way of critiquing the domestic implications of mass surveillance activities as well as providing a path to identify the international implications of such activities. In the context of nation-states, discourses and bargaining processes "are the place where a reasonable political will can develop",

though this will requires the existence of communicative conditions that do not unduly censor or stunt discourse (Habermas, 2001, p. 117). The process of deliberation lets citizens of nation-states develop, critique, and re-develop norms of political activity that are reflexive, temporally specific, and persistently developing; in the Habermasian system the arrival at laws vis-à-vis deliberation "must allow for the greatest degree of inclusion, is never complete and remains open to the demands of future contestation" (Payrow Shabani, 2003, p. 172). Laws and policies which prevent or inhibit deliberation can also be critiqued on grounds that they may inappropriately infringe upon the deliberative capacities of individuals or communities. Such laws and policies may be unjust (though not, necessarily, illegal) if they exclude groups or individuals from participating in deliberation processes linked to politics and lawmaking (Habermas, 1998c). This has implications for surveillance that stunts discourse which takes place amongst communities and groups: such surveillance is unjust where it effectively excludes or hinders certain individuals and communities from developing shared understandings.

Ultimately, the Habermasian model registers how harms to individuals and to communities are problematic. Where an individual is unjustly targeted it can affect how the person subsequently is able to, or is willing to, express their autonomy. This, in turn, can limit their engagement in public deliberation. Such a limitation both prevents a person from regarding themselves as involved in the lawmaking process, thus rendering passed laws as less legitimate, but also stunts public discourse that occurs within and between communities. Consequently a FVEY agency's targeting of an individual has effects for the individual and the community. Monitoring all persons, such as through the massive collection of communications metadata at Special Sources Operations locations, also affects how communities and individuals alike operate. The mapping of communications networks can chill what groups say, how they deliberate, whom they choose to include in deliberations, and the conclusions they decide to consider. The result is that public deliberation itself is stunted. In the process, the individuals composing the groups are also affected insofar as the contexts wherein they develop themselves—amongst the intersubjective bonds between one another and which are entangled to become groups and communities—are stunted in their manifestation. While some of these harms may be acceptable to the deliberating public, such as when a public law is passed which authorizes authorities to wiretap specific persons believed to be engaging in socially disapproved activities, surveillance predicated on largely or entirely secret interpretations of law and which threaten to chill the activities of an entire citizenry represent an unacceptable type of surveillance-related harm because it would inhibit all speech, not just that of specific bad actors.

5. Conclusion

Focusing critique of the FVEY agencies' surveillance practices through the lens of Habermasian critical theory is accompanied by a series of benefits. Such benefits include making it theoretically clear how norm contestation can be broadened beyond national boundaries, inviting novel ways of thinking about legal challenges to such surveillance, and clarifying how communications rights offer a way to critique and rebut unjust surveillance practices. In effect, by basing our understanding of privacy harms in a broader democratic theory we can not only respond to harms associated with privacy violations but also more broadly understand the role of privacy in fostering and maintaining healthy deliberative processes that are central to democratic governance.

To begin, the Habermasian model invites broadening normative claims of harm on grounds that activities which distort or damage the capacity for a citizenry or set of individuals to express public or private autonomy vis-a-vis deliberation can be generally subject to critique. In the case of pervasive mass surveillance, the activities undertaken by Western SIGINT agencies can affect how non-Western citizens deliberate and participate in their political systems. Thus, whereas Nissenbaum was forced to address how a national court could address international-based issues, the Habermasian approach is clearer on the relationship between mass surveillance and international norms. Specifically, such surveillance constitutes a violation of human rights of non-FVEY persons on the basis that human rights "make the exercise of popular sovereignty legally possible" (Habermas, 1998c, p. 259) by establishing the conditions for deliberation needed for the expression of private and public autonomy. In threatening those conditions, the FVEY nations are challenging the ability for other nations' sovereignty not just by spying on them, but by stunting the legitimate deliberative processes of other nations' citizens just as they stunt the deliberative processes of their own citizens. Such stunting follows citizens in non-FVEY nations ceasing or modifying their deliberations. Moreover, such surveillance transforms life-developing communications into instruments or data to potentially be used against foreign persons and the groups they operate within. The FVEY agencies are, in effect, actively subverting the basic rights that people around the world require to secure their private autonomy and create the medium through which those individuals, as citizens, can make use of their public autonomy.

Second, by analyzing the FVEY agencies' surveillance practices through a Habermasian lens it is immediately apparent how the targeting of individuals or the surveillance of the world's populations en masse create reciprocating harms. The interference with individuals has ripple effects on their communities and vice versa.

Future work could explore how the targeting of communities, then, ought to trigger tort-based claims of harm. Similarly, a Habermasian approach might give communities as distinct bodies a way of asserting harm to the collective as a result of their members having been targeted by unjust surveillance practices. In effect the co-originality of private and public autonomy, and associated need for individual persons to protect themselves along with their access to supportive interpersonal relations, social networks, and cultural forms of life, may open novel ways of introducing into legal theory a reciprocal understanding of how harm to individuals is harm to their communities and vice versa.

Finally, focusing on the importance of communications in developing private and public autonomy provides a mode of critiquing SIGINT operations that is more expansive than critiques of the FVEY agencies' operations which are principally driven by theories of privacy. While privacy remains a legitimate path of critique, the broader Habermasian grounded critique lets us consider the breadth of opportunities that communications provide to individuals and communities, to the effect of revealing the extent of the harm tied to massively monitoring the globe's communications. That is, a Habermasian lens lets us critique contemporary mass surveillance practices on the basis that they infringe upon a host of constitutional- and human rights-protected activities, of which privacy is just one such violated right. By shifting our lens of critique to how signals intelligence operations threaten public and private right, vis-a-vis communications surveillance, and recognizing both rights as co-original concepts instead of one preceding another, a range of political concepts, rights, and freedoms can be used in the analysis and critique of the FVEY agencies' activities. Practically, adopting this approach could re-orient popular and scholarly debates: resolving the FVEY agencies' surveillance practices would attend, first, to ensuring that communications rights themselves are secured on the basis of the democratic freedoms associated with such communications. Such a re-orientation should not exclude enhancing privacy protections provided to individuals and the communities they are enveloped and immersed within, but emphasizes that neither individuals nor communities are more or less important and that the principal goal of privacy protections are to ensure that that deliberation and association can occur without undue coercion or surveillance.

In summary, privacy alone should not be the primary or exclusive counter to understanding or critiquing the mass surveillance practices undertaken by Western SIGINT agencies. As discussed in this article, boundary- and intersubjectivity-based theories of privacy have limitations in how they can critique targeted and mass surveillance practices. And even the most promising intersubjective theory of privacy that is specifically attentive to mass surveillance harms is too nationally-focused to account for the global nature of contemporary SIGINT operations. But by adopting a Habermasian approach, which focuses both on communications and situates public and private autonomy as co-original, we can broaden the lens of critique of SIGINT practices while addressing limitations in privacy theories. More work beyond this article must be done to further build out how a Habermasian inspired theory of privacy can accommodate the already entrenched contributions of the existing privacy literature and explore how much, and how well, the contributions born of boundary and intersubjective privacy literatures can be (re)grounded in a Habermasian theoretical framework. But such hard work should not dissuade us from exploring new groundings for theories of privacy which may provide more holistic ways of critiquing contemporary targeted and massive signals intelligence practices.

Acknowledgements

Funding to conduct this research has been provided by the Social Science and Humanities Research Council of Canada and the Canadian Internet Registration Authority's Community Investment Program.

Conflict of Interests

The author declares no conflict of interests.

References

Ackerman, S. (2013, July 17). NSA warned to rein in surveillance as agency reveals even greater scope. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jul/17/nsa-surveillance-house-hearing

Allen, A. (1985). *Uneasy access: Privacy for women in a free society*. Totowa, NJ: Rowman and Littlefield.

Austin, A. (2012). Getting past privacy? Surveillance, the charter and the rule of law. *Canadian Journal of Law and Society*, *27*(2), 381-398.

Ball, J. (2013, September 30). NSA stores metadata of millions of web users for up to a year, secret files show. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

Bamford, J. (2008). *The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America*. Toronto: Doubleday.

Bennett, C. J., & Raab, C. (2006). *The governance of privacy: Policy instruments in global perspective*. Cambridge: MIT Press.

Chambers, S. (2003). Deliberative democratic theory. *Annual Review of Political Science*, *6*, 307-326.

Chandler, J. (2009). Privacy versus national security: Clarifying the trade-off. In I. Kerr, V. Steeves, & C. Lucock (Eds.), *Lessons from the identity trail: Anonymity, pri-*

vacy and identity in a networked society (pp. 121-138). Toronto: Oxford University Press.

Cohen, J. (2000). Examined lives: Informational privacy and the subject as object. *Stanford Law Review*, *52*, 1373-1438.

CSE. (2010, November). CSEC SIGINT Cyber Discovery: Summary of the current effort. *Government of Canada*. Retrieved from https://www.christopher-parsons.com/Main/wp-content/uploads/2015/02/cse-csec-sigint-cyber-discovery.pdf

CSE. (2012b, June). And they said to the Titans: Watch out Olympians in the house! *Government of Canada*. Retrieved from https://www.christopher-parsons.com/Main/wp-content/uploads/2014/12/csec-br-spy.pdf

DeCew, J. W. (1997). *In pursuit of privacy: Law, ethics, and the rise of technology*. Ithaca: Cornell University Press.

Freeze, C., & Dobby, C. (2015, March 17). NSA trying to map Rogers, RBC communications traffic, leak shows. *The Globe and Mail*. Retrieved from http://www.theglobeandmail.com/news/national/nsa-trying-to-map-rogers-rbc-communications-traffic-leak-shows/article23491118

Froomkin, D. (2015, May 5). The computers are listening: How the NSA converts spoken words into searchable text. *The Intercept*. Retrieved from https://firstlook.org/theintercept/2015/05/05/nsa-speech-recognition-snowden-searchable-text

Fung, B. (2013, August 5). The NSA is giving your phone records to the DEA. And the DEA is covering it up. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/05/the-nsa-is-giving-your-phone-records-to-the-dea-and-the-dea-is-covering-it-up

Gallagher, S. (2013a, August 9). Building a panopticon: The evolution of the NSA's XKeyscore. *Ars Technica*. Retrieved from http://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore

Gallagher, S. (2013b, December 31). Your USB cable, the spy: Inside the NSA's catalog of surveillance magic. *Ars Technica*. Retrieved from http://arstechnica.com/information-technology/2013/12/inside-the-nsas-leaked-catalog-of-surveillance-magic

Gallagher, S. (2014, May 14). Photos of an NSA "upgrade" factory show Cisco router getting implant. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant

Geuss, M. (2013, September 28). Bypassing oversight, NSA collects details on American connections. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/2013/09/bypassing-oversight-nsa-collects-details-on-american-connections

Greenwald, G. (2014). How Covert Agents Infiltrate The Internet To Manipulate, Deceive, and Destroy Reputations. *The Intercept*. Retrieved from https://firstlook.org/theintercept/2014/02/24/jtrig-manipulation

Greenwald, G., Grim, R., & Gallagher, R. (2013). Top-secret document reveals NSA spied on porn habits as part of plan to discredit "radicalizers". *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html

Habermas, J. (1998a). Three normative models of democracy. In C. Cronin & P. De Greiff (Eds), *The inclusion of the other: Studies in political theory* (pp. 239-252). Cambridge, MA: MIT Press.

Habermas, J. (1998b). On the relation between the nation, the rule of law, and democracy. In C. Cronin & P. De Greiff (Eds), *The inclusion of the other: Studies in political theory* (pp. 129-154). Cambridge, MA: MIT Press.

Habermas, J. (1998c). On the internal relation between the rule of law and democracy. In C. Cronin & P. De Greiff (Eds), *The inclusion of the other: Studies in political theory* (pp. 253-264). Cambridge, MA: MIT Press.

Habermas, J. (2001). Remarks on legitimation through human rights. In M. Pensky (Ed.), *The postnational constellation political essays* (pp. 113-129). Cambridge, MA: MIT Press.

Israel, T. (2015). Foreign intelligence in an inter-networked world: Time for a re-evaluation. In M. Geist (Ed.), *Law, privacy and surveillance in Canada in the post-Snowden era*. Ottawa: Ottawa University Press.

Maas, P. (2015, February 18). Destroyed by the espionage act. *The Intercept*. Retrieved from https://firstlook.org/theintercept/2015/02/18/destroyed-by-the-espionage-act

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013, June 21). GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*. Retrieved from http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Mead, G. H. (1934). *Mind, self, and society from the standpoint of a social behaviouralist*. Chicago: University of Chicago Press.

Mill, J. S. (1859). *Three essays*. Oxford, Oxford University Press.

Millar, J. (2009). Core privacy: A problem for predictive data mining. In I. Kerr, V. Steeves, & C. Lucock (Eds.), *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* (pp. 103-120). Toronto: Oxford University Press.

National Security Agency (NSA). (2010, September 13). Into to the VPN exploitation process. *United States Government*. Retrieved from http://www.spiegel.de/media/media-35515.pdf

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

Office of the Communications Security Establishment

Commissioner. (2006). Communications security establishment commissioner annual report, 2003—2004. *Government of Canada*. Retrieved from http://www.ocsec-bccst.gc.ca/ann-rpt/2005-2006/activit_e.php#5

Parsons, C. (2015). BOUNDLESSINFORMANT documents (collection). *Technology, Thoughts, and Trinkets*. Retrieved from https://www.christopher-parsons.com/writings/cse-summaries/#boundlessinformant-documents

Parsons, C., Bennett, C. J., & Molnar, A. (2015). Privacy, surveillance and the democratic potential of the social web. In B. Roessler & D. Mokrosinksa (Eds.), *Social dimensions of privacy*. Cambridge: Cambridge University Press.

Payrow Shabani, O. (2003). *Democracy, power, and legitimacy: The critical theory of Jürgen Habermas*. Toronto: University of Toronto Press.

Plouffe, J.-P. (2014). Statement by CSE Commissioner the Honourable Jean-Pierre Plouffe re: January 30 CBC story. *Office of the Communications Security Establishment Commissioner.* Ottawa: Government of Canada.

Regan, P. (1995). *Legislating privacy: Social values and public policy*. Chapel Hill: University of North Carolina Press.

Risen, J., & Lichtblau, E. (2009, June 9). E-Mail surveillance renews concerns in Congress. *The New York Times.* Retrieved from http://www.nytimes.com/2009/06/17/us/17nsa.html

Robinson, B. (2013) Economic intelligence gathering IV. *Lux Ex Umbra*. Retrieved from http://luxexumbra.blogspot.ca/2013/12/economic-intelligence-gathering-iv.html

Robinson, B. (2015). Does CSE comply with the law? *Lux Ex Umbra: Monitoring Canadian Signals Intelligence (SIGINT) Activities Past and Present.* Retrieved from http://luxexumbra.blogspot.ca/2015/03/does-cse-comply-with-law.html

Rule, J. (2007). *Privacy in peril: How we are sacrificing a fundamental right in exchange for security and convenience*. Toronto: Oxford University Press.

Schoeman, F. (1992). *Privacy and social freedom*. Cambridge: Cambridge University Press.

Sensenbrenner, J. (2013, August 19). How Obama has abused the Patriot Act. *Los Angeles Times*. Retrieved from http://articles.latimes.com/2013/aug/19/opinion/la-oe-sensenbrenner-data-patriot-act-obama-20130819

Solove, D. (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.

Steeves, V. (2009). Reclaiming the social value of privacy. In I. Kerr, V. Steeves, & C. Lucock. *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* (pp. 191-208). Toronto: Oxford University Press.

Strandburg, K. (2008). Surveillance of emergent associations: Freedom of association in a network society. In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. De Capitani di Vimercati (Eds), *Digital privacy: Theory, technologies, and practices* (pp. 435-458). New York: Auerbach Publications.

Timm, T. (2014, May 3). Technology law will soon be reshaped by people who don't use email. *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2014/may/03/technology-law-us-supreme-court-internet-nsa

Turkle, S. (2012). *Alone Together: Why we expect more from technology and less from each other*. New York: Basic Books.

Warren, M. E. (1995). The self in discursive democracy. In S. K. White (Ed.). *The Cambridge companion to Habermas* (pp. 167-200). New York: Cambridge University Press.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220.

Weaver, N. (2013, November 13). Our government has weaponized the internet. Here's how they did it. *Wired*. Retrieved from http://www.wired.com/2013/11/this-is-how-the-internet-backbone-has-been-turned-into-a-weapon

Weaver, N. (2014, March 13). A close look at the NSA's most powerful internet attack tool. *Wired*. Retrieved from http://www.wired.com/2014/03/quantum

About the Author

Dr. Christopher Parsons

Christopher Parsons received his Bachelor's and Master's degrees from the University of Guelph, and his Ph.D from the University of Victoria. He is currently the Managing Director of the Telecom Transparency Project and a Postdoctoral Fellow at Citizen Lab, in the Munk School of Global Affairs with the University of Toronto. He maintains a public website at www.christopher-parsons.com.

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

Article

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

Vian Bakir

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

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

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

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

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

1. Introduction

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

Traditional forms of intelligence oversight operate

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

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

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

2. Context

2.1. The Dataveillance

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

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

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

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

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

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

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

2.2. The Struggle

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

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

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

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

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

3. Methodology

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

hence of the likelihood of achieving "equiveillance".

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

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

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

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

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

4. Public Oversight Mechanisms: Surveillance Studies

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Public Oversight Mechanisms: Intelligence Studies and Journalism Studies

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

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

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

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

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

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

6. Discussion

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

6.1. Conceptual Tools: The Veillant Panoptic Assemblage

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

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

6.2. A Framework for Evaluating Equiveillance

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

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

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

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

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

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

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

Acknowledgments

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

Conflict of Interests

The author declares no conflict of interests.

References

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

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

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

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

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

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

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

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

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

Canadian Journalists for Free Expression. (2015).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

About the Author

Dr. Vian Bakir

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

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 3, Pages 26-38
Doi: 10.17645/mac.v3i3.286

Article

Attaching Hollywood to a Surveillant Assemblage: Normalizing Discourses of Video Surveillance

Randy K. Lippert * and Jolina Scalia

Department of Sociology, Anthropology, and Criminology, University of Windsor, Windsor, ON N9B 3P4, Canada;
E-Mails: lippert@uwindsor.ca (R.L.), scalia3@uwindsor.ca (J.S.)

* Corresponding author

Submitted: 5 April 2015 | In Revised Form: 5 June 2015 | Accepted: 15 June 2015 |
Published: 20 October 2015

Abstract
This article examines video surveillance images in Hollywood film. It moves beyond previous accounts of video surveillance in relation to film by theoretically situating the use of these surveillance images in a broader "surveillant assemblage". To this end, scenes from a sample of thirty-five (35) films of several genres are examined to discern dominant discourses and how they lend themselves to normalization of video surveillance. Four discourses are discovered and elaborated by providing examples from Hollywood films. While the films provide video surveillance with a positive associative association it is not without nuance and limitations. Thus, it is found that some forms of resistance to video surveillance are shown while its deterrent effect is not. It is ultimately argued that Hollywood film is becoming attached to a video surveillant assemblage discursively through these normalizing discourses as well as structurally to the extent actual video surveillance technology to produce the images is used.

Keywords
assemblages; discourses; film; normalization; surveillance; video

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

1. Introduction

When a video surveillance image of the Washington, D.C. subway platform helped identify an intern's murderer in the *State of Play*, when footage of a man with a prosthetic leg entering airport Customs helped identify an elusive assassin in *The International,* and when images of a lime drink ordered from a Las Vegas blackjack table revealed an illegal card counting plot in *21*, Hollywood expressed that video surveillance[1] is a widespread, useful investigative tool that can yield positive benefits. At the same time video surveillance continues to spread largely unheeded (Doyle et al., 2012). Already commonplace in malls, banks, convenience stores, casinos and airports by the 1980s, it has since appeared in taxi-cabs, transit stations, trains, buses, fast food restaurants, supermarkets, campuses, schools, private residences, and even within police officers' vehicles and uniforms (Carroll, 2013; Dinkes et al., 2009; Doyle & Walby, 2012; Monahan, 2006; SCAN, 2009; Walby, 2006). Video surveillance is now encountered virtually everywhere, anytime, its images almost instantaneously reproduced and widely disseminated by almost anyone with internet access, a device, and data file-sharing capabilities. This astonishingly rapid proliferation of video surveillance and its generated images, as with many newer forms of surveillance, is troubling because it can seriously threaten personal privacy and can reproduce social inequalities when dis-

[1] We use "video surveillance" rather than "CCTV", since this technology is no longer exclusively closed circuit or has much to do with television (Doyle et al. 2012, p. 5).

advantaged groups defined by race/ethnicity, gender, class, or sexual orientation are disproportionately targeted (Doyle et al., 2012; Lippert, 2009; Monahan, 2010, p. 90; SCAN, 2009). This lack of public opposition to video surveillance's proliferation, with or without fair notification (Lippert, 2009) or built-in privacy-by-design protections (Lippert & Walby, 2015), implies many ignore, forget, or are unaware that these systems pose serious threats. But what is perhaps most puzzling is the wide embrace of video surveillance systems, despite ambiguous evidence of effectiveness in halting or reducing the illegal or other undesired behavior it aims to curtail (see Doyle et al., 2012; SCAN, 2009). Independent and government studies, for example, often suggest video surveillance is quite limited as a violent crime prevention measure (Verga, 2010, p. 10).

How video surveillance and its images are widely understood to be used and experienced may be a more important driver than their actual effectiveness in reducing crime or other unwanted conduct. Plainly one process affecting these understandings is when video surveillance images that are produced in myriad actual settings (such as banks or convenience stores) find their way into television news programs and onto news media websites for purposes of entertainment (or "fun", see Bauman et al., 2014). Another entertainment-related use that may lead to wider acceptance, however, entails featuring video surveillance and its images in fictional Hollywood film. The film scenes depicting video surveillance images, such as those above, may normalize the spread and intensification of video surveillance. This article explores video surveillance images in Hollywood film to discern key normalizing discourses and lend understanding to how Hollywood film may be becoming attached to a video surveillance assemblage.

2. Surveillance Assemblage, Normalization, and Expression

Video surveillance's growth is part and parcel of the broader proliferation of myriad surveillance technologies in "surveillance societies" (Murakami-Wood & Webster, 2009, 2011) where "the gaze is ubiquitous, constant, inescapable" (Lyon, 2007, p. 25). By surveillance we mean "the systematic monitoring of people or groups in order to regulate or govern their behavior" (Monahan, 2011, p. 498). The growing "surveillance studies" literature seeks to understand how new forms of surveillance scrutinize populations (Lyon, 2002, p. 2). But this literature has thus far tended to neglect normalization (Murakami-Wood & Webster, 2009, 2011), the process by which these forms of surveillance become widely accepted in society.

An emergent model of surveillance in surveillance studies is the assemblage (Haggerty & Ericson, 2000; Lippert, 2009; Lippert & Wilkinson, 2010; Wilkinson & Lippert, 2011; Murakami-Wood, 2013), a surveillance entity that involves merging previously distinct elements. Adapted from the philosophy of Deleuze and Guattari (1987), here surveillance is "rhizomatic", its growth occurs "across a series of interconnected roots which throw up shoots in different locations" rather than hierarchically (Haggerty & Ericson, 2000, p. 614). An assemblage works "by abstracting human bodies" from particular sites and sorting them into separate channels; they are then reassembled elsewhere as "data doubles" or entities of pure information that are amenable to closer scrutiny and analysis (Haggerty & Ericson, 2000, p. 606). This examination and calculation occurs at myriad sites to inform strategies of control (Haggerty & Ericson, 2000, p. 613). Surveillant assemblages do not, however, reflect centralized systematic control as evinced in George Orwell's "Big Brother" centralized state or Michel Foucault's panoptic central tower (Haggerty & Ericson, 2000). Foucault's panopticon in particular has been stretched beyond recognition to fit new forms and contexts of surveillance (Haggerty, 2006; see also Zimmer, 2011). For example, its notions of soul-training through discipline in enclosed spaces (see Foucault, 1977) are hopelessly out of sync with how much contemporary surveillance operates across and in spite of spatial barriers (Haggerty, 2006).

But there is more to surveillant assemblages than how they operate. Thus, assemblages tend to be propelled and shaped by specific governmental logics (Lippert, 2009). Of pertinence here is the "precautionary logic" that is associated with neo-liberalism and which presupposes definite "limits of science and technology" in yielding certainty about the future (Ericson, 2007, p. 22). As it enters liberal democratic institutions this logic undercuts trust, raises suspicion and doubt, and fuels criminalization (Ericson, 2007, pp. 21-24). It also overrides longstanding criminal law principles, such as the presumption of innocence (Ericson, 2007, pp. 23-24), thus halting the traditional practice of equating uncertainty with innocence (e.g., convicting persons of criminal offences only when guilt is "beyond a reasonable doubt"). As this logic spreads, surveillant assemblages emerge as a major form of "counter law" or "law against law" (Ericson, 2007, p. 33) to confront the often worst conceivable future outcome, regardless of uncertainty over whether it will ever occur. Perhaps even more relevant to this paper is the mass media logic that demands access to "the real" and which is perhaps best evinced in the remarkable growth of reality television during at least the past two decades (Lippert & Wilkinson, 2010, p. 136). Increasingly viewers are thought to demand, even crave, this access, however illusory it may be (see, for example, Doyle's (2003) insightful analysis of the supposed realism of the long running FOX television program, "Cops").

Surveillant assemblages do not emerge separate from how their elements are expressed and represent-

ed. Consistent with this, Kammerer (2012, p. 105) writes: "The surveillant imaginary is not external to the working of surveillance, but intrinsically linked to its functioning". Where assemblages are concerned, this means, as Bogard (2006, p. 107) explains, "[e]very assemblage must be described both in terms of its content…and its expression…That is, one must examine not only what the assemblage does, but also what it says". How is Hollywood film becoming attached to a video surveillant assemblage? If Hollywood film makes statements about video surveillance when using these images, what does it say?

Film is a powerful medium and like television's effects on violence (e.g., Jamieson & Romer, 2014), it has undergone much study about its relationship to real world problematic behaviors and events too numerous to detail here. It is important to note, however, that film is neither merely a mirror of the *real* world, representing surveillance technologies and processes in realistic ways, nor does it necessarily *directly* affect real world acceptance thereof. Rather, surveillance in film and surveillance in social institutions or the broader society influence one another in ways often difficult to unravel. To suggest film influences the normalization of surveillance demands at a minimum an exploration of how it does this, that is, through what specific discourses. To think of Hollywood film as part of a surveillant assemblage is to begin to move beyond film's representational role. We argue that there is a sense in which film is not merely representing video surveillance in the ways identified below but is actually attaching itself to it. Film may be an element of rather than merely a mirror reflecting complex video surveillance assemblages.

To be normalized, the implanting or implementation of a technology and related processes must receive little or no effective resistance. Normalization entails discourses or "groups of statements which structure the way a thing is thought and the way we act on the basis of that thinking…" (Rose, 2007, p. 142). These discourses express and structure how we understand and act upon an increasingly watched world and the technologies comprising it. Recent work has begun to situate video surveillance in relation to surveillant assemblages (Lippert, 2009; Lippert & Wilkinson, 2010; Wilkinson & Lippert, 2012). One way of conceiving of normalization is as a decidedly overlooked element of these assemblages.

This paper's purpose is to move beyond previous research by approaching the presence of video surveillance images in Hollywood films as elements of a video surveillant assemblage. Specifically, it seeks to extend thinking about surveillance and film by exploring dominant discourses of video surveillance, illuminating the complexity of video surveillance image use in Hollywood film, and theoretically situating film use in a surveillant assemblage. In so doing we seek to fill a gap in surveillance studies about normalization via film, an effort we think is overdue.

The remainder of this article unfolds in five parts. We first discuss previous research on surveillance and film. After discussing our method, we next elaborate results of our exploratory inquiry by showing first that video surveillance is appearing in film more often; it is increasingly worked into film in various ways. We then reflect on this incorporation of video surveillance images to identify the discourses impressed upon viewers in a sample of Hollywood films and how these may contribute to normalization. We then take up how Hollywood is attached to a video surveillance assemblage and conclude by discussing the implications of these findings for existing literature and future research.

3. Previous Research on Surveillance and Film

Most of what is known about surveillance comes from media discourses (Norris & Armstrong, 1999, p. 63), which typically represent video surveillance in positive terms (see Andrejevic, 2004; Barnard-Wills, 2011; Norris & Armstrong, 1999). Reality television (see Doyle, 2006; McCahill, 2003), in particular, has led citizens to become accustomed to surveillance in everyday life, even to enjoy it; it has "train[ed] our eyes and minds for surveillance" (Murakami-Wood & Webster, 2009, p. 264). Television's entertaining or "fun" quality is a key driver of surveillance technologies (Albrechtslund & Dubbeld, 2005).

The broad theme of surveillance in Hollywood films has been explored, along with how its ethical dilemmas, including those relating to privacy, are portrayed (Albrechtslund, 2008). Turner's (1998) research, for example, analyzed a large but now dated sample of Hollywood films. He argued the overabundance of surveillance themes in media "transforms the will and practice of the surveillance society into a spectacle" (1998, p. 107), renders viewers passive, and leads to acceptance of surveillance technology. Since then Levin (2002) noticed Hollywood films were increasingly using recorded video surveillance images to accompany narration, such as in *Thelma and Louise*. Though his focus is beyond video surveillance, Levin (2002, p. 582) was unique in suggesting that film narration has "effectively become synonymous with surveillant" expression and that there is increasingly a structural mutually constitutive tether between surveillance technologies and film. Although not invoking the assemblage concept, and based on only a few films, Levin's assertion is nonetheless supportive of our analysis that follows. Zimmer (2011) similarly considers the rise of surveillance themes in film narratives by focusing on early 20th Century short films and Alfred Hitchcock's *Rear Window*. Suggestive for our analysis below too, Zimmer argues not only that surveillance technologies as depicted are inconsistent with the panopticon (also implied by Gad

& Hansen (2013) as noted below), but that surveillance narratives in film "should be viewed not just as 'reflections' of an increasingly-centred media, but themselves as *practices* of surveillance" (Zimmer, 2011, p. 439; original emphasis). This remark is consistent with our assertion later: there is a more structural or material attachment between Hollywood film and video surveillant assemblages, that in this respect at least there is sometimes no clear division between them.

Such accounts above partially speak to normalization and offer compelling, insightful analyses on which to build, although more detailed attention to more recent Hollywood films is needed. Video surveillance specifically has only begun to be studied in film, despite hints of its growing presence there. Most scholars researching video surveillance in cinema have sought to discover themes by analyzing a few films or a single film, for example, *Red Road* (Lake, 2010) or *Faceless* (Zeilinger, 2012). While these latter efforts have focused on somewhat obscure films, with limited viewership, they nonetheless have uncovered key themes of video surveillance, which can be investigated further. Thus, Lake (2010) effectively underscores in her analysis of *Red Road*, whose protagonist is a woman video surveillance operator, the notion that surveillers in Hollywood film are almost always White men in professional roles. Lake's attention to gender in relation to video surveillers is particularly significant in highlighting the fact that normalization is as much about who can acceptably and properly use video surveillance technology and reap its rewards as about those who become its targets. Similarly, Zeilinger (2012) highlights the near complete lack of critical reflection on video surveillance in film via a compelling analysis of the appropriation method evident in *Faceless,* a film created entirely by appropriating existing video surveillance footage to effectively challenge the growing video surveillance assemblage.

Of most pertinence to this paper, because of a closer focus on video surveillance in Hollywood film, however, are Gad and Hansen (2013) and Kammerer (2004) (from the perspective of film studies, see also Stewart (2012) regarding two 2012 Hollywood films, *Total Recall* and the *Bourne Legacy*). Gad and Hensen (2013, p. 153) argue that a key theme expressed by the film, *Minority Report*, is that prevention is achieved when involving a "complex assemblage" of humans and surveillance technologies (rather than suggesting that prevention is somehow linked, for example, to a panopticon). Unfortunately they do not extend their argument further to suggest films like *Minority Report* are discursively or structurally *attached* to that same assemblage. Kammerer (2004) analyzes three films (*Enemy of the State*, *Minority Report*, and *Panic Room*) with surveillance as a primary theme. He found a major discourse was the flawlessness of surveillance technology. According to Kammerer (2004), these films attest to technological infallibility; only human use of surveillance technology is error prone. Kammerer argued, contrary to Turner (1998), that Hollywood films like these can effectively raise vital issues about video surveillance in society, suggesting not all Hollywood film necessarily contributes to normalization (see also Kammerer, 2012, p. 105). We do not disagree with this assessment of film's critical potential (see also Marks, 2005), especially when considered in conjunction with brilliantly-crafted critical films like *Faceless* and *Red Road.* Yet, we assert a larger, broader sample of contemporary Hollywood films needs to be examined to discover more about whether and *how* they may contribute to normalization and to aid thinking about how they may be becoming attached to surveillant assemblages. This article therefore builds upon this insightful but somewhat mottled body of previous research from social science and the humanities by exploring a larger and broader sample of scenes from contemporary Hollywood films of multiple genres to discover relevant discourses and thereby lend understanding to popular cinema's messages to viewers specifically about video surveillance; how they may be contributing to its normalization through these expressions; as well as how they are becoming part of a video surveillance assemblage.

4. Method

To determine whether video surveillance's presence in film is proliferating we examined the IMDB, a comprehensive online film database[2], for films from the 1960s to the present categorized as featuring "CCTV"[3] surveillance. This examination was not intended to be exhaustive since other databases and keywords could have been used. Rather, it was envisioned as illustrative for this article's modest purposes. A drawback of this procedure was that films were categorized in IMDB only if CCTV surveillance was a prominent theme and thus this understandably underestimated its presence considerably. This was also a rawer measure than a *rate* of video surveillance inclusion (i.e., surveillance images per film), and admittedly there were more Hollywood films produced in each decade after the 1960s. Nonetheless, this procedure provided an initial empirical measure of video surveillance's growing presence in Hollywood film beyond mere impressions and it is one which might prime the pump for the flow of more refined procedures in this neglected realm.

To explore the discourses about video surveillance in Hollywood film our approach differed from most previous analyses of surveillance in film in that we examined 35 Hollywood films screened in North Ameri-

[2] http://www.imdb.com.

[3] We used "CCTV" in this instance because that is what was used in the IMBD database more often than "video surveillance".

can theaters from 1998 to 2015 (see Appendix 1[4]). We assumed Hollywood films screened in major theaters would eventually reach a larger viewership than straight-to-DVD films or more obscure films like *Faceless*, and were thus more apt to contribute to normalization. This is also a period during which video surveillance in film, based on our measure above, has expanded considerably. Rather than a random sample, we purposely included action, comedy, drama, horror, and thriller genres identified using IMDB. Given limited funding available, the cost of securing the films for analysis was also a consideration since some films falling within the parameters above were simply unavailable or too costly to acquire.

Our study then employed discourse analysis of the scenes (see Rose, 2007). This method promised to illuminate how Hollywood film represents video surveillance and how the former might contribute to the latter's normalization through dominant messages. Our analysis identified dominant discourses via two processes: open and focused coding. The open coding began with analyzing without previously formulated categories (Babbie & Benaquisto, 2002, p. 382). This was followed by focused coding whereby we subjected images to predetermined themes of interest from open coding or extant literature described above. The results of these procedures are discussed below.

[4] Though popular, some Hollywood films in the sample undoubtedly will be unknown to at least some readers. Unfortunately there is nowhere near enough space for a synopsis of each film; the reader is therefore encouraged to view unfamiliar films or consult online plot summaries via IMBD.com or rottentomatoes.com, among other sources.

5. Results

5.1. Growth of Video Surveillance in Hollywood Film

Video surveillance is increasingly present in Hollywood film. Our examination of the IMDB using the method described earlier revealed that, especially since 1999, the number of Hollywood and other films featuring video surveillance as a key element has increased dramatically as shown below (see Figure 1) and is accelerating during a time when video surveillance is fast proliferating in society. There were more films (8) featuring video surveillance in 2013 than any previous year. In the next section we examine the discourses concerning video surveillance.

5.2. Discourses of Video Surveillance in Hollywood Film

Our sample of 35 films included comedies like *American Pie* and *Hall Pass* and dramas like *21* and *The Judge* in which viewers may not readily expect to find video surveillance compared to, for example, thriller or crime genres. From our analysis emerged four dominant discourses about video surveillance: 1) Video Surveillance can Identify and Locate People to Advantage; 2) Video Surveillance need not Raise Privacy Concerns or be Resisted; 3) Only some People are Video Surveillance Competent; and 4) Neglect Video Surveillance and its Malfunctions at your Peril. While dominant in our sample, these discourses are not necessarily present in equal proportions across it. Each is elaborated below via illustrative scenes.

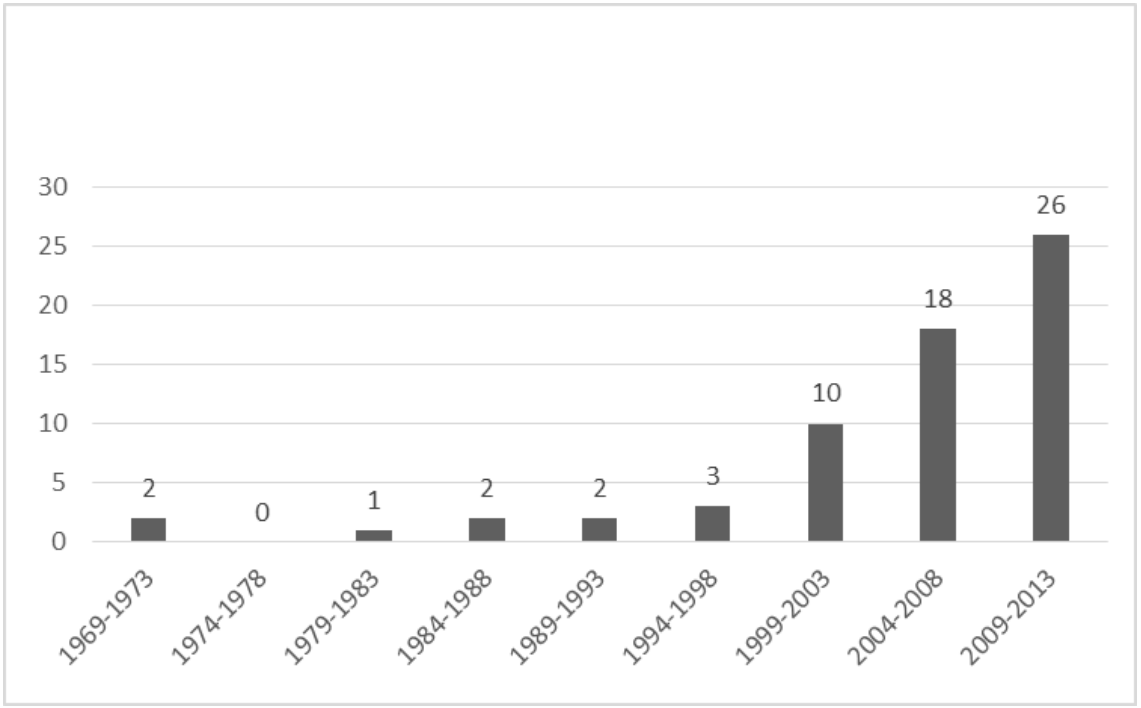

Figure 1. Number of popular films with video surveillance as plot element, 1969–2013.

5.2.1. Video Surveillance Can Identify and Locate People to Advantage

Scenes from 23 films suggested video surveillance can effectively identify or locate persons of interest to advantage or to serve particular interests. Our analysis revealed when this occurred it often lead to a major plot change, most often by discovering a person's true identity or culpability consistent with scenes described below. For example, in *Enemy of the State*, Robert Dean is shopping for a gift for his wife. There he encounters an old friend who frantically requests Dean's help and then exits the store. Shortly after, Dean discovers his friend was killed outside. The corrupt government agents responsible for the murder managed to secure video surveillance images showing the friend dropping an item into Dean's shopping bag. Dean then becomes a person of interest. In *Showtime*, detectives are watching a television show in their homes. While on the phone, one detective glances at the television and notices a person employed as a police department staffer in a bar with a known arms dealer. This image identifies a suspect which leads detectives to solve the case. In *Bourne Ultimatum*, the main character Bourne is in a train station using a cell phone to instruct a reporter to avoid being spotted by video surveillance. The reporter nonetheless draws attention to himself by running through the crowd and is identified via video surveillance by government agents and assassinated shortly thereafter while Bourne, whose location was unknown to this point in the film, is also identified in the crowd via video surveillance.

In other films too, persons were identified and then followed, typically using multiple video surveillance cameras. In *Snake Eyes*, after locating a person of interest on the casino floor via the security room's video surveillance monitors, Rick Santoro races to that location while using a "walkie-talkie" to stay connected to a guard in the security room. The guard directs Santoro to the person of interest using multiple casino surveillance cameras. In these films, video surveillance is seen yielding crucial information, such as a key person's location at a particular time. In several other films it is not a person of interest being sought but instead a vital object or valuable resource. In *The Italian Job*, a gang of thieves searches for one of three trucks containing gold bricks. As each truck passes through the gaze of video surveillance, the three images are compared to discern which truck is lowest to the ground and thus weighed down by an especially heavy load. This visual information helps reveal the gold's location. Across these scenes this information is always seen to be used to the advantage of the person accessing the images, thereby creating a decidedly positive association with video surveillance.

An overwhelming majority of surveillance images in the films did not lead to conventional criminal justice via arrests and convictions. However, video surveillance often effectively aided investigators pursuing these goals. In most films the discovery of suspects or persons of interest occurred because of video surveillance's capacity to provide visual information to solve a case. For instance, in *State of Play*, video surveillance footage of a congressional aide who allegedly committed suicide by stepping in front of a subway train is examined by Della Frye, a news reporter. Frye recognizes a man in the subway platform's video surveillance images whom she believes is implicated in murdering the aide by pushing her in the train's path instead. Frye combines this image with a newspaper photograph showing this man accompanying a congressman with whom the aide had closely worked, thereby implicating the congressman in her death. Thus, video surveillance in Hollywood film is rarely portrayed as possessing an unyielding or unlimited capacity to identify and locate a "bad guy" leading to their capture, punishment or demise. It is only rarely presented as a completely effective retroactive tool to bring criminals to justice on its own. Nonetheless, video surveillance is used consistent with the precautionary logic. Just in case extreme—but in real life, exceedingly rare—instances of murder and robbery may occur, it is plainly prudent to have these systems in place for later advantage if necessary.

Main characters use video surveillance of other characters to advantage in Hollywood film too, a practice sometimes called "lateral" surveillance (see Andrejevic, 2005). How characters were able to create advantage varied. In *Inside Man*, police detective Keith Frazier becomes suspicious of bank robbers who seem to be buying time during a hostage situation in the bank. Recognizing Frazier is suspicious, robbers then position video surveillance to record activity directly inside the bank lobby. In this scene—which viewers watch through a video surveillance monitor—the robbers surround a masked individual. Next, we see the lead robber Dalton Russell shoot this individual and blood disperse as the figure falls to the floor. The robbers use video surveillance to show police—at a safe distance—that they are serious in order to buy more time to accomplish their nefarious aims. In *After the Sunset*, jewel thief Max Burdett creates a diversion to steal a diamond by framing another character for attempting to steal it, thus preoccupying security officers with the other robbery viewed through video surveillance. It was only near Burdett's mission completion that officers notice his robbery. Here characters are imagined using what Marx (2003) termed "counter-surveillance techniques", that is, using surveillance technology against the surveillers. Again, this suggests video surveillance is beneficial not only to officials but to anybody (albeit limited to a great degree by race/ethnicity, class and gender, as discussed below) assumed competent to access or manipulate its presence.

Hollywood film's depiction of the utility of video surveillance for identification and tracking in film fit common assumptions but, surprisingly, not so for its effective deterrent function. None of the 35 films showed video surveillance effectively or completely deterring perpetrators from illegal or unwanted activity. Even if the system was highly sophisticated—such as in *Ocean's Eleven*—characters implemented their plan regardless. In other instances, the obvious presence of video surveillance was ignored during a crime of passion. And on several occasions video surveillance enabled crime, including in *The Italian Job* when a traffic control video surveillance system was hacked to direct a truck carrying gold to a location to be robbed, and as described above, in the *Inside Man*. Hollywood film does not express video surveillance as a useful deterrent to illegal or unwanted behavior, thus again suggesting that while positive associations with video surveillance are expressed it is nuanced.

5.2.2. Video Surveillance Need Not Raise Privacy Concerns or Be Resisted

Hollywood film rarely portrays video surveillance as intrusive, which also normalizes its use. This was consistent across the 35 films. Although several privacy violations were occasionally depicted, they were ignored by characters as such. For example, in *Vacancy* a privacy violation goes unacknowledged since this violation is the least of the worries of the couple now trapped in their hotel room about to suffer a horrific fate. The violation is minimized due to more serious impending events. In *State of Play*, a man holds information about a conspiracy involving a corporation deemed valuable to reporters and wants to avoid identification. However, the subsequent violation of his privacy is downplayed due to the alleged importance of this knowledge. The man is no longer seen as a victim but as the valued key to uncovering a conspiracy. In *American Pie*, the humor created by seeing Jim Levenstein fail sexually leads the viewership to forget the violation of the foreign exchange student's privacy (she was unaware anyone was watching them). She does not even acknowledge the possibility of embarrassment or mortification and by film's end is still communicating with Levenstein. The severe violation is minimized in the comedic context; such a privacy violation via video surveillance is expressed as entertaining and therefore should not raise concern. In his study of several films, Turner (1998, p. 107) had similarly asserted that Hollywood manages to "gloss over the collective anxieties about being spied upon". Overall, these intrusions using video surveillance are minimized, thus helping normalize its use. No films prominently depicted fair notification of video surveillance systems through signage (Lippert, 2009), nor showed the characters using privacy-by-design safeguards (Lippert & Walby, 2015) via, for example, blurring faces within video surveillance images. Only two films (*Enemy of the State* and *Eagle Eye*) of the 35 even noted the deleterious effect on personal privacy that surveillance technologies pose. And while these two films question how much surveillance is necessary, they never express that surveillance of the kinds depicted, including video surveillance, should cease. Thus, although these films at first glance seriously question video surveillance, ultimately they imply it is an inevitable fact of life.

Consistent with the foregoing, twelve films included scenes whereby video surveillance images were neither a preoccupation of characters nor otherwise a focus. Instead video surveillance formed part of the cinematic background. Nothing in these images was plot significant. But this too contributes to normalization. Many of these background images were in security rooms of private companies or government agencies. For instance, in *After the Sunset*, two FBI agents discuss the possibility of a diamond theft with a ship captain while video surveillance images are evident in the background. In *Fracture* and *Panic Room,* video surveillance images flicker in the background of affluent characters' private homes. This use of images constructs video surveillance as normal in workplaces and residences and suggests further that privacy should no longer be expected in these customary private spaces. Video surveillance is prudently already in place to protect against the worst event that might occur there (murder or robbery in the last two films), however unlikely.

Hollywood film does not usually encourage resistance to video surveillance since watchers typically are portrayed using surveillance images appropriately. As noted above, those in authority are usually shown using video surveillance to discover valuable information about suspects. Officials tend not to be depicted abusing their authority by using video surveillance primarily in ways that invade privacy for personal voyeuristic reasons or other immediate self-interest and only secondarily for official business. And those who resist video surveillance tend to do so to protect their criminal identity or otherwise avoid official capture rather than because of a sense of duty to ensure preservation of civil liberties or other ideal principles in the particular institution or broader society.

In nine films, video surveillance was rendered inoperable such that an image was completely inaccessible. This is typically accomplished by blocking, breaking, hacking, or otherwise disabling cameras. For instance, in *Salt*, Evelyn Salt escapes custody from the CIA's headquarters after being accused of spying. She devises an escape by blocking three video surveillance cameras in succession with fire extinguisher foam, then using her underwear to do likewise, and finally shooting a fifth camera's lens. In our sample, the fact a camera no longer functions typically alarms characters who notice, thus underscoring the importance of video surveil-

lance to existing routines and arrangements and thus as proper to everyday life. In *Hostage Part II*, one hostage realizes she is under video surveillance, so to exit the room unnoticed she disables the camera. But the watchers miss seeing this act, leading them to believe events had not transpired as expected. Extra security is summoned. In *The Score*, two guards stationed in a security room monitor a valuable artifact in a secure area through a video surveillance system's bank of monitors. But several screens suddenly momentarily go dark due to thieves seizing control of the system as one thief slowly maneuvers to steal the artifact without the guards noticing. One security guard blames the outdated system. After several minutes, however, the lead guard becomes suspicious and sends three others to investigate. With guards en route, the surveillance system suddenly is made operational again and the lead guard discerns an unauthorized person in the secure area through a monitor. Viewers learn the system had not malfunctioned; it merely had been purposely hacked. Typically, in the films the cause of concern is ultimately shown to be illegal or illicit activity, rather than the numerous technological malfunctions or limitations inherent to video surveillance, including image transfer (see Walby & Lippert 2015; Wilkinson & Lippert, 2012).

The blockage or disabling of a video surveillance system, thus preventing a character's image from being captured and displayed, is a form of resistance that Marx (2003) labels "breaking". Depicting this to some degree fits the notion of film's critical potential in relation to surveillance observed by Kammerer (2004). Yet, such crude resistance is typically not portrayed as administered by an average citizen but instead by criminals avoiding capture. Thus, the films' message is that such crude resistance is an inappropriate way for the upright citizen to respond to harmful effects of video surveillance. Moreover, citizens need not resist video surveillance, unless they have something to hide from authorities. As Hollywood film scenes enter our gaze in theaters and living rooms, and increasingly via new devices (e.g., tablets and smart phones) and websites (e.g., Netflix), they carry with them the proliferating real world "nothing to hide" argument (Solove, 2007) and thus help normalize video surveillance. If you have nothing to hide, why not allow video surveillance to operate, proliferate, and oversee daily life?

5.2.3. Only Some People Are Video Surveillance Competent

Surprisingly, in our film sample we found racial/ethnic minorities and women are not disproportionately portrayed as the targets of video surveillance. However, Hollywood film grants disproportionate permission to gaze through video surveillance or to use the visual information in its images to White, middle class, middle-aged men, largely excluding minorities and women from the powerful position of watcher or surveiller. The epitome of this is the critically acclaimed *Cabin in the Woods*, showing for much of the film two professional White men in front of a bank of video surveillance monitors accordingly orchestrating events unbeknownst to the characters. Of 70 pertinent scenes from the 35 films, 61 show White men as watchers, 31 scenes portray only White men, and 43 scenes feature only men of any apparent race as surveillers. Consistent with video surveillance depicted operating in affluent private residences noted above, no lower class persons, as identified through character back stories or their depicted occupations, are portrayed as surveillers. Moreover, racial/ethnic minorities are rarely depicted as surveillers without being accompanied by White men. In our sample women are often depicted as both surveiller and surveillance target but when portrayed as surveillers they are more often accompanied by men rather than watching on their own. Thus, racial/ethnic minorities and women tend to be shown as largely incapable of operating surveillance technology and interpreting the meaning of its images without White men's presence. Similar to Lake's (2010, p. 232) remark about contemporary cinema, Hollywood film tends to restrict who is allowed to watch and thereby limits the power accompanying this vantage point to a select group. Thus, video surveillance may be expressed in positive terms in Hollywood film, but the message is again more nuanced: not everyone can or should be trusted to use it.

5.2.4. Neglect Video Surveillance and Its Malfunctions at Your Peril

Often films portray video surveillance capturing events in-the-moment while no characters watch video monitors. But the images characters fail to observe would have served their interests. For example, in *Hostage Part II*, people bid for the opportunity to harm innocent others. In the killing ground, viewers see a surveillance image of a hostage taking control of her hired assailant while security guards neglect to notice this act in the monitors. This suggests these events were preventable had they been watched; the inability of humans to keep up with video surveillance prevents receipt of valuable information. But the films nonetheless portray video surveillance as a reliable means of accessing the truth and thus worthy of acceptance into everyday life.

In some scenes it is humanly impossible for characters to pay full attention to the surveillance images. For instance, in *Snake Eyes*, Rick Santoro is sifting through 1,500 video images in a casino's security room to search for a suspect. While he focuses on one surveillance image the person of interest happens to walk through another image directly adjacent to Santoro. In several other films, there is simply no one near to notice the crucial video image. In *Inside Man* described

earlier, for instance, Dalton Russell stops video surveillance's functioning in the bank prior to commencing the robbery by using an infrared beam. Concurrently, viewers see the bank's security room where video surveillance is malfunctioning and no security guards present to notice. The utility of the technology is slowed by its operators or eliminated by their absence. Thus, film conveys the notion that video surveillance is limited by human failure (see also Kammerer, 2004) and there is no obvious reason to doubt the effectiveness of video surveillance on its own. However, Hollywood film's very inclusion of humans in these arrangements, befitting Gad and Hansen's (2013) assertion noted above, suggests that surveillance is best understood as a complex assemblage of technology and humans.

Only a few films in the sample express that video surveillance cannot be trusted due to the possible alteration of its images. In *Eagle Eye*, a computer with artificial intelligence is executing an elaborate plan by manipulating people to murder others. While passing through an airport screening point, a security guard takes her eyes off the x-ray bag scanning screen. At that moment the image is altered to depict random mundane items rather than the characters' syringe injectors, thus allowing the main characters to pass through and avoid capture. Had the screener not looked away, however, she would have noticed this alteration. In *Ocean's Eleven*, a video surveillance image depicts Linus Caldwell standing in a secure elevator leading to the casino vault he intends to rob. While there, the video surveillance operator is distracted and viewers watch Caldwell's image replaced with an image of an empty elevator. Again, had the operator not been distracted, the image alteration arranged by Ocean and his gang would have been noticed, leading to their apprehension and failure. Scenes expressing any doubt about authenticity were almost evenly distributed between images that were after-the-fact and in-the-moment, which contrasts with literature that suggests doubt is observed more often about after-the-fact images (Levin, 2002). But while video surveillance images are at least sometimes portrayed as alterable, this alteration would be noticed only if humans had paid proper attention. Thus, even when alteration occurs, it could be avoided but for human error. This discourse expresses as well the extent of our current reliance on video surveillance technologies such that once they stop functioning one *should* feel uneasy because it means a harmful act outside routine is afoot. Video surveillance is a technology becoming so embedded in everyday life that concern is apt when witnessing a system "malfunction".

6. How Hollywood Is Attached to a Video Surveillant Assemblage

Most previous research takes the flow of Hollywood films for granted, ignoring that this is a key process that constitutes assemblages; if films are unavailable to watch, what they express is irrelevant. Just as there is growing video surveillance in everyday life, the means by which to create and reach a viewership is expanding too. The three "traditional" means of film reaching a viewership are a theater, television (whether via antenna, satellite or cable), and home rental of first videotape and now DVDs of Hollywood films. Now Netflix and similar corporate services deliver Hollywood films chosen by viewers direct to living rooms and onto nearly every new portable device with a screen to be watched in all spaces imaginable. From classrooms to washrooms to public buses to automobiles, Hollywood film can now be watched nearly anytime, anywhere.

Film is both a material link and a communication format; video surveillance images in Hollywood are grafting normalizing expression onto a broader video surveillant assemblage through various means. To the extent films used real video surveillance technology to produce the surveillance images positioned within them (a practice suggested by the distinctive quality of video surveillance images) such as "crudeness, starkness, and graininess" (Doyle, 2006, p. 210) within the larger films, as well as their flickering, shuddering, black and white, and/or dark appearance) that contrast with the film itself (clear, smooth, color, and/or light), this troubles the distinction between the "real" and "the illusory". Indeed, though difficult to establish with certainty, only in a few films did the surveillance images seem simulated, such as in *Fracture* when the images are undergoing police analysis, rather than being a product of real video surveillance technology. To the extent actual video surveillance technology is used to produce the images this way it serves as a specific instance of Zimmer's (2011) broader point about film as the practice of surveillance and suggests how Hollywood is becoming attached to a surveillant assemblage. This means too there is a sense in which when these images are used in film they are not "fake", since the meaning of that term becomes unclear here. The moment of the surveillance image's arrival in film, is the moment of attachment of Hollywood (and all that term represents with its accompanying institutions of production, marketing and dissemination) film to a broader video surveillant assemblage.

In most films, consistent with the foregoing discourses, video surveillance is also portrayed as having a capacity to access reality, to access the truth consistent with the popular notion that "the camera never lies" and in so doing normalizes its use to achieve this vital multi-purpose function. Hollywood film uses video surveillance images in ways that fit this dominant media logic. Here too the video surveillance image troubles the relation between "the real" and "the illusory". Yet the deployment of surveillance images in this way is potentially unstable and may problematize what it ex-

presses. This is because the "realness" of the image and the fictional quality of the broader film in which it is placed contrast. Put differently, the aim to render the film more real comes with the contradictory message that all that happens before and after the image is fiction. When it comes to video surveillance, what Hollywood film expresses is not without nuance, nor is it seamless.

7. Conclusion

This article has extended previous research, surveillance studies, and film studies by exploring how Hollywood film shapes the understanding of the promotion and reception of video surveillance. Normalization of video surveillance occurs in multifaceted ways in Hollywood film. Undoubtedly this normalization has occurred within film production circles; the use of video surveillance as a filmic device to advance a plot in Hollywood film[5] has been normalized. But we think normalization is not limited to this: film's wider expressive normalizing effects and material links beyond itself matter too. If Hollywood film is entirely self-referential, it is unclear we ought to study it any more than we might study the content of a closed circuit video surveillance system. By normalization we mean to suggest how video surveillance in film is accepted far beyond film in the broader society as well and becomes part of a broader surveillant assemblage.

From our analysis emerged four dominant discourses. Hollywood expresses that video surveillance can identify and locate people to advantage and need not raise privacy concerns or be resisted by citizens. Only some kinds of people are competent to use video surveillance and everyone neglects its products and "malfunctions" at their peril. These dominant discourses in Hollywood films help facilitate normalization of video surveillance by assigning it positive attributes, albeit not blithely so. Hollywood also expresses that video surveillance can be used to great advantage, usually coupled with other means; it can be resisted (albeit crudely by criminals or immoral persons with something to hide); and it does not deter. However, overall our results support the notion that Hollywood film conveys video surveillance as a necessary and inevitable component of everyday life; surveillance is typically experienced by characters as largely benign and unobtrusive (Murakami-Wood & Webster, 2009, pp. 266-267). These discourses support earlier accounts about the malfunction of surveillance being attributed to human error (Kammerer, 2004) too and that only some people (mostly White, middle-class men) are competent surveillers (Lake, 2010). When the 35 films from across genres are considered together they appear to coincide mostly with Turner's (1998) view of the ideological function of Hollywood film in relation to surveillance.

More broadly the foregoing suggests that film and related media formats are part of surveillant assemblages. Their often coarse scenes scratch away at smooth sheets of trust that used to characterize the liberal democratic institutions and public spaces they depict, laying bare tiny trenches for seeds of suspicion to germinate and grow. Here trust in institutions to adequately manage risk (of every conceivable harm—Ericson, 2007) and the presumption of innocence of all institutional actors involved in such efforts are replaced with suspicion and pre-emption consistent with a precautionary logic. Accordingly video surveillance is portrayed in film as safely spreading through these newly carved pathways or already positioned to watch for the impending institutional disaster in case it comes that way, however far-fetched its appearance is forecast to be. This message hinders critical analysis, discourages appropriate resistance to video surveillance use and growth in light of its harmful effects, especially on privacy, and facilitates its spread in the wider society. Hollywood film is only one avenue by which video surveillance is normalized, but its increasing incorporation of video surveillance and its vast reach and appeal renders it a significant one. If Hollywood film is becoming discursively and structurally attached to a surveillance assemblage it commences a demand that scholarship draw from both the humanities and the social sciences for adequate understanding of these arrangements. Future scholarship needs to explore dominant discourses in other forms of contemporary popular culture to understand how and why surveillance society continues to so rapidly emerge as well as how to construct alternative critical discourses, informed by privacy principles and humanism.

Acknowledgments

The authors wish to thank the issue editors and anonymous reviewers for their detailed and exceedingly helpful comments on an earlier draft of this article.

Conflict of Interests

The authors declare no conflict of interests.

References

Albrechtslund, A. (2008). Surveillance and ethics in film: Rear window and the conversation. *Journal of Criminal Justice and Popular Culture*, *15*(2), 129-144.

Albrechtslund, A., & Dubbeld, L. (2005). The plays and arts of surveillance: Studying surveillance as entertainment. *Surveillance & Society*, *3*(2/3), 216-221.

[5] We thank one of the remarkably helpful anonymous reviewers for this point.

Andrejevic, M. (2004). *Reality TV: The work of being watched*. Oxford: Rowman & Littlefield Publishers.

Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *3*(4), 479-497.

Babbie, E., & Benaquisto, L. (2002). *Fundamentals of social research* (1st ed.). Scarborough: Thomson-Nelson.

Barnard-Wills, D. (2011). UK news media discourses of surveillance. *Sociological Quarterly*, *52*(4), 548-567.

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

Bogard, W. (2006). Surveillance assemblages and lines of flight. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 97-122). Devon: Willan Publishing.

Carroll, R. (2013, November 4). California police use of body cameras cuts violence and complaints. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/nov/04/california-police-body-cameras-cuts-violence-complaints-rialto

Deleuze, G., & Guattari, F. (1987). *A thousand plateaus*. Minneapolis: University of Minnesota Press.

Dinkes, R., Kemp, J., Buam, K., & Synder, T. (2009). *Indicators of school crime and safety: 2009*. Washington, DC: National Center for Education Statistics, Institute of Education Sciences, U.S. Department of Education, Bureau of Justice Statistics, Office of Justice Programs, and U.S. Department of Justice.

Doyle, A. (2003) *Arresting images: Crime and policing in front of the television camera.* Toronto: University of Toronto Press.

Doyle, A. (2006). An alternative current in surveillance and control: Broadcasting surveillance footage of crimes. In K. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 199-224). Toronto: University of Toronto Press.

Doyle, A., Lippert, R., & Lyon, D. (2012). Introduction. In A. Doyle, R. Lippert & D. Lyon (Eds.), *Eyes everywhere: The global growth of Canada surveillance* (pp. 1-19). London: Routledge.

Doyle, A., & Walby, K. (2012). Selling surveillance: Introduction of videos in Ottawa taxis. In A. Doyle, R. Lippert & D. Lyon (Eds.), *Eyes everywhere: The global growth of Canada surveillance* (pp. 185-201). Toronto: Routledge.

Ericson, R. (2007). *Crime in an insecure world*. Cambridge: Polity Press.

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

Gad, C., & Hansen, L. (2013). A closed circuit technological vision: On minority report, event detection and enabling technologies. *Surveillance & Society*, *11*(1/2), 148-162.

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

Haggerty, K. (2006). Tear down the walls: On demolishing the panopticon. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 23-45). Cullompton: Willan.

Jamieson, P., & Romer, D. (2014). Violence in popular U.S. prime time TV dramas and the cultivation of fear: A time series analysis. *Media and Communication, 2*(2), 31-41.

Kammerer, D. (2004). Video surveillance in Hollywood movies. *Surveillance & Society*, *2*(2/3), 464-73.

Kammerer, D. (2012). Surveillance in literature, film and television. In D. Lyon, K. Haggerty, & K. Ball (Eds.), *Routledge handbook of surveillance studies* (pp. 99-106). New York, NY: Routledge.

Lake, J. (2010). Red Road (2006) and emerging narratives of "sub-veillance". *Continuum: Journal f Media & Cultural Studies*, *24*(2), 231-240.

Levin, T. (2002). Rhetoric of the temporal index: Surveillance narration and the cinema of "real time". In T. Levin, U. Frohne, & P. Weibel (Eds.), *CTRL [space]: The rhetorics of surveillance from Bentham to Big Brother* (pp. 578-593). Cambridge, MA: MIT Press.

Lippert, R. (2009) Signs of the surveillant assemblage: Urban CCTV, privacy regulation and governmentality. *Social and Legal Studies*, *18*(4), 505-522.

Lippert, R., & Wilkinson, B. (2010). Capturing criminals, crime, and the public's imagination: assembling crime stoppers and CCTV Surveillance. *Crime, Media, Culture*, *6*(2), 131-152.

Lippert, R. & Walby, K. (2015). Governing through privacy: authoritarian liberalism, privacy law, and privacy knowledge. *Law, Culture, and the Humanities*, *13*(1), early online version.

Lyon, D. (2002). Editorial. surveillance studies: Understanding visibility, mobility and the phenetic fix. *Surveillance & Society*, *1*(1), 1-7.

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

Marks, P. (2005). Imagining surveillance: Utopian visions and surveillance studies. *Surveillance & Society*, *3*(2), 222-239.

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

McCahill, M. (2003). Media representations of visual surveillance. In P. Mason (Ed.), *Criminal visions: Media representations of crime and justice* (pp. 192-213). Devon: Willian Publishing.

Monahan, T. (2006). Questioning surveillance and security. In T. Monahan (Ed.), *Surveillance and security: Technological politics and power in everyday life* (pp. 1-23). New York: Routledge.

Monahan, T. (2010). *Surveillance in the time of insecurity*. New Brunswick: Rutgers University Press.

Monahan, T. (2011). Surveillance as cultural practice.

The Sociological Quarterly, *52*, 495-508.

Murakami-Wood, D. (2013). What is global surveillance? Towards a relational political economy of the global surveillant assemblage. *Geoforum*, *49*, 317-26.

Murakami-Wood, D., & Webster, C. (2009). Living in surveillance societies: The normalization of surveillance in Europe and the threat of Britain's bad example. *Journal of Contemporary European Research*, *5*(2), 259-273.

Murakami-Wood, D., & Webster, C. (2011). The normality of living in surveillance societies. *Information Technology and Law Series*, *20*(3), 151-164.

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: The rise of CCTV*. Oxford: Berg.

Rose, G. (2007). *Visual methodologies: An introduction to the interpretation of visual materials* (2nd ed.). Los Angeles: Sage.

SCAN (2009). Surveillance camera awareness network—*A report on video surveillance in Canada*. Kingston, Canada: The Surveillance Project, Queen's University.

Solove, D. (2007). "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745-772.

Stewart, G. (2012). Surveillance camera. *Film Quarterly*, *66*(2), 5-15.

Turner, J. (1998). Collapsing the interior/exterior distinction: Surveillance, spectacle, and suspense in popular cinema. *Wide Angle*, *20*(4), 93-123.

Verga, S. (2010). *Closed-circuit TV surveillance evaluation: statistical analysis of the effects on rates of crime*. Ottawa, Canada: Technical Report. Defense Research and Development Canada, Centre for Security Science.

Walby, K. (2006). Little England? The rise of open-street closed-circuit television surveillance in Canada. *Surveillance & Society*, *4*(1/2), 29-51.

Walby, K., & Lippert, R. (2015). *Municipal corporate security in international context*. New York: Routledge.

Wilkinson, B., & Lippert, R. (2012). Moving images through an assemblage: Police, visual information, and resistance. *Critical Criminology*, *20*, 311-325.

Zeilinger, M. (2012). Appropriation and the authoring function of video surveillance in Manu Luksch's *Faceless*. In A. Doyle, R. Lippert, & D. Lyon (Eds.), *Eyes everywhere: The global growth of Canada surveillance* (pp. 262-273). London: Routledge.

Zimmer, C. (2011). Surveillance cinema: Narrative between technology and politics. *Surveillance & Society*, *8*(4), 427-440.

About the Authors

Dr. Randy K. Lippert

Randy K. Lippert is Professor of Criminology at the University of Windsor, Windsor, Canada where he teaches in the areas of policing and security, surveillance, and socio-legal studies. He is currently debates editor for the international journal *Surveillance and Society* and Thinker-in-Residence at Deakin University in Geelong, Australia. He has published more than 60 refereed articles and chapters and six books, including, *Policing Cities: Urban Securitization and Regulation in a 21st Century World* (2013) and *Municipal Corporate Security in International Perspective* (2015), both with Kevin Walby.

Jolina Scalia

Jolina Scalia is a researcher with the Government of Alberta, Canada. She holds an Honors B.A. in criminology and psychology and an M.A. in criminology from the University of Windsor, Windsor, Canada.

Appendix 1. The Hollywood film sample.

1. 15 Minutes. Directed by John Herzfeld, 2001.
2. 21. Directed by Robert Luketic 2008.
3. After the Sunset. Directed by Brett Ratner, 2004.
4. American Pie. Directed by Paul Weitz, 1999.
5. The Bourne Ultimatum. Directed by Paul Greengrass, 2007.
6. Dawn of the Dead. Directed by Zack Snyder, 2004.
7. Eagle Eye. Directed by D.J. Caruso, 2008.
8. Enemy of the State. Directed by Tony Scott, 1998.
9. Fracture. Directed by Gregory Hoblit, 2007.
10. Hall Pass. Directed by Bobby Farrelly and Peter Farrelly, 2011.
11. Hostel Part II. Directed by Eli Roth, 2007.
12. Inside Man. Directed by Spike Lee, 2006.
13. The International. Directed by Tom Tykwer, 2009.
14. The Italian Job. Directed by F. Gary Gray, 2003.
15. Knight and Day. Directed by James Mangold, 2010.
16. The Manchurian Candidate. Directed by Jonathan Demme, 2004.
17. Ocean's Eleven. Directed by Steven Soderbergh, 2001.
18. Panic Room. Directed by David Fincher, 2002.
19. A Perfect Getaway. Directed by David Twohy, 2009.
20. Salt. Directed by Phillip Noyce, 2010.
21. Saw II. Directed by Darren Lynn Bousman, 2005.
22. The Score. Directed by Frank Oz, 2001.
23. Showtime. Directed by Tom Dey, 2001.
24. Snake Eyes. Directed by Brian De Palma, 1998.
25. Spy Games. Directed by Tony Scott, 2001.
26. State of Play. Directed by Kevin Macdonald, 2009.
27. Street Kings. Directed by David Ayer, 2008.
28. Traitor. Directed by Jeffrey Nachmanoff, 2008.
29. Vacancy. Directed by Nimród Antal, 2007.
30. Vantage Point. Directed by Pete Travis, 2008.
31. Dark Skies. Directed by Scott Stewart, 2013.
32. Cabin in the Woods. Directed by Drew Goddard, 2012.
33. Paycheck. Directed by John Woo, 2003.
34. The Judge. Directed by David Dobkin, 2014.
35. Run All Night. Directed by Jaume Collet-Serra, 2015.

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 3, Pages 39-55
Doi: 10.17645/mac.v3i3.292

Article

The New Transparency: Police Violence in the Context of Ubiquitous Surveillance

Ben Brucato

Center for Humanistic Inquiry, Amherst College, Amherst, MA, 01002, USA; E-Mail: ben@benbrucato.com

Submitted: 13 April 2015 | In Revised Form: 21 July 2015 | Accepted: 10 August 2015 |
Published: 20 October 2015

Abstract
Media and surveillance scholars often comment on the purported empowering quality of transparency, which they expect participatory media to promote. From its Enlightenment origins, transparency is related to accountability and legitimacy: its increase is believed to promote these. It has earned a position as an unassailed, prime normative value in contemporary liberal and social democracies. Though still valued, transparency is undergoing change in an era of ubiquitous surveillance. Publics still anticipate governmental and corporate self-disclosure and for such entities to operate visibly; but increasingly, deliberate and incidental surveillance by a range of sources, both institutional and informal, documents the activities of such authorities. More often, civilians participate in producing or amplifying transparency. This article explores this new transparency through a study of U.S. police, focusing on the discourse of police accountability activists and cop watchers to describe how their work adapts traditional notions of transparency. Recognizing the resilience of the police institution despite the new visibility of its violence, the article challenges the presumption that increased transparency will promote institutional reform or crisis. It concludes with a critical comment on prominent expectations that promoting the visibility of police can protect publics and ensure police accountability. This conclusion has implications for other forms of the new transparency, including whistleblowing (e.g., Edward Snowden) and leaking (e.g., WikiLeaks).

Keywords
accountability; Jeremy Bentham; cop watch; legitimacy; media participation; police; Jean Jacques Rousseau; sousveillance; surveillance; transparency

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

1. Transparency, Then and Now

If I were to mobilize a common trope, describing transparency as a "contested term," it would exaggerate the extent to which the word is used with much care or reflexivity. In fact, transparency is a ubiquitous term but is rarely qualified or operationalized; there is a near-absence of contention over its meaning though its significance is rarely clear. This article historicizes contemporary accountability practices, with an extended case study of police accountability activism, showing the intellectual and practical connections from these practices to a political concept rooted in Enlightenment political thought. Transparency is also an unassailed and treasured concept, despite its being taken for granted (Birchall, 2011b; Han, 2012). By raising key features of the historical and ideological origins of the concept, the article suggests transparency's inextricable connections to a degraded form of democracy and harbors widely maligned presumptions about information, knowledge, and their connection to political action.

By placing media studies in conversation with the emerging field of surveillance studies, this article demonstrates how the two can contribute to one another. Like the concept of transparency, an enduring

challenge in each field of inquiry is the presumption that participation in producing media artifacts has self-evidently positive normative value and that it has certain political efficacy. Which politics undergird the position that amateur journalism and participatory media are inherently empowering to publics? Through the use of political theory, this article contributes an answer, one that probes the origins of transparency for guidance and elucidates concerns central in these fields today.

Johnson and Regan (2014) take transparency to mean "a practice that is explicitly targeted to achieve accountability" (p. 1). From its modern normative origins, transparency is visibility combined with some standard of moral regulation that holds individuals or organizations to account. Surveillance adds strategic watching in order to produce that visibility, making available its objects to those agents of a defined regulatory scheme, often performed by or for those with comparatively greater power or authority than those being watched. Political transparency inverts the surveillant gaze, as governments and their agents are made visible to their publics, most often via self-disclosure, and has its origins in practical development of Enlightenment ideals in the construction of modern democratic states (Birchall, 2011b). Hood (2006) claims transparency is "quasi-religious" in nature, not because it suggests the unmediated visibility of an omniscient god—though it certainly connotes this—but because it represents the pinnacle of righteousness in secular democracies. One behaves transparently in public, among fellow citizens, to be held accountable for speech and action.

In this first section, I begin with the Enlightenment origins of the concept of transparency as it relates to its use in discourse about policing's new visibility. My argument is that policing's new visibility suggests a particular history of transparency, provided below and framing the case study that follows. Andrew J. Goldsmith (2010) first applied John B. Thompson's (2005) conception of the new visibility to police. In the following section, I provide a case study of cop watching. Cop watching emerged in the 1990s as an organized political movement by activists who deliberately recorded police stops in order to document and deter police violence. In this century, cop watching has become increasingly incidental, performed by individuals more often than organizations. People increasingly have a digital camera with them at all times, for instance as a feature on their smart phones. More importantly, police accountability activists promote serendipitous cop watching by civilians, seizing upon already widespread participation in the documentation of everyday life. This case study reveals that the new visibility has adapted the Enlightenment normative and political ideal for transparency, such that the kind of visibility they produce has become identified with political transparency. New activities (e.g., participatory media) and related technologies have become central to how transparency is enabled and produced in many contemporary societies. The new transparency[1] identifies the ocular visibility provided by digital technologies with the Enlightenment concept, and strengthens its ideological connection to expectations for accountability and legitimacy.

Similar changes in transparency are occurring elsewhere in contemporary discursive and political activity. I close with comment on how transparency is everywhere being reasserted through these activities. In the next section, this history of modern transparency is conceptually bounded by its relevance to the case study. In this regard, I aim to find in the origins of the ideal of transparency the logics that enable the present. More importantly, the case illustrates ways the practice of transparency has changed, specifically by emphasizing the broad public participation in producing transparency, rather relying on the self-disclosure and publicity of political officials and functionaries.

1.1. The Enlightenment Origins of Transparency

Though he never used the term, Jean-Jacques Rousseau believed transparency was the pre-civilization condition of the state of nature (Hood, 2006). Nothing in human nature had changed, but in the lost state of nature, people "found their security in the ease with which they could *see through* one another and this advantage, of which we no longer feel the value, prevented their having many vices" (Rousseau, 1913, p. 132, emphasis added). This seeing through articulates a literal meaning of transparency. For Rousseau, the opaqueness of citizens within the modern city represented a threat to social order. Though Rousseau considered transparent relations among citizens as an *intrinsic* virtue and opaque relations as an intrinsic vice, he also valued transparency as an *instrumental* good, as a social condition that is necessary for civic cooperation (Hill, 2006).

Visibility is a precondition for social regulation, enabling virtue and the potential for guarding against vice. In the political realm, visibility entailed *publicity*. Rousseau held that public servants ought to perform "in the eyes of the public," and "to permit no office-holder to move about *incognitio*" (in Hood, 2006, p. 7). Here we find in publicity the roots of the contemporary conception of political transparency as a condition where political officials, organizations, and policies are publicly visible in order to be held to account. Public

[1] I am not the first to use this term. The Surveillance Studies Centre at Queen's University has had a multi-year research initiative called The New Transparency. I intend no association, neither practically nor conceptually. I use this term to associate John B. Thompson's (2005) concept of the new visibility with the political concept of transparency.

visibility was an assurance against an accumulation of vices among individuals, and this applied just as well to public officials. In moral relations, if transparency is instrumental, a means rather than an end, then accountability is its end. On the other hand, if political transparency is a means, then *legitimacy* is its end. This legitimacy is—partly, though necessarily—earned through visibly displaying reliable accountability. Fundamental to the Enlightenment project of the democratic state was "to make power visible—to illuminate it" (Andersson, 2008, p. 1). Though early modern states abandoned Rousseau's insistence on direct, participatory republicanism, his desire for transparency by way of publicity was influential. For instance, Kant's adaptation of Rousseau argued that popular acceptance legitimates governance (Davis, 1991), and so political transparency came to be a means of achieving a properly representative government (Birchall, 2011b; Heald, 2006). Transparency was a means of reconciling the "vertical inequality" between law-makers and citizens (Machin, 2012).

Just as important since its inception was the modern state's deep dependence on surveillance (Torpey, 2000). Jeremy Bentham coined the term transparency and with the maxim that "the more strictly we are watched, the better we behave" (in Hood, 2006, p. 9).[2] This at least nominally applied to public officials, but it practically applied to citizens. While Rousseau's desire was for citizens to self-disclose to one another, Bentham's intention was additionally to maintain social security by compelling their disclosure to the state. Bahmueller explained that for Bentham, "The persons and objects of that [social] world must be weighed and counted, marked out and identified, subjected to the brightness of the public light, the better to be seen by the public eye. Only then could they be controlled and security made possible…" (in Hood, 2006, p. 8). When transparency—as moral regulation—merges with the state, it takes on this police function and as a matter of existential demand. Nicholas de La Mare's "police science" in his *Traité de la Police* in 1713 articulated strategies for the prevention of disorder that emphasized street lighting and open spaces, optimizing public view and surveillance (Hood, 2006). This early approach to *policy* shows a technocratic orientation to transparency, where the visibility of citizens was made a function of the built environment. Nonetheless, for Bentham, transparency of public officials was to be assured through reporting practices and was intended to make officials just as subjected to the public as prisoners were in his panopticon. Importantly, the motivation for this ubiquitous transparency was not the assurance of democracy, but of security. Bentham provides a particular reference point in the genealogy of the relatedness of transparency and surveillance, particularly by virtue of their nexus in the state. As I argue below, the new transparency is partly defined by the extent to which transparency and surveillance have become inseparable.

As the modern state developed, political transparency was seen as a prerequisite for or even an assurance of accountability of officials or bureaucracies. Here, it became a result of rules being publicized, procedures being predictable, and the self-disclosure of institutionally empowered actors demonstrating conformity to these standards (Hood, 2006; Tyler, 2006). Since transparency was seen to enable accountability, its successful performance would allow for legitimacy to be reproduced. David Beetham's (1991) influential account of legitimacy explains legitimacy rests on conformity to *known* rules. Legitimacy, then, requires transparency because rules must be displayed, seen, and understood by publics, and that understanding should result in a perceived coherence between institutional standards and community norms (Levi et al., 2009). These rules rely on broadly shared beliefs or norms, and legitimation is formally expressed through public consent, demonstrated through widespread, voluntary submission to the rule of law and its enforcement, and demonstrated by trust in representatives and agents of government. For instance, Sir Robert Peel's influential principles for policing in 1829 emphasized the role of public consent to be policed through willing cooperation (Chrismas, 2013; Tyler & Fagan, 2008).

Transparency was core to the idealization of the social pact in modern states. The rule of law demands legitimate governments follow the rules that govern its institutions with the same reliability with which the governed are expected to conform to the rules that govern publics (Tyler, 2006). In democratic societies, legitimacy is important because it fosters self-restraint by the dominant and governing institutions, as well as cooperation and compliance by the governed (Tyler & Fagan, 2008). This is conditioned on appearances, not simply promises (Tyler, 2006). The performances of institutions must be transparent in that they visibly demonstrate accountability to agreed-upon standards. Without this visibility, institutions cannot be legitimated, and without such legitimacy, they cannot successfully administrate democratic societies. Accountability is not automatic, though the need for legitimacy ensures it. The transparent state by revealing its accountability processes function reliably may only then produce the consent of the governed. Even still, this is a necessary but insufficient condition (Machin, 2012). According to this model, when legitimacy is absent in-

[2] Johnson and Regan (2014) explain that surveillance and transparency are rarely studied under the same lens. That transparency emerges as a discourse with Bentham has a particular irony after Michel Foucault (1979) appropriated Bentham's panopticon, where this prison model functions as a metaphor for the modern societies.

stitutions crumble in the face of social unrest, or rely on the successful use of violent force to suppress uprisings. The axiom of this model is that without legitimacy, either democracy or governments fail.

While the criticisms of the model are well known (e.g., O'Kane, 1993), it profoundly influenced the constitution of representative democracies. Moreover, the ideal of transparency has inspired—and continues to—social movements to strengthen democratic citizenship. Such movements should be expected in some measure as a consequence of the degraded status of the citizen relative to the very structures and functions of political institutions fostered by this model.

The following will explain how this modern conception of transparency has been preserved, adapted, and is even amplified within the new transparency, an outcome both of the performances of a surveillance society, and the mythos of what Byung-Chul Han (2012) has called *transparenzgesellschaft*, or the "transparency society."

1.2. Transparency in Transition

If transparency relies on visibility, then the means by which persons are made apparent is crucial. During the latter half of the twentieth century, and especially since, these means have undergone significant transition, and so then transparency is in transition. David Lyon (2001) recognizes, like Rousseau, that "disappearing bodies is a basic problem of modernity" but this problem "has been accentuated with the growth and pervasiveness of communication and information technologies" (p. 15). Surveillance societies are those that "depend on bureaucratic administration and some kinds of information technology" (Lyon, 2007, p. 11) and have turned to deliberate, routine protocols and techniques "to make distant bodies reappear" (Lyon, 2001, p. 15). Surveillance is now fundamental to the production of visibility.

Transparency not only connotes public visibility, but functions through it. Imaging technologies have become crucial in what is publicly visible, and information and communication technologies have changed the form and scale of the dissemination of images (Thompson, 2005). Without these technologies, visibility is often bidirectional: one available to be seen can see the watcher (Lyon, 2001). Police and surveillance in early modern states relied on techniques more than on technologies for making the public visible for regulatory purposes (Ellul, 1964; Neocleous, 2000; Torpey, 2000). Surveillance etymologically suggests a comparatively powerful entity *watching over* the actions of subordinated persons (Mann, Nolan, & Wellman, 2003). Imaging technologies enable this kind of oversight, and are approaching ubiquity in the Global North (Lyon, 2007). The extent to which photographic and video surveillance has come to inform the connotation of surveillance indicates broad recognition that many experience surveillance when the watcher is potentially—and often is—hidden to those being watched (Koskela, 2003). Not only is visibility mediated, but the watchers and the watched negotiate with imaging technologies to modulate their visibility, often, though not always, producing a hidden, remote watcher (Marx, 2009).

The broadly shared experience of being watched has been normalized, such that publics have internalized the surveillant gaze of the state (Foucault, 1979; Marx, 2006). Complying with laws and social norms is partly a result of feeling one is being watched even if the watchers are not apparent. This is the most fundamental aspect of the panopticon metaphor, that publics subconsciously recognize the possibility of being watched at any moment (Lyon, 2006). Panoptic surveillance is an attempt at an efficient solution to when total transparency is infeasible, one intended to manufacture voluntary submission to regulation. A powerful criticism suggests that surveillance regimes are not so totalizing in consequence as the panopticon metaphor suggests, as watchers carefully select among various publics key populations to monitor and regulate (Hier, Walby, & Greenberg, 2006; Norris & Armstrong, 1999). This suggests that surveillance has not resulted in the ubiquity that the ideal for transparency would advocate. The ideal of transparency would suggest the surveillant gaze is too discriminatory, and is in need of "democratization" (Hier, 2003).

Surveillance for over a century, and increasingly over the past decades, has involved imaging technologies that produce durable, archivable artifacts: *documentations*. Not only are watchers able to be hidden to those they surveil, but the visual field is also no longer bound by spatial and temporal co-presence of watcher and watched (Thompson, 2005). Being ephemerally visible is insufficient; transparency now requires a record, and that record must also be archived and available to be accessed. Negotiations over who can see what, how, and when have been the primary substance of discourse about and political contentions over information transparency (Turilli & Floridi, 2009). New technologies have allowed for hidden and remote viewing of the documentations thereof. Though the ideal of information transparency would call for documentations to be universally available, their distribution has been historically determined or filtered by virtue of political-economic power, discussed further in the next section.

The methods of making bodies visible are various, but the effect of such surveillance is to render the body as an object of classification and record (Bruno, 2011; Crary, 1992; Sekula, 1978). Powerful institutions and the privileged actors therein have access to technologies, techniques, and institutions that enable control over the visible body for the purposes of direction, pro-

tection, and administration (Lyon, 2001). Deviant and criminal activities are made visible and archived as a result of surveillance in ways it could not have otherwise without imaging and database technologies. Photographic and video surveillance regularly produces evidence used to incarcerate. Those in surveillance societies are familiar with the success of surveillance in making people subject to the disciplinary functions of the criminal justice system. Yet, everyday life also provides experience of the success of surveillance techniques in providing security, productively directing behaviors, and delivering benefits—and occasionally risks unique to surveillance activity, such as what has been named "identity theft."

For the Enlightenment democratic ideal, bidirectional transparency was essential. The state and its populace required for their security both to render the public visible and on popular submission to surveillance. Just as important, the public was meant to watch state actors as a check on their authority. Because states have economic and technical resources to procure and control surveillance technologies, and because they are legally enabled to use them, this bidirectionality exists mostly in principle, rarely in practice. People in surveillance societies have a wealth of experience of the inequity in distribution of surveillance capacities. As we will see below, the unequal distribution of surveillance *capabilities* is often blamed for inequities in surveillance *power*. If the public could produce the visibility of state actors with similar ease and at the same scale, then the modern democratic ideal would be made possible by virtue of the enabling technologies.

1.3. The Neoliberalization of Political Transparency

In the Enlightenment model of transparency, self-disclosure and self-restraint is key. Monitoring from outside of institutions was always normatively encouraged, but new technical means are fundamental to the new transparency, in a society that permits no shadows, nothing hidden from view. Visibility produces awareness of official action (Andersson, 2008), and this awareness is seen as an essential foundation for meaningful participation in holding the powerful to account (Mulgan, 2003). Today, the ocular visibility suggested by transparency is much less metaphorical. The new transparency signifies a deliberate, emphatic reassertion of political transparency through two important transitions. The first transition is the informatization of visibility. Physical appearance is no longer the primary means of visibility; it is also produced through the *circulation* of media content. More crucially, this content is identified with information. Second, the relationship between publics and the state has changed in that transparency is no longer exclusive to self-disclosure by state agents. Birchall explains that transparency now extends beyond voluntary self-disclosure by state actors aspiring to the modern ideal, and now "has taken on the identity of a political movement with moral imperatives" (2011b, p. 62). Recognizing that "transparency as a cultural ideal of modernity" has failed (Teurlings & Stauff, 2014, p. 4), civilians increasingly participate in producing transparent relations, partly through participatory media, in order to realize this ideal. This movement includes advocacy for open government initiatives by state actors and non-governmental organizations, but also on "the guerrilla fringes of the transparency movement" (Birchall, 2011b, p. 78) are organizations like WikiLeaks and cop watching organizations discussed below. In the following subsections, I detail each of these two transitions.

1.3.1. Exhibits as Information

Discussions of transparency, particularly in policy arenas, frequently focus on information transparency and open government initiatives. The technical and organizational activities of realizing broadly shared support for such initiatives have produced a wealth of case studies and in turn debates over causes for failures and about best practices. Though often aimed at producing practical advice, Birchall (2011a) finds these studies can reveal and even criticize the liberal ideological underpinnings of political transparency and the ways in which the concept has undergone neoliberalization.

The reassertion of transparency appears while trust in governments is failing (Birchall, 2011b, p. 66). In order to rebuild trust,[3] transparency paradoxically offers a particularly neoliberal option of private oversight, one without granting any real political power to publics. Instead, transparency allows members of publics to exert their consumer power in addition to the authority of the ballot vote. In its contemporary ideal, transparency allows the expansion of choices, and for selection to be made by individuals through unhindered access to rich information. As Garsten and Montoya explain, this depicts a "neoliberal ethos of governance" through promoting "individualism, entrepreneurship, voluntary forms of regulation and formalized types of accountability" (in Birchall, 2011b, p. 65).

Governments are expected to be "open," and the criterion of openness is information transparency (Curtin & Meijer, 2006). In the Open-Source Manifesto, author and former Whole Earther, Robert David Steele connects demands for open government with open-source software and other "open" models of production. The maxim for "open everything": "Demand transparency and truth from every person, every organization, every government. Consider this the modern information-era equivalent of the Golden Rule" (Steele, 2012, p. 56). This recalls transparency as the

[3] Trust is often treated as an indicator of legitimacy in empirical research, see Levi, Sacks, Audrey, & Tyler, 2009.

Enlightenment's secular alternative to religious moral codes. Here we see not only a new credo, but one with a particular Enlightenment legacy being adapted to a new sociotechnical condition. This is not without precedent. Three decades ago, Langdon Winner (1986) critiqued the treatment of information as self-evidently and positively valuable, calling it "mythinformation." In the 1970s and 1980s, the "computer romantics" associated with the Whole Earth movement advanced a techno-utopian view of the promise of information technology to assure participatory democracy, eliminate toil, and assure environmental sustainability. It is this very contingent named and critiqued in Winner's essay, in which he describes mythinformation as grounded in four key assumptions: first, people are bereft of information; second, information is knowledge; third, knowledge is power; and finally, increasing access to information enhances democracy and equalizes social power. What is unique to the contemporary moment is evinced in calls for open government, which demonstrate political transparency is now also a response to "neoliberal audit culture" (Birchall, 2011b, p. 65).

The new transparency encourages beliefs in images speaking for themselves, in cameras as mechanically objective witnesses, and in information as self-evident. Together, the articulation of these beliefs function as a realist narrative (Harris, 2011). The view of mechanical objectivity has deep historical precedent. The first cameras were said to provide "a release from the 'artistic aids' that always threatened to make interpretation a personal, subjective feature of depiction." This mechanical objectivity was "defined by its moralized and automatic status beyond the reach of the artist's hand…boosters of mechanical objectivity…were automatic and as such did not pass through the dreaded dark glass of interpretation" (Galison, 1999).

Technologies that produce indexical images (e.g., photographic cameras) were originally idealized as tools that aided in observation that could communicate "truthful inferences about the world." Crary argues that the camera only briefly maintained this status, which quickly became seen as "a model for procedures and forces that conceal, invert, and mystify truth" (Crary, 1992, p. 29). The new transparency, however, radically repels such cynicism about images, invoking the spokesmen from the Enlightenment who distrusted the corruptible and biased minds of humans and favored the mechanical objectivity of the camera (Galison, 1999). The modern models of mind and perception that see human consciousness as a mirror of the world—"to look means to see, or that to see means to understand" (Burnett, 1995, p. 3)—is reasserted through the new transparency.

A special kind of objectivity is earned by virtue of qualities of new media technologies that produce the new transparency. Yesil explains:

> Camera phones… play a significant role in… documenting the misconduct of others, and functioning as tools of surveillance. They reorganize visual documentation and the construction of truth and reality, especially through the emphasis placed on users, and raw, unedited footage. They are generally conceptualized as instruments that we can believe in as neutral recorders of truth and reality, and stand as symbols of neutral vision and transparency mostly because they serve as 'nonhuman witnesses' in the sense that human capacities are irrelevant to their operation. As such these devices have begun to occupy a central position within the matrix of visual documentation and the construction of truth and reality. (Yesil, 2011, p. 285)

The discourse of the new transparency establishes that mediation occurs not as a result of imaging, information, and communication technologies, but by virtue of political interference with or suppression of content. Though traditional norms guiding journalists and media industries have promoted transparency, in that an "essential function of the media in liberal democracies is to legitimate power by holding it to account" (Schlosberg, 2013, p. 213), this ideal has been undermined by political-economic influence. Political-economic approaches to media emphasize economic interests that filter or manipulate content that would otherwise be unproblematic for audiences to commonly receive, absent any need for interpretation, as *mere information*. Criticism of consolidated media ownership and normative claims that favor pluralization suggest the decentralization of and participation in production and distribution afforded by convergence culture and the network society have inherent democratizing potentials (Bagdikian, 2004; Castells, 2010; Jenkins, 2008; McChesney, 1997). The problem from such perspectives has to do with ownership and control. The propaganda model of Herman and Chomsky (2002) stresses media ownership as fundamental to the content that circulates. The historically concentrated ownership of media by elites aided hegemony and the production of the consent of the governed. Removing the manipulation of communication by hegemonic powers results in content that is stripped down to mere objective information. This perspective has been criticized as a "hypodermic" model of media, where content is "injected" into viewers (Croteau & Hoynes, 2000).

Openness and sharing, and technologies like social media and clouds, all contribute to information being seemingly liberated from traditional political-economic filters. Documentations travel far, often not fully under control by those responsible for their origination, and "images literally flee from organized control" (Koskela, 2006, p. 164). Beyond this liberation of information from elite control, as Byung-Chul Han (2012) explains, what is made visible in the transparency society is now

beyond need for interpretation. What is made visible is objective, pure information, and it is computed via pure machinic logics. In fact, the demand for transparency is invoked most emphatically in conjunction with norms expressing the inherent freedom of information that must be preserved, not infringed upon. Televisibility flattens time and space, makes activities persistently visible, archivable, retrievable. Transparency today denies the occurrence of mediation by rejecting temporal significance. Rather than mediated, transparent images are *immediated*, in terms of their instantaneity. Temporal actions are subordinated to predictable, timeless access, for ease in monitoring and control. Televisible images are produced, instantly available, stored, accessed, and circulated. Transparency now represents unmediated contact because images become mere information. It permits neither gaps in information nor gaps in one's field of vision.

1.3.2. Media Participation and Neoliberal Citizenship

Just when images are simplified as information, the governed are homogenized into a single mass public. The new transparency amends Rousseau's general will with Habermas's public sphere. In the modern bourgeois conception of the public,

> "private persons" assembled to discuss matters of "public concern" or "common interest"…These publics aimed to mediate between "society" and the state by holding the state accountable to "society" via "publicity." At first this meant requiring that information about state functioning be made accessible so that state activities would be subject to critical scrutiny and the force of "public opinion." Later it meant transmitting the considered "general interest" of "bourgeois society" to the state… (Fraser, 1993, p. 4)

For Habermas, "the full utopian potential of the bourgeois conception of the public sphere was never realized in practice" (Fraser, 1993, p. 5). A stratified society produced conditions for exclusion from the public sphere and unequal authority within it. With the explosion of the mass media, the increasing scale of industrial production, and the growth of conspicuous consumption, critics like Thorstein Veblen, John Dewey, and Walter Lippmann saw the potential of the public sphere in crisis. They saw, according to Aronowitz, that "knowledge of public events had become impossibly fragmented, everyday life had become increasingly privatized, and, perhaps most importantly, the whole society had become absorbed in an orgy of consumption" (Aronowitz, 1993, pp. 75-76). Informatization provides a resolution, cohering the public once again. The new transparency now sees the instrumental conditions available to realize the full utopian potential of McLuhan's (1965) global village, and media participation is a primary means of civic participation in this space. This ideal model of global citizenship is founded in the coincidence of neoliberalism and informationism (Neubauer, 2011).

Transparency connotes unmediated visibility. In the new transparency, key mediating qualities historically recognized as fundamental to indexical and moving images are eclipsed by emphasizing the qualities of new digital technologies. Incidental or serendipitous recording by civilians and the ubiquity of surveillance cameras removes the mediating effects of editorial selection (Schwartz, 2009; Yesil, 2011). In the past, state and corporate institutions had greater capacity to engage in surveillance, but consumer-grade cameras and social media technologies have made available similar capacities to civilians. The smart phone with its video capability and data-connection permits incidental recording of activities both everyday and anomalous (Yesil, 2011). As Birchall explains, "the availability of technologies of surveillance and information exchange ensures we can be both objects and agents of intelligence" (Birchall, 2011a, p. 11). As costs for consumer electronics have lowered, the threshold to acquire imaging surveillance technologies have increasingly enabled *sousveillance*, the watching by publics of those with institutional authority. In this way, the modern panopticon is joined by the *synopticon*, where the many are now—or once again, as in Rousseau's state of nature—able to watch the few (Mathiesen, 1997). Synoptic technologies, Yesil claims, promote visibility in a "'viewer society' where individuals are not only subject to surveillance by government agencies, state institutions, corporations, etc. but also become surveillers themselves as they 'watch' the few and scrutinize them through mass media and television" (Yesil, 2011, p. 285). Increasingly, little is left out of the frame, all shadows have light cast into them—or "night vision"-enabled cameras pointed at them. Mobile technologies and other comparatively inexpensive technologies, like digital editing software, lower the financial barriers to entry into media production. Social media platforms function as distribution channels, so barriers to distribute content are also lower (Jenkins, 2008; Yesil, 2011). Viral circulation of content by users of social media and similar platforms makes up for the filtering effects of editorial staffs and the powerful interests that persuade them. These qualities are prioritized by advocates for the democratizing or liberating qualities of new technologies, once again reasserting the camera as an objective witness, now in the hands of billions of users worldwide. Larry Diamond calls these "liberation technologies" and "accountability technologies", because they "provide efficient and powerful tools for transparency and monitoring" (Diamond & Plattner, 2012, p. 10). "Individuals use their camera phones not only for personal communication," Yesil (2011) ex-

plains, "but also for documenting the misconduct of others, which leads to the description of such socio-technological practices as enablers of inverse surveillance that empower ordinary individuals to watch the authorities from below" (p. 285). This sousveillance is claimed to afford the expansion of political, social, and economic freedom (Diamond & Plattner, 2012).

Given new technological affordances to produce exhibits, today "the lines between reader and reporter, news and opinion, and information and action have all become blurred" (Diamond & Plattner, 2012, p. x). As such, media users are now simultaneously producers and consumers, or "prosumers" (Jenkins, 2008), who participate in the production of transparency. Anthony and Thomas (2010) explain "participatory media technologies that allow for the creation and distribution of user-generated content overturn traditional notions of all-powerful news media that define and restrict a largely passive audience" (p. 1283). Policymakers and scholars frequently express belief that such digital tools have profound political impacts, and emphasize the role played by access to alternative and independent sources of information enabled by unfiltered access to the internet (Etling, Faris, & Palfrey, 2010). That the "arena for political commentary and competition is more fast-paced, more decentralized, and more open to new voices and social entrepreneurs than ever before," is taken as evidence that the ease and efficiency in generating and dispersing a diversity of media content is inherently democratizing (Diamond & Plattner, 2012, p. x). As the digital divide in surveillance technology is closing (Mann et al., 2003, p. 335), a singular public is both enabled and expected to be media prosumers as a key performance of their citizenship (Dean, 2008).

When institutions themselves are deemed inappropriately transparent, civilians increasingly—enabled by cheap and abundant digital technologies—monitor institutions and official actors. Watchdog media checks and augments information provided by the self-disclosure of officials and institutions. More recently, civilians are active as watchdogs of their own sort, not only as intentional, planned activity, but also through incidental, happenstance documentation of official conduct (Anthony & Thomas, 2010). Civilians monitor wildlife, air and water quality, and produce similar environmental indices (Jalbert, Kinchy, & Perry, 2014; Kinchy, Jalbert, & Lyons, 2014; Kinchy & Perry, 2012; Ottinger, 2010). This activity is done as a form of redundancy, to quantitatively improve extant data or enhance quality of knowledge thus produced through repetition. This activity may be done where extant data is deemed deficient, either of poor quality or limited in quantity, to fill in gaps of knowledge otherwise left incomplete in quality or coverage. Finally, it can be undertaken when existing monitoring is deemed negligent, an oversight. In the new transparency, anything that escapes view is a source of risk or danger by virtue of its invisibility. Civilian voluntarism increasingly supplements or replaces activity historically in the purview of governments. This may be done, as we might expect, when there is a breakdown in trust among publics for the institutions that are or would usually be tasked with such surveillance. Redundant monitoring is especially indicative of this lack of trust. But it is also activity promoted by neoliberalization, as government agencies scale back due to funding and other cuts. Civilian monitoring steps in where government surveillance is deficient, negligent, or underfunded. In such a situation, the production of transparency by civilians develops a quality of civic participation, and in democratic societies, this confers a positive normative quality to the activities of monitoring (Dean, 2008). To produce transparency is to be a good citizen.

Since the new transparency ascribes absolute, positive value to visibility, the technologies and techniques that render bodies visible to surveillance produce power, and presumably with symmetry. This discourse frames imaging, communication, and information technologies as plastic, amenable to serving and empowering any interests. Surveillance activity is not exclusive to powerful institutions and actors who derive authority from these. The new transparency encourages a view of surveillance that is neutral, one where watching from below is productive of new powers for those outside the traditionally recognized structures of authority. Despite reliable substantiation for expectations that these new capabilities foster consequential political participation, the pervading doctrine of the new transparency allows such expectations to persist in absence of a demand for evidence supporting them. Even the most hopeful advocates for liberation technology (see, e.g., Diamond & Plattner, 2012) recognize the limited or equivocal evidence supporting their descriptions of these technologies as such. Here, the quasi-religious, doctrinal quality of the new transparency is revealed: it is, at its core, a faith rooted in history, ritually reproduced through insistence upon its efficacy and popular use predicated on this efficacy.

2. The New Transparency of Police

The prior section details the intellectual origins and social shaping of a concept that figures centrally in discourse about of policing's new visibility (Brucato, 2015; Goldsmith, 2010; Thompson, 2005). Transparency relies on a visibility produced by surveillance. During the past century, the use of camera surveillance became crucial to the maintenance of order just as citizens were increasingly tasked with producing transparent relations. In this section, I explain these two changes coincide with the new transparency of police. Using a situational analysis (Clarke, 2005), my research began by archiving videos documenting police violence, profil-

ing organizations that circulated these on social media, and building situational maps that identified key themes in pertinent discourse. My primary objective was to explain the proliferation of these videos. After years of studying discourses involving them, the theme of transparency was found to clearly pervade discussion of these videos and of policing's visibility (Boyatzis, 1998). I established an archive including scholarly research, public press articles, online and social media posts by activists, and supplemented these with original data from interviews and field notes. From this archive, I have selected and provided below key content that establishes the role played by modern notions of transparency and the discursive work in contemporary political contentions about police violence that are modifying these notions to develop the new transparency.

2.1. A New Era of Police Visibility

In 1991, the beating of Rodney King by Los Angeles Police Department (LAPD) officers was incidentally and covertly video recorded. Its release exposed the brutality of policing beyond the communities that chronically experience such violence (Skolnick & Fyfe, 1993). The video, which Mann and colleagues refer to as "probably the best-known recent example of sousveillance" (Mann et al., 2003, p. 333), made visible what the Christopher Commission later determined was routine police practice by the LAPD. This genetic moment in the history of incidental video documentation of police violence demonstrates the discourse of the new transparency. Los Angeles attorney and former State Department official, Warren Christopher, headed an independent investigation into a pattern of civil rights violations and violence by the LAPD. He wrote this Commission

> owes its existence to the George Holliday videotape of the Rodney King incident. Whether there even would have been a Los Angeles Police Department investigation without the video is doubtful, since the efforts of King's brother, Paul, to file a complaint were frustrated, and the report of the involved officers was falsified. Even if there had been an investigation, our case-by-case review of the handling of 700 complaints indicates that without the Holliday videotape the complaint might have been adjudged to be "not sustained," because the officers' version conflicted with the account by King and his two passengers, who typically would have been viewed as not "independent." (Independent Commission on the Los Angeles Police Department, 1991, p. ii)

Yesil (2011) explains the lasting significance of the Rodney King video, writing it "has served as one of the first and most widely-viewed examples of the power of mobile recorded image. The message of the Rodney King tape was that no person, institution or organization was immune from being monitored" (p. 280). The tape's power, she argues, was earned through its contents being widely disseminated and generating unprecedented public awareness about police violence. Responding to the Rodney King controversy, Skolnick and Fyfe (1993) argued that, "in the absence of videotapes or other objective recording of gratuitous violence, brutality rarely causes public controversy and is extremely difficult to prove" (p. 19). Here, not only is video objective, able to "prove" what happened, but public controversy is conditioned on this particular mode of exhibition. Crucial for the new transparency is that the value of this video remains even though the officers who brutalized King were exonerated in criminal court.

At the turn of the century, Regina Lawrence (2000) claimed that "most instances of police use of force are spontaneous, and the vast majority do not occur in the glare of television lights" (p. 14). Just a decade later, Diamond explained "incidents of police brutality have been filmed on cellphone cameras and posted to YouTube and other sites, after which bloggers have called outraged public attention to them" (Diamond & Plattner, 2012, p. 10). Now, Goldsmith (2010) explains, "video is the new reality" with "policing's new visibility." Jeffries (2011) argues, "cell phone surveillance" has "'turned on its head' the idea that the citizen-police officer relationship is an asymmetrical one" (p. 74). In just a decade, the game has seemingly changed, and the new technologies (e.g., mobile phones, microblogging and other social media) that produce and distribute this surveillance are credited for having changed the power dynamics in political culture. Disguising or hiding illegal or other offensive behavior is not as fully within the command of officers and agencies as they had been in the past. While acknowledging he is unclear about *how* this visibility will offer it, Goldsmith (2010) nonetheless finds it "highly probable that the new capacities for surveillance of policing inherent in these technologies may increase the police's accountability to the public" (p. 915).

Yesil (2011) claims that the use of cellphones to document the misconduct of others leads "to the description of such socio-technological practices as enablers of inverse surveillance that empower ordinary individuals to watch the authorities from below" (p. 285). Each new video documenting police brutality is said to produce "ruptures" in the "social fabric" because they bring up past injustices, as with the beating of Rodney King (Anthony & Thomas, 2010, p. 1292). In 2009, dozens of witnesses watched BART (Bay Area Rapid Transit) Police Officer Johannes Mehserle shoot Oscar Grant in the back, killing him while another officer restrained him, prone on a train platform in Oakland, California. The incident was video recorded by several of these witnesses. Since then, dozens of beatings and killings

by police have been documented by civilians on their cell phones, including Eric Garner being choked and suffocated by New York Police Department Officer Daniel Pantaleo in July 2014; Charly "Africa" Leundeu Keunang being shot and killed by a LAPD Sgt. Chand Syed and Officers Francisco Martinez and Daniel Torres in February 2015; and Walter Scott being shot and killed by North Charleston Police Officer Michael T. Slager in April 2015.

According to the discourse of the new transparency of police, the ability for civilians to produce policing's visibility empowers them in ways previously never imagined. These powers emerge from the mechanically objective qualities of cameras and the self-evident—even scientific—qualities of the media they produce. New popular abilities to make truthful claims backed by documentation and to thereby hold officials accountable are importantly joined by a protective power: to prevent police violence from being used against other community members or oneself (Brucato, 2015). This preventative power, provided by the visibility cameras produce, recalls Bentham's claim that behavior improves when people are strictly observed.

2.2. Cop Watching

This case is provided to demonstrate how the discourse of transparency functions in contemporary political contention. Regardless of the validity of the Enlightenment ideal for transparency in adequately describing the actual functioning of contemporary democracies, this conception lives on in the discourse and political activities of advocates for transparency. The following case study focuses especially on particular groups of such advocates: self-described "police accountability" activists who video record police and advocate that civilians also engage in such documentation. Cop watching has come to describe two kinds of activities. Cop watching has always referred to organized, intentional documentation of police by community groups; but it increasingly also describes the incidental, happenstance documentation by independent civilians (Huey, Walby, & Doyle, 2006; Toch, 2012; Wilson & Serisier, 2010). The modern ideal of transparency would suggest that making visible the administration of the law would protect civilians from its excesses, because transgressions would be subjected to accountability—or otherwise administrators would lose legitimacy. In my original interviews with them and in their public statements, cop watchers describe their motivations for making policing more visible. Like Pete Eyre, a co-founder of the organization Cop Block, who says "I'm a definitely a big advocate of transparency" (WeAreChange, 2013), these police accountability activists leverage what they see as the police's need for legitimacy to promote accountability.

On August 9, 2014, in Ferguson, Missouri, while on duty a white police officer, Darren Wilson, shot and killed Michael Brown, an unarmed, 18-year-old Black man. While this incident captured the attention and inspired the mobilization of existing activists and organizations across the country, it also produced a spontaneous uprising in Ferguson that continued for months. David Whitt lives in the housing project where Brown was killed. Despite not having an activist history, he became active daily in political agitation in his community. Whitt was both protesting the killing, but also engaging in efforts to constructively respond to what he saw as a pattern of excessive force, and particularly against people of color. He founded the Canfield Watchmen, who engaged in daily cop watch "patrols" to record police stops. With the support of a crowdfunded campaign by We Copwatch, the Canfield Watchmen distributed over one hundred wearable video cameras to area residents for them to serendipitously record police stops on an individual basis.

Cop watchers see their activities as preventing the invisibility of police violence. Like Rousseau, they see opacity as a vice itself and one that encourages further unethical behavior, often with brutal or deadly consequences. Video keeps individual officers honest. Those who transgress can be targeted as on this basis by cop watchers. Pete Eyre of the police accountability organization, Cop Block, claims because "it's individuals who act…it's individuals who are responsible for their actions" (personal communication, February 17, 2015). Here we see transparency functioning in its modern normative sense: enabling the mutual regulation of individual behavior.

Community organizer and independent journalist, Gregory Malandrucco, articulates that camera surveillance enables the kind of bi-directional transparency Bentham preferred:

> Today, video captures not only civilians acting beyond the bounds of legality against the state and its laws, but also egregious instances of police officers breaking the very laws they are sworn to uphold. Technology presents us with the unforeseen potential to hold public officials accountable for their actions in swift and certain terms, as equal members of society… (Malandrucco, 2012)

Civilian participation in media production places civilians on more equal footing with police and other state actors. This view demonstrates in action the idea that this kind of transparency works to legitimate vertical inequalities in representative democracies. More importantly, if officials, functionaries, and other agents of the state are insufficiently visible, individual citizens can now offer the corrective. Jeffries writes that "using a cell phone camera to monitor police work is a relatively easy way to participate in the democratic process. Doing so gives people a sense of efficacy; that they can impact

what the government does" (Jeffries, 2011, p. 74).

Given the new transparency, the content of these videos is self-evident and objective, prior to or even forbidding any interpretation. Eyre presents transparency as a technically-enabled quality: "If I say 'Hey, this just happened,' they don't have to try to determine if I'm being factual or not." Because "the lens of the camera is objective," he says, "People don't have to know me, or trust me… They can just look at the video." (WeAreChange, 2013).

Cop watchers see themselves not only as participating in viewing the articulation of state power, but also as producing new popular power. The belief that popular media production and circulation can produce power is grounded in three claims. The first is because it circumvents filtering effects enabled by the political economic power of the mass media. Matt Agorist of *The Free Thought Project* claim that unfiltered content generation and circulation is "changing the world." "Technology and the internet," he writes, "is giving way to amateur reporters putting out unfiltered and unedited news. This is the future, this is how REAL change is brought about; not from fat cats in nice suits lying to you" (Agorist, 2014). As Eyre explains:

> We live in a time now with technology, where we can go around the would-be censors that really thrive on the control and access to information. Today with the internet and other technologies we can really bypass those gatekeepers and support each other…(personal communication, February 17, 2015)

Second, media produced by civilians shapes the agenda in political forums and in mass media reporting. Grant A. Mincy of Center for a Stateless Society claims "new technology, independent media and good old human communication" have provoked increased attention by mainstream news outlets that are following agenda-setting happening at the grassroots. "We are connected, we talk, we control the public arena and we make stories go viral," he explains. "In the face of increased violence folks are taking to social media to spread news and directly confront state power" (Mincy, 2013). Finally, because of the supposed civilizing quality of transparency, cameras provide their users with protective power. Wendy McElroy (2010) claims "cameras have become the most effective weapon that ordinary people have to protect against and to expose police abuse."

2.3. Exhibiting Unaccountability

Sen (2010) applies the modern triad of transparency, accountability, and legitimacy to police, explaining that in a democratic society police are accountable to the people, and also have "a proximate responsibility to the law of the land which expresses the will of the people" (p. 1). He further maintains that "the police should be transparent in its activities. Most of the police activities should be open to scrutiny and subject to reports to regular outside bodies" (Sen, 2010, p. 9).

Prenzler and Ronken (2001) reviewed several decades of research throughout the Anglophone world to systematically review predominating models of police accountability. Initial police accountability included accountability to law and to elected officials, to which was later added internal investigations and review by external agencies. Cop watchers may advocate using video footage to ensure greater accountability through such processes. However, they add to or replace these processes by promoting the withdrawal of police legitimacy by publics.

Cop watching, Jeffries (2011) contends, "has introduced an element of accountability that heretofore has been absent" (p. 74). By filming police, "unknown cameramen and women lived out high democratic ideals" through this mode of bearing witness (Meyer, 2015). Acknowledging "that civilian-held cameras are [not] always effective at securing a conviction," Meyer (2015) cites the example of Eric Garner, killed by New York Police Department Officer Daniel Pantaleo in Staten Island on July 17, 2014. The killing of Garner was video recorded, but no officers were indicted by the Richmond County Grand Jury. Nonetheless, as in the Rodney King incident, the significance of video is that *we know*. After all, in the new transparency, *to see is to know* (Han, 2012). According to contemporary perspectives that venerate transparency, political problems are a result of a deficient or incomplete set of information to be solved through accumulating more and better information (see Winner, 1986).

According to the discourse of the new transparency, once police-civilian interactions are made visible, accountability is the likely or certain outcome. In his report on police repression of Occupy Wall Street protests, Harmon Leon (2011) wrote that "cell phones and social media are the great equalizers in keeping law enforcement accountable." Similarly, Carlos Miller (2014) of the advocacy group, Photography Is Not A Crime!, explains that "justice prevails every once in a while," but "only because it was all caught on video." However, if accountability is not reliably demonstrated, many cop watchers believe this will undermine the police institution by causing a crisis of legitimacy. They agree with journalists like Matt Taibbi (2014), who claims that as a result of the deaths of Michael Brown in Ferguson and Eric Garner in New York, "the police suddenly have a legitimacy problem in this country." Friedersdorf (2014) contends that "the police continue to lose the trust of the public, due largely to documented instances of bad behavior by fellow officers, as well as law enforcement's longstanding inability to police themselves."

Meyer (2015) acknowledges a poor model for justice requires police accountability "rely on someone always standing nearby with a smartphone. But the

process of ascertaining the truth of the world has to start somewhere." Many cop watchers are not only aimed at holding individual officers responsible for transgressions. For Eyre, filming is also desirable

> to make clear a pattern of unaccountability that's built into the so-called justice system. The idea that it's just a few rogue people that are doing something is not true…. If people see this as a pattern then….[this will undermine] the legitimacy that they grant to these institutions, or their own willingness to call them and utilize them, or deferment to them, or even the funding of their apparatus… (personal communication, February 17, 2015)

Through accumulation of videos, these will allow the public to see the depicted incidents are not isolated or exceptional, but instead form a pattern revealing the normal function of police. If publics routinely see videos followed by a failure to demonstrate institutional accountability, they would retract the legitimacy they grant to these institutions. "That's ultimately to me what's necessary to have a change" explains Eyre (personal communication, February 17, 2015).

As Rojek, Alpert and Smith (2012) observe, sousveillance media documenting policing activity "provide the public with a snapshot of what the police do" (p. 302). Lersch and Mieczkowski (2005) explain videocameras and media attention may foment distrust and fear of police. This exposure could create the impression that police violence is increasing, when in fact "violent police behavior has a long history, dating back to the early years of law enforcement" (Lersch & Mieczkowski, 2005, p. 553).[4] Because "cell phone camera surveillance of police officers is exposing behavior that some police officers have gotten away with for years" (Jeffries, 2011, p. 73), routine problems of policing are now subject to popular oversight.

When transparency fails to produce accountability, when it does not fulfill the promise of protection, the modern transparency-accountability-legitimacy triad would suggest that legitimacy is certain to fail. Many cop watchers wish to undermine the legitimacy of the police institution, so they believe making its essential violence visible will result in a withdrawal of legitimacy, and this alone will force change. This is why these cop watchers choose media circulation as their primary activity, rather than more traditional means of community organizing to issue demands to or to directly confront governmental institutions. The battle is over legitimacy, and transparency is the tactic of choice.

3. The Resilience of Police

Despite the increased visibility of policing (Goldsmith, 2010), declining violent crime rates (Truman & Planty, 2012) and increased officer safety (Center for Officer Safety & Wellness, 2014), officer use-of-force incidence does not appear to be waning (Alpert & Dunham, 2000, 2004, 2010). Furthermore, officers are equipped with more weaponry to use (Kraska & Kappeler, 1997) in more striated continuums of force (Walker, 2005). In the past decade, police have killed thousands of Americans, and yet only 54 police have been criminally charged for the killings (Kindy & Kelly, 2015). Of those cases that are resolved, less than a third were convicted. These police were sentenced to serve about three years in jail or prison, on average. Oscar Grant's killer, former Officer Johannes Mehserle, served just over a year and a half in jail. The rapid growth in police monitoring should leave us skeptical over claims made regarding its political efficacy. Police know they are now visible, and yet the police institution and its use of violence do not appear to be changing in any fundamental way—certainly not in the ways most cop watchers expect. For all the talk about the popular empowerment caused by cheap imaging and communication technologies, the police institution remains resilient.

Though transparency is widely believed to produce the possibility of accountability (Mulgan, 2003), and is therefore productive of popular power (Birchall, 2011b), this expectation is frustrated by the actual outcomes of documenting police violence. The very proliferation of such media speaks to the limitations of visibility as a protective power. Roger Holliday was hidden in his apartment while LAPD officers beat Rodney King at night in 1991. However, the more recent 2008 video-recorded beating of Michael Cephus showed the close proximity of several citizens filming police during daylight as one officer struck Cephus so hard with a baton that the officer lost his grip on it and it rolled across the street. Hurst Texas Police Department Officer Disraeli Arnold taunted a cameraperson as he brutalized and threatened to kill an already restrained 17-year old, Andrew Rodriguez, in 2012. After kneeing Rodriguez in the head and shouting "Move and die!" he marched him, handcuffed, past the camera and shouted—without prompting—his badge number into the camera. Following the killing of Michael Brown, months of sustained protests in Ferguson, Missouri, sporadic related protests throughout the United States, President Barack Obama signed a bill to fund the adoption of 50,000 on-officer wearable cameras (Brucato, 2015). Rather than demonstrating accountability, publics were offered more transparency.

Cop watching exemplifies the adaptation of modern transparency to contemporary conditions. The new transparency retains qualities from its Enlightenment origins, and renews its conceptual and practical connections to accountability and legitimacy. Emphasizing transparency's connection to ocular visibility, now visibility paradoxically benefits from its mediation, be-

[4] For a detailed history, see Brucato (2014).

cause it allows for televisibility and archivability while simultaneously maintaining its objectivity. The affordances of new technologies allow for both access and instantaneity. Mediation only retains its positive qualities that allow for transcending the limits of time and distance, providing an archivable object with its own persistent access, but also lending direct access to *what really happened*. Since documentations are not edited or filtered by editorial staffs working for multinational megacorporations, raw footage gives amplified access to what Szarkowski (2007) calls "the thing itself." With streaming video and Tweeted photographs, this can happen instantaneously. Time is suspended, and so images are no longer the embodiment of an afterlife, but rather a sign that the metaphors of life and death do not apply to media. Everything is now. Transparency is presence.

The new transparency undergirds the political strategies not only of most activists and other civil society groups focusing on police violence, but it also motivates considerable political activity on matters of crucial social and environmental importance. Not only do civilians watch police, but they document many aspects of the built and natural environment, both their friends and governmental institutions. Most of all, civilians champion the courage of whistleblowers; WikiLeaks and Edward Snowden have revealed to the world the extensive functions and seemingly shocking outcomes of the military and security apparatus, and the leakers are lauded as heroes.

In his influential conceptualization of "the new visibility," Thompson argues, "mediated visibility is not just a vehicle through which aspects of social and political life are brought to the attention of others: it has become a principal means by which social and political struggles are articulated and carried out" (Thompson, 2005, p. 49). He explains this new visibility is a "double-edged sword." When cameras are ubiquitous and the internet lowers thresholds to reach audiences, both the governed and the governing are exposed. Yet clearly, both edges of this blade do not always cut the same or as deeply.

What might explain the excitement over WikiLeaks, cop watching, and similar struggles for visibility? Setting aside for a moment common concerns about privacy, might it be that many civilians find in surveillance the possibility of alleviating anxieties by returning to what Rousseau saw as our lost state of nature? New technological affordance allow us to *see through one another*, to make actions apparent in public so people can be held to popular account. But this ideal does not square with current political realities. We might meet the precondition of transparency, the means treasured today as in the early modern period; but the ends of this ideal—a democracy governed through broad participation by all publics, where the powerful are held to account—is far from a reality. Perhaps this footage provides not a transparent lens into reality, but a mirror reflecting back on its viewers. As Žižek (2011) wrote about WikiLeaks, the shame these disclosures produce is not only directed toward public officials and functionaries, but also back at ourselves "for tolerating such power over us." More importantly, this shame "is made more shameful by being publicised." This, of course, is simply a restatement of the transparency-accountability-legitimacy model: that there is no authority except that which persists with public consent.

Videos documenting police violence in the United States most often depict Blacks being brutalized, often by white officers, and this squares with long-established patterns in police outcomes (Brucato, 2014). Though public disapproval of police agencies may increase after publicized incidents involving charges of brutality, this disapproval does not become entrenched, especially not among whites (Weitzer, 2002). Not only is there a strong majority approval of police in the United States, this approval is not impacted among whites even when they believe police are brutal and racist (Thompson & Lee, 2004). In keeping with Sir Robert Peel's belief that the public consent and trust are necessary for successful policing, criminological researchers presume its necessity despite so rarely finding it (Reiner, 2010), especially among those populations most intensively policed—Blacks living in segregated urban neighborhoods (Kane, 2005).

The United States is not comprised by a single, homogeneous mass public that together grants its consent to public institutions—neither is any other contemporary liberal-democratic nation, for that matter. Rather the United States was historically and is currently deeply divided along the color line. Joel Olson (2004) referred to the United States as a "white democracy" on the grounds that it has two practical political orders: democracy for white citizens and tyranny for everyone else. This division has always been crucial to the police mandate (Brucato, 2014). While some documented incidents of police brutality have prompted uprisings, these have been few in number, unsustained, and resulted in little more than nominal commitments by public officials to improved police accountability. The rebellions in Ferguson in 2014 and in Baltimore in 2015 were exceptional on many grounds. Importantly, mostly poor, Black nonactivists populated both uprisings, and they remained militantly active in the streets for weeks. Police were shown on amateur video and mainstream media using military vehicles, weapons, armor, and other equipment to suppress both rebellions. When a defined segment of the fragmented U.S. population then demonstrated a persistent lack of consent to the brutal policing that is an ambient presence in their lives, police suppressed this rebellion using military weapons and tactics and in full view of broader publics.

The new transparency casts new technologies as

enablers of a "global village," allowing a universal humanity to transcend sociospatial divisions, of which the color line is but one indicator. The persistence of this presumption not only avoids the inability for publics to efficaciously act on the basis of such a capacity. This presumption also reinforces what Cheliotis (2010) calls "narcissistic sensibilities and practices, either by presuming that the included already possess a kind-heartedness in wait only for specific directions, or by framing 'others' as human only insofar as their stories reflect our own emotional world" (p. 172). The transparency-accountability-legitimacy model presumes an undivided public, perhaps permitting some inequality within it, but not capable of accounting for the categorical exclusion or domination of an entire population.

The new transparency is grounded in the mistaken idea that documentations are self-evident, and that this divided population would make the same sense of videos documenting police violence. As Butler (1993) argued with reference to the Rodney King case, not only are U.S. populations racialized, but, in part because of this, the visible is itself a racially contested terrain. Transparency casts video as capable of speaking for itself. When partisans expect video to function this way, they neglect the political task of engaging in public speech that would provide an antiracist, counterhegemonic interpretation against the dominant reading that interprets police as providers of security and those most intensively policed—people of color, and especially young Black men—as threats to the social order.

Acknowledgments

Thanks to Crina Archer, Langdon Winner, and Nancy D. Campbell for crucial comments on earlier drafts. Thank you to three anonymous reviewers and the editors for close reading and helpful commentary. I appreciate the assistance of Jennifer Mann in finalizing the copy. This research was partly conducted while supported by the Humanities, Arts, and Social Sciences Fellowship at Rensselaer Polytechnic Institute.

Conflict of Interests

The author declares no conflict of interests.

Bibliography

Agorist, M. (2014, January 20). How individuals with smartphones and cameras are changing the world by filming corruption. *The Free Thought Project*. Retrieved from http://thefreethoughtproject.com/individuals-smartphones-anhd-cameras-changing-world-filming-corruption.

Alpert, G. P., & Dunham, R. G. (2000). *Analysis of police use of force data.* Washington, DC: National Institute of Justice.

Alpert, G. P., & Dunham, R. G. (2004). *Understanding police use of force: Officers, suspects, and reciprocity*. New York, NY: Cambridge University Press.

Alpert, G. P., & Dunham, R. G. (2010). Policy and training recommendations related to police use of CEDs: Overview of findings from a comprehensive national study. *Police Quarterly, 13*(3), 235-259.

Andersson, K. (2008). *Transparency and accountability in science and politics: The awareness principle.* New York, NY: Palgrave Macmillan.

Anthony, M. G., & Thomas, R. J. (2010). "This is citizen journalism at its finest": Youtube and the public sphere in the oscar grant shooting incident. *New Media & Society, 12*(8), 1280-1296.

Aronowitz, S. (1993). Is democracy possible? The decline of the public in the American debate. In B. Robbins (Ed.), *The phantom public sphere* (pp. 75-92). Minneapolis: University of Minnesota Press.

Bagdikian, B. (2004). *The new media monopoly.* Boston, MA: Beacon Press.

Beetham, D. (1991). *The legitimation of power.* Atlantic Highlands: Humanities Press International.

Birchall, C. (2011a). Introduction to "Secrecy and Transparency": The Politics of Opacity and Openness. *Theory, Culture & Society, 28*(7/8), 7-25.

Birchall, C. (2011b). Transparency, Interrupted: Secrets of the Left. *Theory, Culture & Society, 28*, 60-84.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development.* Thousand Oaks: Sage Publications.

Brucato, B. (2014). Fabricating the color line in a white democracy: From slave catchers to petty sovereigns. *Theoria: A Journal of Social and Political Theory*, *61*(141), 30-54.

Brucato, B. (2015). Policing made visible: Mobile technologies and the importance of point of view. *Surveillance & Society*, *13*(3/4).

Bruno, F. (2011). A brief cartography of smart cameras: proactive surveillance and control. In R. J. Firmino, F. Duarte, & C. Ultramari (Eds.), *ICTs for mobile and ubiquitous urban infrastructures: Surveillance, locative media and global networks* (pp. 257-271). Hershey, PA: IGI Global.

Burnett, R. (1995). *Cultures of vision: Images, media & the imaginary*. Bloomington: Indiana University Press.

Butler, J. (1993). Endangered/endangering: Schematic racism and white paranoia. In R. Gooding-Williams (Ed.), *Reading Rodney King/Reading urban uprising* (pp. 15-22). New York: Routledge.

Castells, M. (2010). *The rise of the network society: The information age: Economy, society, and culture, volume I* (2nd ed.). Malden: Blackwell Publishing.

Center for Officer Safety and Wellness. (2014). *2013 Line-of-duty officer deaths: An overview*. Alexandria, VA: International Association of Chiefs of Police.

Cheliotis, L. K. (2010). The ambivalent consequences of

visibility: Crime and prisons in the mass media. *Crime Media Culture, 6*(2), 169-184.

Chrismas, R. (2013). *Policing in the 21st century: A frontline officer on challenges and changes.* Montreal, QC: McGill-Queen's University Press.

Clarke, A. E. (2005). *Situational analysis: Grounded theory after the postmodern turn.* Thousand Oaks, CA: Sage.

Crary, J. (1992). *Techniques of the observer.* Cambridge, MA: MIT Press.

Croteau, D., & Hoynes, W. (2000). *Media/society: Industries, images, and audiences.* New York: Pine Forge Press.

Curtin, D., & Meijer, A. J. (2006). Does transparency strengthen legitimacy? A critical analysis of European Union policy documents. *Information Polity, 11*, 109-122.

Davis, K. R. (1991). Kantian "publicity" and political justice. *History of Philosophy Quarterly, 8*(4), 409-421.

Dean, J. (2008). Communicative capitalism: Circulation and the foreclosure of politics. In M. Boler (Ed.), *Digital media and democracy: tactics in hard times* (pp. 101-121). Cambridge, MA: The MIT Press.

Diamond, L., & Plattner, M. F. (2012). *Liberation technology: Social media and the struggle for democracy.* Baltimore, MD: The Johns Hopkins University Press.

Ellul, J. (1964). *The technological society.* New York, NY: Vintage.

Etling, B., Faris, R., & Palfrey, J. (2010). Political change in the digital age: The fragility and promise of online organizing. *SAIS Review, 30*(2), 37-49.

Foucault, M. (1979). *Discipline and punish: The birth of the prison.* New York: Vintage.

Fraser, N. (1993). Rethinking the public sphere: A contribution to the critique of actually existing democracy. In B. Robbins (Ed.), *The phantom public sphere* (pp. 1-32). Minneapolis: University of Minnesota Press.

Friedersdorf, C. (2014, August 18). Video killed trust in police officers. *The Atlantic.* Retrieved from http://www.theatlantic.com/national/archive/2014/08/police-officers-havent-earned-our-instinctive-trust/378657

Galison, P. (1999). Objectivity is romantic. In J. Friedman, P. L. Galison, S. Haack, & B. E. Frye (Eds.), *The humanities and the sciences* (pp. 15-43). Philadelphia: American Council of Learned Societies.

Goldsmith, A. J. (2010). Policing's new visibility. *British Journal of Criminology, 50*, 914-934.

Han, B.-C. (2012). *Transparenzgesellschaft.* Berlin, Germany: Matthes & Seitz.

Harris, C. V. (2011). Technology and transparency as realist narrative. *Science, Technology, & Human Values, 36*(1), 82-107.

Heald, D. (2006). Transparency as an Instrumental Value. In C. Hood & D. Heald (Eds.), *Transparency: The key to better governance?* New York: Oxford University Press.

Herman, E. S., & Chomsky, N. (2002). *Manufacturing consent: The political economy of the mass media.* New York: Pantheon Books.

Hier, S. (2003). Probing the surveillant assemblage: On the dialectics of surveillance practices as processes of social control. *Surveillance & Society*, *1*(3), 399-411.

Hier, S. P., Walby, K., & Greenberg, J. (2006). Supplementing the panoptic paradigm: Surveillance, moral governance and CCTV. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 230-44). Portland, OR: Willan Publishing.

Hill, G. (2006). *Rousseau's theory of human association: Transparent and opaque communities.* New York: Palgrave Macmillan.

Hood, C. (2006). Transparency in historical perspective. In C. Hood & D. Heald (Eds.), *Transparency: The key to better governance?* (pp. 3-23). New York: Oxford University Press.

Huey, L., Walby, K., & Doyle, A. (2006). Cop watching in the downtown eastside: Exploring the use of (counter)surveillance as a tool of resistance. In T. Monahan (Ed.), *Surveillance and security: Technological politics and power in everyday life* (pp. 149-165). New York, NY: Routledge.

Independent Commission on the Los Angeles Police Department. (1991). *Report on the independent commission on the Los Angeles police department.* Los Angeles: Independent Commission on the Los Angeles Police Department.

Jalbert, K., Kinchy, A. J., & Perry, S. L. (2014). Civil society research and marcellus shale natural gas development: Results of a survey of volunteer water monitoring organizations. *Journal of Environmental Studies and Sciences, 4*(1), 78-86.

Jeffries, J. (2011). Democracy for the few: How local governments empower cops at citizens' expense. *Journal of Law and Conflict Resolution, 3*(5), 71-75.

Jenkins, H. (2008). *Convergence culture: Where old and new media collide* (Revised ed.). New York: New York University Press.

Johnson, D., & Regan, P. (2014). *Transparency and surveillance as sociotechnical accountability: A house of mirrors.* New York: Routledge.

Kane, R. J. (2005). Compromised police legitimacy as a predictor of violence crime in structurally disadvantaged sommunities. *Criminology, 43*(2), 469-498.

Kinchy, A. J., & Perry, S. L. (2012). Can volunteers pick up the slack? Efforts to remedy knowledge gaps about the watershed impacts of marcellus shale gas development. *Duke Environmental Law & Policy Forum, 22*, 303-339.

Kinchy, A., Jalbert, K., & Lyons, J. (2014). What is volunteer water monitoring good for? Fracking and the plural logics of participatory science. *Political Power and Social Theory, 27*(2), 259-289.

Kindy, K., & Kelly, K. (2015, April 11). Thousands dead, few prosecuted. *The Washington Post.* Retrieved from http://www.washingtonpost.com/sf/investigative/2015/04/11/thousands-dead-few-prosecuted

Koskela, H. (2003). "Cam Era": The contemporary urban panopticon. *Surveillance & Society, 1*(3), 292-313.

Koskela, H. (2006). "The other side of surveillance": Webcams, power and agency. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 163-181). Portland: Willan Publishing.

Kraska, P. B., & Kappeler, V. E. (1997). Militarizing American police: The rise and normalization of paramilitary units. *Social Problems, 44*(1), 1-18.

Lawrence, R. G. (2000). *The politics of force: Media and the construction of police brutality.* Berkeley, CA: University of California Press.

Leon, H. (2011, October 10). Cop punches occupy wall street protester: The whole world is watching! *SFGate.* Retrieved from http://blog.sfgate.com/hleon/2011/10/14/cop-punches-occupy-wall-street-protester-the-whole-world-is-watching

Lersch, K., & Mieczkowski, T. (2005). Violent police behavior: Past, present, and future research directions. *Aggression and Violent Behaviour, 10*, 552-568.

Levi, M., Sacks, A., & Tyler, T. (2009). Conceptualizing legitimacy, measuring legitimating beliefs. *American Behavioral Scientist, 53*(3), 354-375.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life.* Buckingham: The Open University Press.

Lyon, D. (2006). The search for surveillance theories. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 3-20). Portland, OR: Willan Publishing.

Lyon, D. (2007). *Surveillance studies: An overview.* Malden: Poliy.

Machin, D. J. (2012). Political legitimacy, the egalitarian challenge, and democracy. *Journal of Applied Philosophy, 29*(2), 101-117.

Malandrucco, G. (2012, June 7). Video is the new reality: One year after Flint Farmer was senselessly killed by Chicago police. *The Enemy Within: Modern Policing Within a Global Perspective*. Retrieved from http://www.uscop.org/video-is-the-new-reality-one-year-after-flint-farmer-was-senselessly-killed-by-chicago-police

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society, 1*(3), 331-355.

Marx, G. T. (2006). Soft surveillance: The growth of mandatory volunteerism in collecting personal information: "hey buddy can you spare a dna?" In T. Monahan (Ed.), *Surveillance and security: Technological politics and power in everyday life* (pp. 37-56). New York: Routledge.

Marx, G. T. (2009). A tack in the shoe and taking off the shoe: Neutralization and counter-neutralization dynamics. *Surveillance & Society, 6*(3), 294-306.

Mathiesen, T. (1997). The viewer society: Michel Foucault's "panopticon" revisited. *Theoretical Criminology, 1*(2), 215-234.

McChesney, R. (1997). *Corporate media and the threat to democracy.* New York, NY: Seven Stories Press.

McElroy, W. (2010, May 31). *Are cameras the new guns? The Freeman: Foundation for Economic Education.* Retrieved from http://fee.org/freeman/detail/are-cameras-the-new-guns

McLuhan, M. (1965). *Understanding media: The extensions of man.* New York: Signet.

Meyer, R. (2015, April 8). The courage of bystanders who press "record". *The Atlantic.* Retrieved from http://www.theatlantic.com/technology/archive/2015/04/the-courage-of-bystanders-who-press-record/389979

Miller, C. (2014, January 22). Connecticut cop sentenced to 30 months in prison after arresting priest for recording. *Photography Is Not A Crime.* Retrieved from http://photographyisnotacrime.com/2014/01/22/connecticut-cop-sentenced-30-months-prison-arresting-priest-recording

Mincy, G. A. (2013, 12 11). Hot rocks from the peacekeepers, polemics from the public. *Before it's news.* Retrieved from http://c4ss.org/content/22918.

Mulgan, R. G. (2003). *Holding power to account: Accountability in modern democracies.* New York, NY: Palgrave Macmillan.

Neocleous, M. (2000). *The fabrication of social order: A critical theory of police power.* Sterling, VA: Pluto Press.

Neubauer, R. (2011). Neoliberalism in the information age, or vice versa? Global citizenship, technology, and hegemonic ideology. *tripleC, 9*(2), 195-230.

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: The rise of CCTV.* New York: Bloomsbury Academic.

O'Kane, R. H. (1993). Against legitimacy. *Political Studies, 41*(3), 471-487.

Olson, J. (2004). *The abolition of white democracy*. Minneapolis, MN: University of Minneapolis Press.

Ottinger, G. (2010). Buckets of resistance: Standards and the effectiveness of citizen science. *Science, Technology, & Human Values, 35*(2), 244-270.

Prenzler, T., & Ronken, C. (2001). Models of police oversight: A critique. *Policing and Society, 11*(2), 151-180.

Reiner, R. (2010). *The politics of the police* (4th ed.). New York, NY: Oxford University Press.

Rojek, J., Alpert, G. P., & Smith, H. P. (2012). Examining officer and citizen accounts of police use-of-force incidents. *Crime & Delinquency, 58*(2), 301-327.

Rousseau, J.-J. (1913). *The social contract & discourses.* London: J.M. Dent & Sons, Ltd.

Schlosberg, J. (2013). *Power beyond scrutiny media, justice and accountability.* New York: Pluto Press.

Schwartz, L.-G. (2009). *Mechanical witness: A history of motion picture evidence in U.S. courts.* New York, NY: Oxford University Press.

Sekula, A. (1978). Dismantling modernism, reinventing documentary (notes on the politics of representation). *The Massachusetts Review, 19*(4), 859-883.

Sen, S. (2010). *Enforcing police accountability through civil oversight.* Thousand Oaks, CA: Sage.

Skolnick, J. H., & Fyfe, J. J. (1993). *Above the law: Police and the excessive use of force.* New York, NY: The Free Press.

Steele, R. D. (2012). *The open-source everything manifesto: Transparency, truth, and trust.* Berkeley: Evolver Editions.

Szarkowski, J. (2007). *The photographer's eye* (Reprint ed.). New York, NY: The Museum of Modern Art.

Taibbi, M. (2014, December 5). The police in America are becoming illegitimate. *Rolling Stone.* Retrieved from http://www.rollingstone.com/politics/news/the-police-in-america-are-becoming-illegitimate-20141205

Teurlings, J., & Stauff, M. (2014). Introduction: The transparency issue. *Cultural Studies ↔ Critical Methodologies, 14*(1), 3-10.

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

Thompson, B. L., & Lee, J. D. (2004). Who cares if police become violent? Explaining approval of police use of force using a national sample. *Sociological Inquiry, 74*(3), 381-410.

Toch, H. (2012). *Cop watch: Spectators, social media, and police reform.* Washington, DC: American Psychological Association.

Torpey, J. (2000). *The invention of the passport: Surveillance, citizenship and the state.* Cambridge: Cambridge University Press.

Turilli, M., & Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology, 11*(2), 105-112.

Tyler, T. R. (2006). Psychological perspectives on legitimacy and legitimation. *Annual Review of Psychology*, *57*, 375-400.

Tyler, T. R., & Fagan, J. (2008). Legitimacy and cooperation: Why do people help the police fight crime in their communities? *Ohio State Journal of Criminal Law, 6*, 231-275.

Walker, S. E. (2005*). The new world of police accountability.* Thousand Oaks, CA: Sage Publications.

WeAreChange. (2013, August 23). Cop blocking with Pete Eyre in NYC. *YouTube*. Retrieved from https://www.youtube.com/watch?v=jmfBfH2Wrnk

Weitzer, R. (2002). Incidents of police misconduct and public opinion. *Journal of Criminal Justice, 30*, 397-408.

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

Winner, L. (1986). Mythinformation. In *The whale and the reactor: A search for limits in an age of high technology* (pp. 98-117). Chicago, IL: University of Chicago Press.

Yesil, B. (2011). Recording and reporting: Camera phones, user-generated images and surveillance. In *ICTs for mobile and ubiquitous urban infrastructures: Surveillance, locative media, and global networks* (pp. 272-293). Hershey, PA: IGI Global.

Žižek, S. (2011, January 20). Good manners in the age of WikiLeaks. *London Review of Books, 33*(2), 9-10.

About the Author

Dr. Ben Brucato

Ben Brucato is an interdisciplinary scholar and political theorist, working at intersections of media, technology, surveillance, policing, and race. Currently a postdoctoral fellow in the Center for Humanistic Inquiry at Amherst College, he works on the *Mattering Lives* project. Brucato earned his Ph.D. in Science & Technology Studies from Rensselaer Polytechnic Institute.

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 3, Pages 56-67
Doi: 10.17645/mac.v3i3.268

Article

First They Came for the Poor: Surveillance of Welfare Recipients as an Uncontested Practice

Nathalie Maréchal

School of Communication, University of Southern California, Los Angeles, CA 90007, USA; E-Mail: marechal@usc.edu

Submitted: 8 April 2015 | In Revised Form: 15 July 2015 | Accepted: 4 August 2015 |
Published: 20 October 2015

Abstract
There have been moments in American history when government surveillance of everyday citizens has aroused public concerns, most recently Edward Snowden's 2013 revelations concerning widespread, warrantless surveillance of Americans and foreigners alike. What does not arouse public concern are longstanding governmental practices that involve surveillance of poor people who receive certain types of public benefits. This article traces the political history of U.S. poverty-relief programs, considers the perspective of welfare beneficiaries themselves, analyzes American cultural beliefs about the poor in order to offer some thoughts on why those surveillance practices garner little public concern, and argues that those who are concerned about warrantless surveillance of ordinary citizens should do more to protect ordinary poor citizens from surveillance.

Keywords
beneficiaries; poor; poverty; public benefits; surveillance; welfare

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

1. Introduction

There have been moments in American history when government surveillance of everyday citizens has aroused media attention. These moments include Edward Snowden's revelation of NSA practices in 2013, the 1972 media revelations of FBI widespread surveillance of United States citizens, and perhaps even the Joseph McCarthy hearings in 1954. What does not arouse public concern are longstanding governmental practices that involve surveillance of poor people who receive certain types of public benefits. This article outlines some of those surveillance practices, offers some thoughts on why those surveillance practices garner little public concern, and argues that those who are concerned about warrantless surveillance of ordinary citizens should do more to protect ordinary poor citizens from surveillance.

Since Edward Snowden's first revelations in July 2013, Americans—and the world—have learned that millions of individuals are under surveillance by the U.S. national security apparatus. The controversy surrounding these practices is typically framed in terms of trade-offs between civil rights and liberties (including privacy) on the one hand, and national security concerns on the other. These national security concerns almost invariably invoke the specter of the 9/11 terrorist attacks. However, the trend toward increased surveillance predates 9/11. Notably, federal national security and law enforcement agencies systematically infiltrated and spied on African American communities, civil rights activists and anti-war groups throughout the 1950s, 1960s and early 1970s under the COINTELPRO program (Glick, 1989). The specific targets of state surveillance vary, but the logic stays the same: surveil, control and isolate the sources of perceived risk in order to prevent contagion to the rest of society (Beck, 1992). Since 9/11, Arab and Muslim communities have been the prime targets of domestic surveillance (Greenwald & Hussain, 2014), and several recent books

have examined the Internet economy's reliance on commodification of myriad data points concerning citizen-consumers, gradually habituating us all to pervasive surveillance (Angwin, 2014; Scheer, 2015).

One group of individuals who have been consistently surveilled for decades is generally left out of this conversation: the poor. Indeed, low-income Americans must submit to invasive monitoring of their private lives in order to receive the benefits to which they are legally entitled. This has been the case for decades, with the breadth and depth of surveillance expanding along with the affordances of available technologies. In contrast, very little documentation is required to receive benefits in the form of tax rebates, which generally benefit the rich and amount to much higher sums. Moreover, this mass invasion of privacy receives broad support from the American public, including from many recipients themselves, who often have only vague ideas of what the computerized welfare system knows about them or how this information is acquired (Gustafson, 2011).

Thus, one of the features of 21st century American welfare is widespread surveillance that is poorly understood by its subjects—and, I will argue, whose subjects are largely invisible to mainstream American society. In this paper I use John Gilliom's definition of surveillance: "the increasingly routine use of personal data and systematic information in the administration of institutions, agencies, and businesses" (Gilliom, 2001, p. 2). As we have learned since 2013, mass surveillance has become a hallmark of 21st century American life. Writing in The New Prospect, SUNY professor Virginia Eubanks warns that "the revelations that are so scandalous to the middle class—data profiling, PRISM, tapped cell phones—are old news to millions of low-income Americans, immigrants, and communities of color." She recounts an interview with a young mother on welfare, who told her that while receiving her food stamps though Electronic Bank Transfer (EBT) was convenient, her case worker used the system to review her grocery purchases item by item. "Poor women are the test subjects for surveillance technology," the young woman told Eubanks, "and you should pay attention to what happens to us. You're next." This conversation occurred a decade ago (Eubanks, 2014, para 2).

This article analyzes the cultural norms and beliefs embodied by the American welfare system, considers these norms and beliefs' involvement in other aspects of the surveillance society, critiques the current regime of welfare data collection, and calls for an administration of the social safety net that is both more humane and more effective. After providing an overview of the history of the American social safety net as it stands, emphasizing Johnson's War on Poverty and the Clinton welfare reform, I will turn to the perspectives of welfare recipients themselves and of the general American public, before finally suggesting some directions for future research and policy action.

2. The American Welfare State

The phrase "welfare state" refers to a normative view of government that holds the public sector ultimately responsible for the physical, social and economic well-being of the citizenry. While European countries began providing state-run and tax-funded social safety nets and labor protections starting in the late 19th century, in the U.S. the prevailing view of the elites was that assistance to the needy would only encourage idleness and other undesirable behavior, and that social Darwinism would ensure that only the individuals with the best work ethic and moral character would prosper and reproduce. Franklin Delanoe Roosevelt's New Deal, in the wake of the Great Depression, represented a departure from the past through programs such as the Works Progress Administration, later renamed the Works Projects Administration (WPA), which created employment through great works projects; Social Security, a retirement program for old age and the disabled; and many other poverty-relief programs collectively referred to as "welfare" (O'Connor, 2003).

In addition to Social Security, intended to care for those relatively few (compared to today) individuals who made it to old age, New Deal welfare programs were designed to replace the earnings of an absent, deceased or otherwise incapacitated father figure, thereby allowing mothers to continue in their roles as home-makers and primary care-givers for their children. It is important to note that women of color were largely excluded from receiving benefits through both structural and individual-level racism on the part of program administrators (Mink, 1996; Neubeck & Cazenave, 2001; O'Connor, 2003; Quadagno, 1994).

Decades later, Lyndon Johnson's Great Society, which included both the War on Poverty and civil rights legislation, went a long way toward easing the structural barriers preventing poor blacks from receiving aid as well as institutionalizing the welfare system. However, as black Americans fought to access welfare programs (Piven & Cloward, 1979), public perception of the average welfare recipient shifted from the virtuous white widow heroically raising her children alone to the lazy, promiscuous, deviant (and wholly imaginary) black "welfare queen" mythologized by Ronald Reagan (Gilliom, 2001; Gustafson, 2011; O'Connor, 2003).

The welfare assistance program was further expanded in the 1960s as part of Lyndon Johnson's Great Society initiative, intended to eradicate poverty and correct structural racial injustice. The War on Poverty was thus intertwined with government efforts to enact the demands of the civil rights movement. A comprehensive policy analysis of the War on Poverty would fall outside the scope of the present paper; however a few key facts merit foregrounding. The 1965 Social Security Act raised benefits, increased eligibility, created Medicare (federally-funded medical insurance for Americans

over age 65) and Medicaid (medical insurance for low-income Americans, jointly funded by the federal and state governments), while the 1964 Food Stamp Act made the program permanent (it had consisted of pilot programs until then). Other legislation created the school lunch program, through which poor children receive meals through their schools, and even provided contraception for poor adults through state health departments. By the end of the Johnson Administration, the U.S. appeared to be on its way to easing, if not eradicating, poverty (O'Connor, 2003).

Even as surveillance, work requirements and fraud prevention programs continued to grow, the 1970s, 1980s and early 1990s saw two broad social changes that would prove crucial to the welfare system: changes to the family structure and demographic composition of welfare rolls, and technological advances in information management (Gilliom, 2001; O'Connor, 2003). Divorce and single parenthood became more prevalent, some of the structural barriers preventing poor people of color from accessing aid were dismantled, and the availability of birth control made single motherhood seem more and more like a choice, and less like an unavoidable tragedy. As a result, the American public (and legislators) became less willing to provide support to the poor, and especially to poor, black, single mothers who were increasingly stigmatized as lazy, promiscuous and undeserving. The "welfare queen" rhetoric espoused by Reagan and others also contributed to increased prejudice and stigmatization of poor Americans (Hancock, 2004; Gilens, 1999; Gustafson, 2011; O'Connor, 2003). Writing in 1982, M. Donna Price Cofer warned that "the current mania in this country to dismantle thirty years of social programs will adversely affect not only public assistance recipients but also the agencies that administer these benefits" (Cofer, 1982).

At the same time, networked databases made it possible to classify and surveil large populations, and to do so across administrative boundaries of city, county and state human services offices. To be sure, no welfare state could function without some degree of administrative surveillance. Frank Webster (2014) summarizes the intertwined nature of publicly administered benefits and some degree of surveillance succinctly, reminding us of Anthony Giddens' (1987) assertion that "the administrative power generated by the nation-state could not exist without the information base that is the means of its reflexive self-regulation" (p. 180), and of Paddy Hillyard and Janie Percy-Smith's (1988) conclusion that "the delivery of welfare benefits and services is at the heart of the system of mass surveillance, because it is here that the processes of classification, information gathering and recording are constantly multiplying" (p. 172) (cited in Webster, 2014, p. 298-299).

The combination of increased motivation to reduce welfare spending and increased technical ability to monitor welfare recipients could only lead to increased surveillance, and Cofer's fears would be realized as part of a deal between Bill Clinton and the Gingrich Republicans in the run-up to the 1996 election (O'Connor, 2003).

The 1996 welfare reform bill, formally (and tellingly) titled the Personal Responsibility and Work Opportunity Reconciliation Act (PRWORA), was the culmination of two decades of "conservative ideological and political victories" (O'Connor, 2003, p. 223). As such, it was more concerned with sending a message to the poor about personal morality than about designing evidence-based interventions to provide Americans with a basic minimum standard of living, much less durably lifting families out of poverty. As O'Connor notes, "the preamble to the PRWORA openly describes it as being principally concerned with overcoming the problems caused by out-of-wedlock births and welfare dependency. Further, the act claims that its purpose is to strengthen marriage, personal responsibility, and the work ethic" (O'Connor, 2003, p. 224). Actually reducing poverty is nowhere on the agenda.

The Clinton welfare reform was based on the premise that nearly all parents should work outside the home to support their children, even if the wages they could command in the labor market were less than the cost of childcare. By the 1990s, women's participation in the workforce was already well-entrenched, and the idea that welfare ought to provide an income to poor, husbandless mothers, so that they might stay at home raising their children, was at odds with the new norm of dual-income families. For many, the difficulties of raising children alone while working outside the home were simply the natural consequence of the "irresponsible choice" to have children without a husband's practical and financial support. As we will see, restricting poor women's options with respect to their sexual and reproductive lives—arguably the most personal, private realms of human existence—is a feature, not a bug, of the American welfare system.

The welfare-to-work program featured a number of "sticks and carrots" intended to incentivize work and discourage fraud (or so the claim went), but in practice, the rules were (and continue to be) poorly understood, haphazardly applied, and, it seems, arbitrarily enforced (Gustafson, 2011; Hasenfeld, 2000; Schram, 2000). Moreover, benefit levels are woefully inadequate[1], and

[1] Any good faith discussion of welfare fraud must begin by acknowledging the inadequacy of benefits. To use California as an example, as of 2011, the minimum basic standard of adequate care, as determined by the federal government, for a family of three was $1,135 per month. The Maximum Income for Initial Eligibility for a Family of Three was $1,224, meaning that families earning more than that amount are ineligible for aid. Families needed to already be significantly below the poverty line before they could even apply for aid. The asset limit was $2,000 ($3,000 for households including an elderly per-

families must resort to alternative sources of income to make ends meet. The result is both endemic fraud and widespread underutilization of benefits to which individuals and families are legally entitled (Gustafson, 2011).

The 1996 Act set time limits on how long individuals could receive benefits, imposed work requirements, and drastically tightened eligibility rules. The federally-run Assistance for Families with Dependent Children (AFDC) was replaced by Temporary Assistance for Needy Families (TANF), which is implemented by the states. Under PRWORA the states are given clear incentives from the federal government to "get as many of their welfare population working as possible" (O'Connor, 2003, p. 230). States are also free to impose even tighter eligibility rules and shorter time limits than those envisioned by the PRWORA. The guiding principle of TANF is not meeting the basic needs of poor Americans, but "fraud prevention" (Gustafson, 2011, p. 96).

The Act also empowered state governments to delve into the personal and sexual lives of women of all ages, by requiring single mothers to identify the biological fathers of their offspring and by capping TANF payments to families, meaning that "recipients do not receive any further money if they have more children while on the TANF program" (O'Connor, 2003, p. 230). These "family size caps" are meant to dissuade women from having additional children while on welfare by barring newly born children from being included in benefit calculations. The implication is that the only "legitimate" children are those born to a married mother and father, and that, by definition, the child of a mother on welfare is not "legitimate." During the PRWORA negotiations, "much of the debate cast 'illegitimacy' as America's most pressing social problem, and quickly blamed 'welfare' as its root cause" (O'Connor, 2003, p.235).

While the Act's authors preferred co-parents to be married to each other, in the absence of marriage they were determined to more strictly enforce child support requirements. The implementation of a "national computer tracking system" made it easier to "locate non-resident parents across state boundaries" and garnish their wages (O'Connor, 2003, p. 232). Mothers who can't or won't identify their children's biological father risk losing their TANF eligibility. Money recouped from so-called "dead-beat dads" goes not to the children or their mother, but to the state as a reimbursement for the cost of support that the father should have been providing in the first place, with the exception of a $50 pass-through (O'Connor, 2003). Mothers thus have every economic incentive to resist identifying their children's father.

States also "have the discretion to deny benefits to unmarried teenage mothers," "can mandate teenage mothers attend school," and "require unwed minors to live with a parent or guardian" to receive aid (O'Connor, 2003, p. 230)—regardless of whether that is in the best interest of the young mother or her child. Meanwhile, "the act required the federal government to spend $50 million per year on a new abstinence education program in American schools" (O'Connor, 2003, p. 231) and provided "financial rewards to states that reduce the number of out-of-wedlock births as long as there is not a corresponding increase in the number of abortions performed in that state" — though these "illegitimacy bonuses" were short-lived (O'Connor, 2003, p.231). For all the emphasis on preventing child-bearing by unmarried poor women, PRWORA did nothing to promote use or affordability of methods of birth control other than sexual abstinence. The real problem that PRWORA sought to eradicate wasn't child poverty or even fatherlessness, but sexual activity by poor women (and especially poor women of color) outside the bounds of holy matrimony.

3. Welfare Surveillance: The Recipients' Perspective

According to John Gilliom (2001), "high levels of investigation into the lives of the poor have always been a central part of relief programs" in the United States, "generally designed with little attention to the dignity of the client" (pp. 13-14). This surveillance focuses on "whether or not a family will be eligible for assistance," which is accomplished through a "means test" consisting of "some mechanism for determining if someone is eligible by assessing their needs, their resources, or their capacity to work." For Gilliom, "this one constant in American welfare surveillance, reflecting both our faith in the importance of labor and our suspicion that people will do nearly anything to avoid it, is the central point in the ongoing state examination of the poor" (Gilliom, pp. 19-20).

Ethnographic work by Gilliom (2001), Gustafson (2011), Seccombe (2011), and others provides rich insight into the ways that welfare recipients experience their interactions with the state's surveillance system. Gilliom writes:

> Low-income American mothers live every day with the advanced surveillance capacity of the modern welfare state. In their pursuit of food, health care, and shelter for their families, they are watched, analyzed, assessed, monitored, checked, and reevaluated in an ongoing process involving supercomput-

son), plus one automobile per licensed driver—requiring families to have sold off virtually all their assets. The Maximum Monthly Benefit for a Family of Three with No Income was $638 (non-exempt) or $714 (exempt)—slightly more than half of what the government considers necessary for survival. By contrast, the MIT Living Wage Calculator project estimates that such a family needs $54,764 per year, or $4,564 per month, to make ends meet in California (Glasmeier & Schulteis, 2015).

> ers, caseworkers, fraud control agents, grocers, and neighbors. (Gilliom, 2001, p. xiii)

Additionally, the burden of complying with eligibility verification requirements is often so time-consuming that it interferes with recipients' ability to look for work or care for their families. In rural areas with scant public transportation options, a visit to deliver paperwork to the welfare office can take an entire day. Electronic submission of required documents is either disallowed by the welfare agency, or unavailable to recipients who lack the necessary hardware, Internet access, and computer skills. To add insult to injury, many offices require the same paperwork to be resubmitted on a recurring basis, even though the documentation (Social Security cards, children's birth certificates) does not change over time. As Gustafson notes,

> The documentation of daily life is a form of state surveillance to which welfare recipients submit but also a form of surveillance which they resist, sometimes to their detriment. It was this routine documentation that the interviewees described as invasive and oppressive (Gustafson, 2011, p. 97).

Gilliom's field work also revealed that "the mothers complained about the hassle and degradation caused by surveillance and the ways that it hindered their ability to meet the needs of their families" (Gilliom, 2001, p. 6). Time spent traveling to the welfare office is often perceived as time wasted, and means tests dissuade recipients from taking part-time work or work that would pay less than their welfare benefit—unless they can hide this income from the eligibility worker. Gilliom and Gustafson both describe the calculations that mothers in particular engage in before rationally concluding that their duties to their children demand that they engage in welfare fraud, whether by working under the table or claiming not to know the father's identity or his whereabouts—even if he is in fact a part of the children's lives. Thus, "as the state struggles to know as much as it can about the poor—and to use its knowledge with critical consequences for poor people's lives—an inevitable struggle over information and perception comes to define the unfolding politics of surveillance" (Gilliom, 2001, p. 20).

As with other populations under similar surveillance, welfare recipients feel the psychic weight of living their lives under the watchful eye of the State. The following quotation exemplifies the psychological effect of pervasive surveillance:

> You have to watch every step like you are in prison. All the time you are on welfare, yeah, you are in prison. Someone is watching like a guard. Someone is watching over you and you are hoping every day that you won't go up the creek, so to speak, and (that you will) get out alive in any way, shape or form. You know, "Did I remember to say that a child moved in?" "Did I remember to say that a child moved out?" And, "Did I call within that five days?" You know…making sure all the time….It's as close to a prison that I can think of. (Mary, a forty-something mother of three, on welfare, in Appalachian Ohio (cited in Gilliom, 2001, p. 1))

Paradoxically, Gustafon's field work "revealed that while these welfare recipients found it impossible to comply with the rules and most considered it impossible for anyone to follow the rules, many of the interviewees nonetheless believed that the work requirements, the time limits, the family caps, the extensive reporting rules, and the stiff penalties for breaking the rules were good, necessary, and legitimate" (Gustafson, 2011, p. 170). The women interviewed by both Gilliom and Gustafson had internalized the widespread cultural prejudice against people living in poverty, often buying into tropes that had no basis in reality, such as the Welfare Queen invented by Ronald Reagan. In both studies, virtually all respondents shared the attitude that while they themselves needed and deserved the social safety net, most other people on aid were abusing the system—a perception that is sadly prevalent. The next section delves into the cultural norms and beliefs held by mainstream American society about the poor in general, and welfare recipients in particular.

4. Welfare Surveillance: The "Taxpayers'" Perspective

The following quote, from the online comments on Virginia Eubanks' article in *The New Prospect*, illustrates the widespread belief that welfare payments belong not to the recipient, but to the taxpayer: "As a taxpayer I applaud looking at EBT records to see if you are spending MY money on WHAT I approve of, as in MY money" (online comment to Eubanks, 2014). This line of argumentation suggests an opposition between taxpayers and welfare recipients, between working Americans and poor Americans (even though these conditions are hardly mutual exclusive), in a telling throwback to the 18th and early 19th centuries, when only landowners—who were, of course, exclusively white and male, and didn't necessarily work themselves—could vote. Nearly 200 years later, arguments that full participation in society is tied to economic participation through tax-paying remain, framing the right to vote as the province of the "productive," and not as an inherent right conferred by citizenship. Dorothy E. Roberts characterized this divide as one between citizens and subjects (Roberts, 1996). This conception, of course, obscures the fact that no one is a tax payer throughout the life cycle (childhood, old age), and there are very few people who never pay taxes. We can see this wealth-based model of citizenship at work

in present-day efforts to pass voter ID requirements, which overwhelmingly impact the poor, and to the drastically different rhetoric surrounding taking advantage of tax deductions, which disproportionately benefit the wealthy and upper-middle classes.

This frame was prominent during Mitt Romney's 2012 presidential campaign, especially after Romney was recorded telling a room of wealthy campaign donors that "47 per cent" of Americans were "moochers" who "paid no income tax" and didn't take "personal responsibility…for their lives" (Beutler, 2014). Romney's running mate Paul Ryan similarly contrasted "makers" to "takers," and a number of political commentators have noted that this was a "foundational belief" of the Romney/Ryan campaign (Beutler, 2014, para 8). In contract, Barack Obama, who was then running for reelection, was quick to retort:

> When you express an attitude that half the country considers itself victims, that somehow they want to be dependent on government…maybe you haven't gotten around a lot…the American people are the hardest-working people there are. Their problem is not that they're not working hard enough or that they don't want to work, or they're being taxed too little, or that they just want to loaf around and gather government checks. People want a hand up, not a handout" (quoted in Landler, 2012).

The claim that entitlement spending was out of control and unaffordable for the federal budget reemerged in late 2013 as Congress debated whether to authorize an extension of unemployment benefits for the millions of Americans who lost their jobs during the Great Recession and whose unemployment insurance was about to expire. Yet even the strongest advocates of extending unemployment insurance, such as the office of Harry Reid, then the Senate Majority Leader, differentiated between the deserving unemployed who had fallen victims to the recession "through no fault of their own" and "need this lifeline to make ends meet while they continue to look for work" (Kaplan, n.d.), and the undeserving, unmentioned masses of the poor dependent on other forms of public assistance.

While Democrats, liberals and progressives essentially remain quiet about welfare recipients, Republicans and other conservatives are quite vocal about their beliefs that poverty is primarily the individual's fault, and that poverty relief hurts rather than helps the poor. For example, a Forbes article by Peter Ferrara claims that the War on Poverty caused poverty rates to rise after 1965, while simultaneously asserting that "one major reason that poverty stopped declining after the War on Poverty started is that the poor and lower income population stopped working" (Ferrara, 2013, para 7), and foregrounding the War on Poverty's "association with the breakup of lower-income families and soaring out-of-wedlock births" (Ferrara, 2013, para 8). Yet despite its incendiary title ("'Welfare State' Doesn't Adequately Describe How Much America's Poor Control Your Wallet") the article does nothing to connect spending on social welfare programs to the individuals wallets of Forbes' imagined audience. A review of several recent publications by the Heritage Foundation, a leading conservative think tank, reveals that for conservative thinkers, the success of a given welfare program or policy should be measured by its stinginess, and not by whether it helps the poor maintain a basic standard of living. For example, The Daily Signal's[2] coverage of a TANF program extension in Colorado notes, "the [program] documents conceded the change could increase money going to welfare recipients and keep them on the program longer" (Kane, 2014, para 4). In the context of an anemic economic recovery that is concentrated in the upper socioeconomic classes, it would seem that an increase in benefits would be precisely the point of such a policy change. Similarly, articles by Edwin J. Feulner and by Robert Rector (2014) decry the dollar figures of welfare spending without ever considering the lived experiences of the poor. Human beings living in poverty are completely absent from the conversation about welfare, except when they are villainized and shamed.

Though it failed to pass, in late 2014 Congress considered an amendment to the Farm Bill requiring food surveillance in the Supplement Nutrition Assistance Program (SNAP). The legislation would have "mandated that retail food stores collect, and report to the Secretary of Agriculture, detailed information that identifies food items purchased with benefits provided under the supplemental nutrition assistance program" (Rogers, 2014). It is not at all clear what the amendment's sponsors thought should be done with this information, but the logic behind such a proposal is exactly what the commenter on Eubanks' article spelled out: welfare benefits are funded with tax dollars, which come from individual (as well as corporate) taxpayers, *ergo* said taxpayers have a right to know and control what welfare recipients purchase. This is the same logic that Hobby Lobby and its supporters used in *Burwell vs. Hobby Lobby Stores, Inc.* to successfully argue that at least some corporations should be exempt from the Affordable Care Act's requirement that health insurance plans cover birth control at no additional cost (beyond the insurance premium itself). Financial contribution, no matter how indirect, is construed as a source of legitimacy for controlling women's bodies. Poor women, by definition, lack the financial resources to combat

[2] A "national network of investigative reporters covering waste, fraud and abuse in government" affiliated with the Franklin Center for Government & Public Integrity. The Heritage Foundation's website prominently links to The Daily Signal, signaling the outfit's ideological affiliation.

these claims, whereas wealthier women are exempt from this control, as they tend to have better health insurance coverage or can afford to pay out-of-pocket. Yet we seldom hear serious arguments from pacifists that they should be able to veto defense expenditures because they pay taxes, or from scientists who refuse to pay for public school systems that teach Creationism, for example. There seems to be a cultural link between conservative thought and the belief that financially contributing to something, no matter how indirectly, creates a right to control distant outcomes.

5. Analysis

Welfare offices at every level of government spend exorbitant sums cross-referencing databases, following up on tips from welfare fraud hotlines, drug-testing, physically surveilling, and legally prosecuting the poor, ostensibly to save the taxpayer money by cutting off welfare frauds and cheaters. In many jurisdictions, the amount spent on welfare enforcement dwarves the sums saved by removing "cheaters" from welfare rolls. For example, the state of Utah spent $30,000 over the course of a year to ferret out presumed drug use among welfare recipients. The program found that only 2.6% tested positive for illegal drugs, which is well below the national use rate, 8.9% (Kelly, 2013). Programs in Arizona, Oklahoma and Florida similarly failed at their purported goal of saving taxpayer money. In fact, the Florida program cost the state $45,780 in testing expenditures (Alvarez, 2012).

One might think that this money would be better spent on welfare itself, especially in the context of the Great Recession and anemic recovery. However, a large body of social science research suggests that the guiding logic of the U.S. welfare system is not the actual wellbeing of poor families, but punishing the poor *for being poor* and setting them up as cautionary examples to discourage others from being poor as well (Bussiere, 1997; Gustafson, 2011; Eubanks, 2012; Piven & Cloward, 1993; Gilliom, 2001; O'Connor, 2003; Seccombe, 2011; Soss, 2002). As Salon's Brian P. Kelly put it,

> Welfare-based drug testing is only a symptom of a larger societal ill that sees the poor as inherently parasitic and viceful (e.g., "They take advantage of government programs, not us." "They do drugs, not us."). As a result, legislators heap unfair, ineffective policies on those in poverty simply to court public favor by playing to their prejudices. The welfare queen, cashing government checks, smoking drugs and living the life of luxury, continues to be a useful myth when it comes to winning votes. And as more of these policies, whose support is borne by an unfounded disdain for the poor, are enacted, the humanity of those living in poverty is further eroded as the chasm between the haves and the have-nots grows even wider. (Kelly, 2013)

Indeed, for Gustafson, "the drug testing of welfare recipients particularly highlights the conflation of poverty and crime and the widespread assumption that poor women of color are the causes of crime" (Gustafson, 2011, p. 60). While it seems that awareness of the limited usefulness of drug testing is relatively widespread in policy circles, the systematic surveillance of welfare recipients is either ignored or uncontroversial.

While mass drug testing seeks to control the risk that is presumably caused by poor women's bodies, electronic surveillance situates the assumed risk in the practices of everyday life, not least of which include poor women's sexual and reproductive lives. As more and more of daily life is captured by electronic databases whose data can be matched and analyzed in increasingly revealing ways, more facets of the human condition become susceptible to surveillance (Bauman & Lyon, 2013). Electronic surveillance of the poor is particularly insidious for three reasons. First, welfare recipients who lack formal education and computer skills often have trouble conceiving of the types of data and computational analysis that are possible. Second, they lack the political capital to fight the system, much less change it, particularly as many welfare recipients have so internalized the trope of the "Welfare Queen" that they profess to believe that the system and its rules are necessary and just, even as they themselves "cheat" the system in whatever ways necessary to survive and provide for their families (Gilliom, 2001; Gustafson, 2011).

And finally, in the United States the receipt of most kinds of public assistance is highly stigmatized (with the important exception of maximizing tax deductions, which is widely applauded), and there is widespread support for all kinds of government intrusion in the lives of the poor: unannounced home visits, mandatory drug testing, electronic and physical surveillance, and family benefit caps intended to discourage women who receive welfare from giving birth to additional children. For example, the third comment on the online version of Eubanks' New Prospect article contains multiple assertions that "As a taxpayer I applaud looking at EBT records to see if you are spending MY money on WHAT I approve of, as in MY money" (Eubanks, 2014, online comments). This quote is representative of widespread cultural beliefs, as I discussed in the previous section.

6. Conclusion

This paper has tackled the systematic surveillance of Americans by foregrounding the well-entrenched practice of surveilling the poorest and most vulnerable members of society: welfare recipients. This practice is, outside of certain activist and academic circles, utterly uncontroversial and enjoys wide public support, even as other kinds of surveillance are coming under scrutiny. Writing in 2008, Henman and Marston noted that "the

social policy literature seems to have taken a limited interest in recent developments in surveillance practices" (Henman & Marston, 2008, p. 188) and that "academic interest in the social division of welfare has waned in recent years" (Henman & Marston, 2008, p. 191).

While the academic and legal literature on this topic is very rich and conservative think tanks are prolific on the perils of welfare spending, the issue appears to be all but ignored in progressive public policy circles, even as they focus attention and resources on the mass surveillance programs that Edward Snowden exposed. I found only one reference to welfare surveillance among recent think tank policy papers, a collection of essays on "Big Data and Discrimination" published by New America (Peña Gangadharan, 2014). The digital rights sector doesn't perform much better: for example, the Electronic Privacy Information Center (EPIC) website has a page dedicated to "Poverty and Privacy," but it doesn't refer to any materials published since 2003. I have, however, been privy to confidential conversations and strategy meetings of civil society researchers and activists about the surveillance to which communities of color, including welfare recipients, are subjected. It remains to be seen what will come of these projects. Professional advocacy organizations tend to pick battles that they think they can win, and so far there is no indication that fighting for the civil rights and human dignity of welfare recipients is a winning political tactic. Updated research in the vein of Piven and Cloward's excellent "Poor People's Movements" (1979) is needed if poor Americans are to regain their dignity and humanity. Encouragingly, the aforementioned Virginia Eubanks is currently working on a book about welfare surveillance.

The paucity of the policy-oriented literature may very well be due to the absence of data, as the decentralized structure of welfare administration since 1996 makes it all but impossible to come by nationally comparable datasets on the welfare population or benefit levels. Because welfare programs are administered by the states on a county-by-county basis, the federal government has little to no authority to oversee or critically assess the adequacy of benefit levels, bureaucratic processes, or the return on investment in terms of assuring a decent quality of life for the poorest among us. For example, the statistics maintained by the Department of Health and Human Services (HHS) measure expenditures and the number of beneficiaries; no effort is made to account for how well welfare programs meet recipients' basic needs, or how well the programs are administered. In fact, states measure the success of their welfare programs by the number of needy Americans they can remove from the welfare rolls, regardless of what happens to these families afterward.

As discussed previously, welfare policy is plagued by the inaccurate beliefs that many Americans hold about public assistance beneficiaries. Speaking at a 2015 symposium organized by the University of Southern California Law School, Kaaryn Gustafson went so far as to say that we have "no chance" of living in a society where everyone (notably poor mothers) is treated with dignity and humanity until we dispense with the "Welfare Queen" trope. In turn, correcting these misperceptions is hindered by the information and data flows concerning welfare and its beneficiaries. The official statistics on welfare and poverty measure the wrong things in the wrong way, thereby creating nonfactual "knowledge" that hides genuine problems (hunger, poverty) while surfacing imaginary ones (illegitimacy, drug abuse, fraud, etc.).

Rather than measuring the prevalence of poverty and its human costs, federal statistics focus on the administration of the programs. For example, the Tenth TANF Annual Report to Congress noted that in 2011 (the most recent year for which this report is available), the Federal poverty threshold for a family of four (two adults plus two children) was $22,811, that 21.9% of children were living in poverty that year (16.1 million), and that the child poverty rate in 2011 was 5.7 percentage points higher than in 2000. However, the report does not mention whether TANF (or other welfare programs) was successful in reducing the number of American children (much less adults) living in poverty, or the percentage of need that is met. Even the report's authors seem to be aware of the limitations of their data, noting:

> Participation of Eligible Families
> While many see TANF's caseload decline as a measure of the success of welfare reform, the sharp decline in participation among eligible families also raises concerns about its effectiveness as a safety net program. HHS uses an Urban Institute model to estimate the percentage of families eligible for assistance under state rules that are actually receiving TANF assistance.
> As shown in Figure 2-E, and Appendix Table 2:3, this participation rate data shows that the share of eligible families receiving TANF declined from 84 percent in 1995 to 32 percent in 2009. (Tenth TANF Report to Congress, 2013, p. 21)

From these figures, it should be possible to compare benefits awarded against the need they are intended to ameliorate, yet this is not done. The closest that the report comes is Figure 9B, "Income Poverty Gap for All Families with Children 1997–2011" (p. 54). The poverty gap refers to the amount of money that would be required to raise all poor families to the poverty line. However, the figures are only provided with respect to families with children—demonstrating a lack of concern for adults living in poverty—and are not broken down by state or by any other category. The figures convey the fact that in 2011, it would have cost $76.5

billion to raise all American children out of poverty, but stops short of providing any information that would help achieve this.

The report also highlights the low rates of participation of TANF-eligible families, yet it does not provide any additional information on possible reasons why less than a third of families that are eligible for TANF are not receiving benefits, stating:

> In FY 1994, the assistance caseload reached a high of an average monthly 5.05 million families; six years later, the assistance caseload declined to an average monthly 2.36 million families in FY 2000. This decline has been attributed to a host of events, including economic growth (and the concomitant drop in poverty), welfare reform implementation, and other policies designed to promote work among low-income families with children (such as expansions in the Earned Income Tax Credit and child care subsidies). Throughout this period, there was a dramatic increase in the number of single mothers leaving TANF for work. (Tenth TANF Report to Congress, 2013, p. 15).

The last sentence clearly refers to the myth of Welfare Queen—still very much a concern for bureaucrats and elected officials alike. The reference to "welfare reform implementation" is a blatant tautology: welfare reform tightened eligibility requirements, and as a result fewer people were eligible for benefits—hardly the same thing as eliminating or even reducing poverty.

The example of federal statistics concerning TANF illustrate the broader reality that assessments of welfare programs emphasize inputs such as expenditures, ignoring program outputs and other measures of human wellbeing. From a public administration perspective this makes sense: the Department of Health and Human Services is legally mandated to collect and report these statistics. The question remains why it does not also provide measures of human wellbeing.

Moreover, the fact that a practice is legally mandated provides an explanation for why it exists, but does not constitute a moral or ethical reason. As with many other situations (legal protections for whistleblowers come to mind), the United States and postmodern societies more broadly lack a mechanism for reconciling the gap between what is legal and what is ethically or morally just.

The information that is most crucially lacking in the current data flows concerning welfare fall under three categories: the extent of need, how much of that need is met by the social safety net, and cost/benefit analyses of fraud prevention. The fact that so many members of the wealthiest society in human history are needy is reprehensible, and welfare programs ought to be evaluated by their success in meeting that need. Granular datasets and tables that examine these two types of measures by state, county, and various demographic dimensions would shed light on outcome disparities between different groups, thus allowing for targeted remedies. Finally, the effectiveness of fraud-prevention schemes should be methodically assessed. Schemes that cost more than the amount saved should be eliminated, and the funding reinvested into benefit payments. For example, in 2009 the California State Auditor found that "the measurable savings resulting from early fraud detection activities exceed the costs of such efforts for CalWORKs and approach cost neutrality for the food stamp program" (Howle, 2009). By this logic, then, early fraud detection was a valuable investment for CalWORKS, but not for food stamps. More state and local level auditors and Inspectors General should pursue this kind of analysis and pressure the agencies that administer welfare programs to do the same.

It is vitally important that researchers in academia, in government, and in civil society do the work of generating accurate, nationally comparable empirical evidence to inform policy and debate. Indeed, the lack of data is a key barrier to both research and advocacy. Even as the system relentlessly seeks out every scrap of information about the poor to verify their deservingness, it deliberately fails to provide systemic data that would help administer programs more effectively. This is a stunning paradox: a system whose guiding principle is the collection of information yields virtually no data that could meaningfully inform public policy.

To the lay person the argument that welfare surveillance robs the poor of their dignity and humanity may seem like wild hyperbole. But as Gilliom reminds us,

> Surveillance programs are ways of seeing and knowing the world. They assert values, identify priorities, define possibilities, and police the departures. In so doing, they build important structures of meaning that help to shape our world and our place within it (Gilliom, 2001, p. xiii).

Welfare surveillance is also a feminist issue. As I have discussed, surveillance of welfare recipients is overwhelmingly concerned with the sexual and reproductive lives of poor women, as reflected by practices such as bed checks, family size caps, and home visits designed to catch women living with an unrelated male. Additionally, poor women—and increasingly, working class women—are denied access to birth control, then shamed and punished for becoming pregnant. As abortion care becomes increasingly restricted, the message sent to poor women is a simple choice: marriage or abstinence. Meanwhile, poor men are largely excluded from receiving aid since most welfare programs are designed to support children (and by association their caregivers, albeit begrudgingly). The main mechanism through which poor men are expected to interact with

the welfare system is through child support collections.

Popular opposition to welfare is deeply rooted in the historical legacy of racism (Gordon, 1994; Quadagno, 1994). Indeed, opposition to the social safety net is connected to the (inaccurate) belief that welfare recipients are overwhelmingly black (Gilens, 1999). Surveillance of any kind is "not a mere glance exchanged between equals—it is both an expression and instrument of power" (Gilliom, 2001, p. 3). By exercising their right to surveil and control the daily lives of poor Americans via the state, self-proclaimed "taxpayers" assert their position of privilege over the poor and mark them as Other.

Nor is welfare distinct from the plight of low-wage workers in a neoliberal society. Under the transatlantic leadership of Reagan and Thatcher, the 1980s saw "an assault on organized labor, initially the trade unions, but extending to collectivist ideas *tout court*" (Webster, 2014, p. 85)—including the notion of a social safety net. This trend has only accelerated over the past 30 years. As companies increasingly automate low-skilled work and outsource jobs to cheaper labor markets, the share of the U.S. workforce that is contingent (i.e. cycling between employment and unemployment) has been growing steadily, reaching up to 25% of the labor market (Webster, 2014, p. 89). The most vulnerable among these are discursively excluded from society, and are instead constructed as an underclass "thought to inhabit the inner city ghettoes and isolated parts of the regions, but significantly it is considered a tiny group *detached* from the vast majority of society, separate and self-perpetuating, which, if an irritant to law-abiding, is apart from the bulk of the populace, which is mortgage-owning, self- and career-centered" (Webster, 2014, p. 89). As a result, the poor, left "without a stake in post-industrial society…are to be pitied, feared and condemned (Dalrymple, 2005; Mount, 2010)" (Webster, 2014, p. 90).

While it is true that the poor's standard of living is higher today than it was in the industrial era, the poor have been increasingly marginalized relative to the middle and upper classes. Webster (2014) notes that "while in the past the working class was subordinate to the owners of capital, it was widely accepted that it was still indispensable" (Webster, 2014, p. 123). Today, with much of American manufacturing and blue-collar jobs having been outsourced to countries with lower labor costs (and often lesser or non-existent regulatory protections for labor), it is much easier for the middle and upper classes to dismiss the poor as a distant "Other" whose struggles are theoretically troubling, but practically irrelevant. This is why I propose to change the data inputs into the cybernetic machine of the welfare state (Wiener, 1988). Only when the state, and the bureaucrats who comprise it, start measuring success by human impact factors rather than economic measures of thrift will meaningful policy change be possible. Civil society should lead the way by producing these datasets to the extent possible, perhaps by focusing on a specific state or local jurisdiction, then confronting relevant public sector actors about the relative inadequacy of their own data. The California State Auditor's report is an encouraging example of what can be accomplished.

In this paper I have alluded to the surveillance society's shifting gaze as one group after another has become targeted for surveillance. The function of surveillance is to monitor and isolate the risk that each group is deemed to present to society: welfare recipients, African Americans, civil rights activists, Arab and Muslim Americans, journalists, individual police officers, and more. In addition to direct state surveillance, 21st century Americans are also subject to commercial and social surveillance through social networking sites, which often provide the mechanism for state surveillance (Angwin, 2014; Scheer, 2015). Much like the proverbial frog who is boiled to death because he fails to realize that the water is getting warmer, we as a society—Americans in particular, but not exclusively—are in danger of waking up in a Panopticon of our own creation.

Acknowledgements

The author wishes to thank the following individuals for their comments on early versions of this article: Manuel Castells, Cat Duffy, Henry Jenkins, and Andrew Shrock.

Conflict of Interests

The author declares no conflict of interests.

References

Alvarez, L. (2012, April 17). No savings found in Florida welfare drug tests. *The New York Times*. Retrieved from http://www.nytimes.com/2012/04/18/us/no-savings-found-in-florida-welfare-drug-tests.html

Angwin, J. (2014). *Dragnet nation: A quest for privacy, security, and freedom in a world of relentless surveillance* (First edition). New York: Times Books, Henry Holt and Company.

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

Beck, U. (1992). *Risk society: Towards a new modernity*. London, Newbury Park, CA: Sage Publications.

Beutler, B. (2014, September 30). Mitt Romney blames his "47 percent" comment on a donor. Paul Ryan blames…Mitt Romney. *The New Republic*. Retrieved from http://www.newrepublic.com/article/119645/romney-47-percent-quote-was-donors-fault-paul-ryan-it-was-wrong

Bussiere, E. (1997). *(Dis)entitling the poor: The Warren*

Court, welfare rights, and the American political tradition. University Park, PA: Pennsylvania State University Press.

Cofer, M. D. P. (1982). *Administering public assistance: A constitutional and administrative perspective*. Port Washington, NY: Kennikat Press.

Dalrymple, T. (2005). *Our culture, what's left of it: The mandarins and the masses*. Chicago: Ivan R. Dee.

Eubanks, V. (2012). *Digital dead end: Fighting for social justice in the Information Age*. Cambridge, MA, London: MIT Press.

Eubanks, V. (2014, January 15). Want to predict the future of surveillance? Ask poor communities. *The American Prospect*. Retrieved from http://prospect.org/article/want-predict-future-surveillance-ask-poor-communities

Ferrara, P. (2013, June 23). "Welfare state" doesn't adequately describe how much America's poor control your wallet. Retrieved from http://www.forbes.com/sites/peterferrara/2013/06/23/welfare-state-doesnt-adequately-describe-how-much-americas-poor-control-your-wallet

Giddens, A. (1987). *The Nation-state and violence*. Berkeley: University of California Press.

Gilens, M. (1999). *Why Americans hate welfare: Race, media, and the politics of antipoverty policy*. Chicago: University of Chicago Press.

Gilliom, J. (2001). *Overseers of the poor: Surveillance, resistance, and the limits of privacy*. Chicago: University of Chicago Press.

Glasmeier, A. K., & Schulteis, E. (2015). Poverty in America: Living wage calculator (California). Boston, MA: Massachusetts Institute of Technology. Retrieved from http://livingwage.mit.edu/states/06

Glick, B. (1989). *War at home: Covert action against U.S. activists and what we can do about it* (1st ed.). Boston, MA: South End Press.

Gordon, L. (1994). *Pitied but not entitled: Single mothers and the history of welfare*. New York, NY: The Free Press.

Greenwald, G., & Hussain, M. (2014, July 8). Meet the Muslim-American leaders the FBI and NSA have been spying on. *The Intercept*. Retrieved from https://firstlook.org/theintercept/2014/07/09/under-surveillance

Gustafson, K. S. (2011). *Cheating welfare: Public assistance and the criminalization of poverty*. New York: New York University Press.

Hancock, A. M. (2004). *The politics of disgust: The public identity of the welfare queen*. New York: NYU Press.

Hasenfeld, Y. (2000). Organizational forms as moral practices: The case of welfare departments. *Social Service Review*, *74*(3), 329-351.

Henman, P., & Marston, G. (2008). The social division of welfare surveillance. *Journal of Social Policy*, *37*(2), 187-205. doi:10.1017/S0047279407001705

Hillyard, P., & Percy-Smith, J. (1988). *The coercive state*. London: Fontana.

Howle, E. M. (2009). *Department of social services: for the CalWORKs and food stamp programs, it lacks assessments of cost-effectiveness and misses opportunities to improve counties' antifraud efforts* (84 pp.). California State Auditor. Retrieved from https://www.bsa.ca.gov/pdfs/reports/2009-101.pdf

Kane, A. (2014, November 19). Colorado's new welfare rule increases benefits, costs taxpayers. Retrieved from http://dailysignal.com/2014/11/19/colorados-new-welfare-rule-increases-benefits-costs-taxpayers

Kaplan, R. (n.d.). John Boehner nixes unemployment insurance extension. Retrieved from http://www.cbsnews.com/news/john-boehner-nixes-unemployment-insurance-extension

Kelly, B. P. (2013). An inane, money-eating sham: Drug tests for welfare a huge failure. Retrieved from http://www.salon.com/2013/08/29/gop%e2%80%99s_inane_money_eating_sham_drug_tests_for_welfare_a_huge_failure

Landler, M. (2012, September 20). Obama hits Romney over 47 percent remark. *The New York Times "The Caucus" Blog*. Retrieved from http://thecaucus.blogs.nytimes.com/2012/09/20/obama-hits-back-at-romney-on-47-percent-remark

Mink, G. (1996). *The wages of motherhood: Inequality in the welfare state, 1917–1942*. Cornell University Press.

Mount, F. (2010). *Mind the gap 2010*. London: Short.

Neubeck, K. J., & Cazenave, N. A. (2001). *Welfare racism: Playing the race card against America's poor*. Psychology Press.

O'Connor, B. (2003). *A political history of the American welfare system: Ehen ideas have consequences*. Lanham, MD: Rowman & Littlefield.

Office of Family Assistance, Administration for Children and Families, U.S. Department of Health and Human Services. (2013). *Tenth TANF Report to Congress*. Washington, DC. Retrieved from http://www.acf.hhs.gov/programs/ofa/resource/tenth-report-to-congress

Peña Gangadharan, S. (2014). Data and Discrimination: Collected Essays. Washington, DC: New America. Retrieved from http://www.newamerica.org/downloads/OTI-Data-an-Discrimination-FINAL-small.pdf

Piven, F. F., & Cloward, R. A. (1979). *Poor people's movements: Why they succeed, how they fail* (Vol. 697). New York: Vintage books.

Piven, F. F., & Cloward, R. A. (1993). *Regulating the poor: The functions of public welfare*. New York: Vintage Books.

Quadagno J. (1994). *The color of welfare: How racism undermined the war on poverty*. New York, NY: Oxford University Press, 1994.

Rector, R. (2014, February). Help the poor by trans-

forming, not growing, welfare. Retrieved from http://dailysignal.com/2014/02/01/help-poor-transforming-growing-welfare

Roberts, D. E. (1996). *Welfare and the problem of black citizenship* (University of Pennsylvania Law School Faculty Scholarship Paper 1283). Retrieved from http://scholarship.law.upenn.edu/faculty_scholarship/1283

Rogers, J. (2014, September 25). *Food surveillance is not welfare reform*. *CapAllies Post*. Retrieved from http://capallies.com/2014/09/food-surveillance-is-not-welfare-reform

Scheer, R. (2015). *They know everything about you: How data-collecting corporations and snooping government agencies are destroying democracy*. New York: Nation Books.

Schram, S. (2000). *After welfare: The culture of postindustrial social policy*. NYU Press.

Seccombe, K. (2011). *"So you think I drive a Cadillac?": Welfare recipients' perspectives on the system and its reform* (3rd ed.). Boston, MA: Allyn & Bacon.

Soss, J. (2002). *Unwanted claims: The politics of participation in the U.S. welfare system*. Ann Arbor: University of Michigan Press.

Webster, F. (2014). *Theories of the information society* (4th ed.). Abingdon, Oxon: Routledge.

Wiener, N. (1988). *The human use of human beings: Cybernetics and society*. New York, NY: Da Capo Press.

About the Author

Nathalie Maréchal

Nathalie Maréchal is a PhD student in Communication at the University of Southern California. Her research interests include media and international relations, media history, international and comparative media, media ethics, technology and society, and cross-cultural communication, while her own work focuses on privacy, surveillance, human rights, activism, and the political economy of circumvention and anonymization technology.

COGITATIO

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 3, Pages 68-80
Doi: 10.17645/mac.v3i3.301

Article

"Austerity Surveillance" in Greece under the Austerity Regime (2010–2014)

Minas Samatas

Sociology Department, University of Crete, Rethymno, 74100, Crete, Greece; E-Mail: samatasm@uoc.gr

Submitted: 25 April 2015 | In Revised Form: 15 August 2015 | Accepted: 4 September 2015 | Published: 20 October 2015

Abstract
In this article we have tried to analyze "austerity surveillance" (AS), its features, and its functions under the extreme austerity regime in Greece during 2010–2014, before the election of the leftist government. AS is a specific kind of coercive neoliberal surveillance, which in the name of fighting tax evasion and corruption is targeting the middle and lower economic strata and not the rich upper classes. It is based mainly on "coveillance," i.e. citizen-informers' grassing, public naming, and shaming. Functioning as a domination and disciplinary control mechanism of the entire population, it works within a post-democratic setting without accountability or democratic control. We provide empirical evidence of these features and functions, including some indicative personal testimonies of austerity surveillance subjects. After presenting some cases of electronic surveillance as an indispensable supplement to AS, we then briefly underline the negative personal, and socio-political impact of this surveillance. In conclusion, a tentative assessment is made of AS' efficiency in the Greek case, comparing it with other types of past and present authoritarian surveillance in Greece and in other current surveillance societies, considering also the prospects for its abolition or its reproduction by the new leftist government.

Keywords
austerity; coveillance; Greece; surveillance

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

1. Introduction

According to Greek mythology, *Argos Panoptes* was a hundred-eyed giant, a very effective watchman, used by Zeus' wife, Hera, to watch Zeus' lover, Nymph Io. Zeus sent Hermes to rescue his lover, and Hermes slew Argos with his sword. To commemorate her faithful watchman, Hera had the hundred eyes of Argos preserved forever, on the peacock's tail, her sacred bird. *Panoptes* ("All-seeing") signifies on the one hand the wakeful alertness of a watchman, who had so many eyes that only a few of them would sleep at a time, while there were always eyes still awake.[1] On the other hand, *Argos Panoptes* signifies surveillance as a very effective, but also contested, control instrument, used by the powerful authorities. The questions of who is using *Panoptes* against whom, and for what reason, who trusts him and to whom he is faithful, and how one can get rid of him are eternal questions about surveillance, either in the case of spying enemies or allies, or simply of watching individuals, citizens, consumers, etc. *Panoptes*' myth is always appropriate when talking about surveillance in Greece, especially nowadays when Greek people struggle against the draconian austerity regime and its *Panoptes* surveillance.

Our analysis here refers to the austerity regime in Greece from 2010–2014, before the electoral victory of the leftist party SYRIZA on January 25, 2015 and the formation of Alexis Tsipras' government.

Although we live in the "age of austerity" (Schaefer

[1] See http://www.theoi.com/Gigante/GiganteArgosPanoptes.html

& Streeck, 2013) and most democratic states enforce austerity measures, these are particularly harsh in southern Europe, with Greece as the most extreme case. It seems that Greece has been chosen by the Troika, i.e. the IMF, the European Central Bank (ECB), and the European Commission (EC) as a laboratory for a new model of socioeconomic organization for the European over-indebted countries. This laboratory aims, under extreme austerity and surveillance, to create a disciplined society, totally passive and receptive to the neoliberal policies of market domination and social disintegration (Douzinas, 2013; Stavrakakis, 2014).

We have to remind one that Greece is the weakest member in the Eurozone debt crisis, which began to unravel in 2009. Worries that Greece would default on its debt forced the European Union (EU) to rescue the Greek economy with two bailouts, in 2010 and 2014, totaling €240 billion, under draconian memoranda for shrinking the public sector and enforcing severe constraints of social spending. Since the first bailout of Greece, an austerity regime has been established under the strict supervision of the Troika, enforcing a neoliberal austerity policy to save the Greek banks and pay off the lenders, but with detrimental results for the Greek population. According to data collected by Eurostat, the EU's statistics agency, about 30 percent of the Greek population now lives below the poverty line—with 15 percent living in conditions of extreme poverty.[2]

The argument that Greece has been a "debt colony," shackled to its lenders, sounds more and more persuasive. It is a subservient state to a trust of Eurocrats, Euro-bankers, and neoliberal governmental elites in northern Europe, which collaborates with the Greek ruling elite to impose the neoliberal austerity doctrine, regardless of its apparent failure and detrimental impact on the Greek people (Kotzias, 2012; Stavrakakis, 2014; Tsimitakis, 2012). In order to impose strict austerity measures, the pro-austerity Greek governments under the Troika pressures have *de facto* given up national sovereignty and continuously used undemocratic methods, like legislative ordinances, that circumvent the Greek constitution (Chrysogonos, 2013).

This Greek austerity regime is organized according to the austerity memoranda, which have prescribed the rules, norms, and key austerity policies of governance, under the strict supervision of the Troika. The austerity governance was implemented by a coalition government of the traditional rival, post-dictatorial ruling parties, i.e., the right-wing New Democracy party and the center-left "socialist" PASOK party, which are both responsible for Greek bankruptcy, due to their clientelist and corrupt politics.

The Greek austerity regime has been using a specific type of surveillance, which we call "austerity surveillance," to create a coercive, insecure and disciplined society of informers; this type of surveillance and its impact we aim to analyze in this article. For our analysis we have to consider that Greece is a post-authoritarian surveillance society, which due to the post-civil war police state and military dictatorship (1949−1974) has resisted during the entire post-dictatorial period and before the financial crisis (1974−2009) any kind of new, electronic surveillance (Samatas, 2004). Based on pretty good constitutional and legislative protections of freedoms and privacy, post-dictatorial Greece had a good record of privacy and data protection, as was confirmed by the EPIC survey of 2006, discussed further below.

In this article we try first to define "austerity surveillance" (AS), describing its features and functions, which reflect the extreme austerity regime in Greece during 2010−2014; second, we provide empirical evidence of these features, and some indicative personal testimonies of austerity surveillance subjects; then, we present some cases of electronic surveillance, as an indispensable supplement to the AS; then, we briefly underline the impact of this surveillance, comparing it with other types of authoritarian surveillance in the Greek past as well as current coercive surveillance in advanced surveillance societies; finally, we conclude with a tentative assessment of the efficiency of AS in Greece and consider the prospects for the abolition or reproduction of the austerity surveillance by the new leftist government.

We have tried to substantiate our arguments about the features of this particular type of surveillance with lots of empirical data. Also, as we have done with our research on anticommunist surveillance in Greece, where we had used an in-depth conversational analysis (Samatas, 2005), we have similarly examined "austerity surveillance" through "exploratory discussions" with a number of selected individuals who have been victims of or have resisted the austerity regime, discussing and listening to their narrative "stories," following a similar narrative methodology with the IRISS report (2014, p. 4).

2. The Features of "Austerity Surveillance" as a Basic Control Mechanism of the Greek Austerity Regime

Surveillance implies power and control, since it means monitoring people, gathering and analysing personal information in order to regulate or govern their behavior (Gilliom & Monahan, 2013, p. 2). State surveillance in a democratic setting can be an effective control mechanism provided that it is legitimate and

[2] About 1,000 more people lose their jobs every day, and long-term poverty is knocking at the door of a new class of low-paid workers. Greeks' purchasing power has fallen by half since 2010; also, while the public healthcare system is being destroyed and spending on public education has fallen to levels last seen in the 1980s, the cost of living in the country remains high. All these push the young educated Greeks to massively emigrate abroad (Tsimitakis, 2012).

accountable, having the citizens' acceptance and trust; because within a democratic setting there are rules of limitation and oversight of the watchers, protecting the watched (Haggerty & Samatas, 2010). However, in a draconian austerity regime such as the five-year austerity regime in Greece from 2010–2014, surveillance, as we'll see, is a coercive, neo-authoritarian mechanism that serves the ruling elite and the lenders' interests, actually punishing ordinary citizens and harming democracy.

In fact, "austerity surveillance" (AS) is a special kind of coercive surveillance, which has been used by the extreme austerity regime in Greece in the name of fighting tax evasion and corruption, while targeting the middle and lower economic strata—not the rich upper classes—is based mainly on "coveillance," i.e., citizen-informers' grassing, public naming, and shaming. It involves potential or actual coercion, stigmatization, and punishment as a domination and disciplinary control mechanism of the entire population; it functions in a neoliberal and post-democratic setting, namely without accountability and democratic control. "Austerity surveillance" is not just a financial or credit surveillance, collecting and processing data on financial behavior; it is a surveillance promoted by the austerity regime as a way of citizens' lives (Gilliom & Monahan, 2013, pp. 34-38), suspecting and targeting every one as untrustworthy, a potential cheater, a tax evader, and corrupted. AS is not an original type of monitoring, since its mechanics have been dictated by the Troika and are imported from countries such as the UK, with an embedded "coveillance" culture of neighborhood watch (NW) and "citizens watching citizens" (CWC) (Rowlands, 2013; Webster & Leleux, 2014).

2.1. The Basic Features of Greek Austerity Surveillance

Austerity surveillance, as it has been developed during the years of crisis in Greece, reflects all features of the Greek austerity regime; it is basically coercive, neoliberal, post-democratic, and class-oriented.

2.1.1. AS Is Coercive, Causing Stigmatization and Punishment

Christian Fuchs (2012, p. 685) has underlined the coercive features of surveillance in the capitalist context, which resemble with the coercive character of AS in Greece:

> [Surveillance] is the collection of data on individuals or groups to control and discipline their behaviour. It can be exercised through threats of targeting someone by violence....Surveillance operates with threats and fear; it is a form of psychological and structural violence that can turn into physical violence. Surveillance is a specific kind of information gathering, storage, processing and assessment, and its use involves potential or actual harm, coercion, violence, asymmetric power relations, control, manipulation, domination and disciplinary power. It is an instrument and a means for trying to derive and accumulate benefits for certain groups or individuals at the expense of other groups or individuals.

AS implies actual violence, like arrest and imprisonment, and symbolic violence, such as public naming and shaming, as we analyze it further below. There have been numerous arrests and imprisonments of tax and loan debtors, after citizens' accusations and "snitching."

We can also use Lazzarato's (2012) analysis of the function of debt equally for the "debt or austerity surveillance" as "a technique of domination, as a technology of power, combining financial management with control over subjectivity."

2.1.2. AS Is a Neoliberal Control Mechanism Especially Targeting Public Servants and Welfare Recipients

The Greek austerity regime, under the Troika's tutelage and direct supervision, has enforced a neoliberal policy of defaming everything relating to the state and public sector; neoliberalism is a market rationality that colonizes most spheres of public life, "pushing responsibility onto individuals for what used to be the purview of the state, effectively depoliticizing social problems and normalizing social inequalities…The convergence of surveillance and neoliberalism supports the production of insecurity subjects, of people who perceive the inherent dangerousness of others and take actions to minimize exposure to them, even when the danger is spurious" (Monahan, 2010, pp. 2, 11).

2.1.3. AS Is Working Under a "Post-Democratic Setting"

Post-democratic is, according to Crouch (2004, p. 6):

> one that continues to have and to use all the institutions of democracy, but in which they increasingly become a formal shell....Elections and electoral debate, which can still change governments, are transformed into a "tightly controlled spectacle," managed by professional experts and restricted to a set of issues selected by them, with most citizens reduced to a passive, apathetic role.

All these post-democratic features have characterized the five years (2010–2014) of the Greek austerity regime. In this setting, AS is actually antidemocratic because it is functioning without any democratic control and accountability, violating privacy, human rights, and constitutional freedoms.

2.1.4. AS Is Class-Oriented, Against the Lower Social Strata, Protecting the Rich Dominant Classes

As we prove later, AS, like the austerity regime, is overtly class-discriminatory against the lower middle classes, the poor, and the needy, and conspicuously in favor of the elite and rich upper strata.

In brief, "austerity surveillance" in Greece is a coercive or neo-authoritarian type of surveillance, using stigmatization by naming and shaming, encouraging citizen informants, besides the advanced surveillance technologies. It is targeting every citizen as a "debtor," owing his own share of debt, and as a potential tax evader, accountable and guilty before the austerity regime. With neoliberal fierceness, it firstly attacks the public sector servants and functionaries, all welfare recipients, and then private sector professionals. "At the end of the day, a 'pound of flesh' is demanded from all—with the normal exclusion of the politico-economic elite of the super-rich" (Stavrakakis, 2013).

3. The Basic Mechanics and Functions of the AS in Greece

The following are a wide and interesting range of examples, illustrating the aforementioned mechanics and functions of austerity surveillance in Greece.

3.1. "Coveillance": Grassing, Naming, and Shaming for the Austerity Regime by Citizen Informants

The austerity regime cultivates "coveillance," a kind of horizontal surveillance by citizens who have the "duty to inform" on their fellow citizens; it is an "outsourcing" of state institutional control and surveillance responsibility to the Greek public, as it is practiced in several countries, especially in the UK.[3] So, for example, in Scotland, the "Made from Crime" initiative encourages people "to eye one another suspiciously," and to monitor each other's living arrangements: "How can he afford that flash car? How did she pay for all those designer clothes? How can they fund so many foreign holidays?" Citizens' reports can be made by post, online, or by phoning, anonymously, with no evidential requirements or limit to the frequency and number of accused people.[4]

[3] In recent years, a plethora of UK government publicity campaigns have urged the public to report those who exhibit suspicious behavior in relation to a wide range of offenses, including terrorism, benefit fraud, social housing violations, bad driving, and even the improper use of rubbish bins" (Rowlands, 2013).

[4] Indicative enough is the British government's scheme in November 2009 that would pay £500 to the first 1,000 people whose telephone tip-offs led to a council house being repossessed (Rowlands, 2013).

3.1.1. Hotlines

Similarly, we also have in Greece, under the austerity regime, anonymous tip-offs, which can be made by post, online, or by phoning the following hotlines:

- 1517, the most popular and busiest hotline, for accusations to the Greek Financial and Economic Crime Squad (SDOE);
- 11012 for the Economic Police, who receives 50 calls per day;
- 10190 for corruption cases to the International Transparency of Greece; it received 500 calls in 2013;
- 1142 for the Health line against smoking in public places and other health issues, which received 20,000 calls against smokers in the first days of its establishment in 2010, but it receives less and less calls because the antismoking campaign has failed and no sanctions are imposed.
- 2313-325.501 in Northern Greece for accusations on environmental pollution, receiving 40-50 calls per day in the wintertime, when people burn unsuitable materials in their fireplaces to keep warm.

Reports can be made anonymously and with no evidential requirements. There are many instances of people claiming to have endured financial hardship and lengthy legal battles due to spurious allegations made by vindictive neighbors, relatives, divorcees, rivals, etc.

According to journalist sources: the SDOE hotline 1517, which was established in 2008 for tax evasion, had received 4,000 telephone calls in 2008 and 4,500 in 2009, and since a 2010 media campaign there has been a significant increase, having received 18,500 accusations of all forms, and 19,500 in 2011, while in the following years of 2012–2014 these accusations have been doubled. It is estimated that starting in 2014, this hotline receives an average of 200 calls per day and close to 70,000 calls per year (Elafros, 2015; Margomenou, 2014). According to SDOE statistics, six out of ten calls are made by relatives; 20 percent are accusations against rivals in the same business, or come from employees who have been fired and who accuse their former employers of tax evasion. Indicative enough is the fact that the percentage of named accusations is increasing, allegedly by taxpayers accusing others of tax evasion. SDOE has admitted that it has successfully arrested some serious tax evaders thanks to informers.

Moreover, according to Law 3610/2007, "whoever has denounced a tax or customs offense to the authorities, and this denunciation has been confirmed and punished by the enforcement of a pecuniary fine, s/he is entitled an award equal to 1/10 percent of the collected fines."

3.1.2. Public Naming and Shaming

Citizens' grassing reports on their relatives, neighbors, and fellow citizens is supplemented by public naming and shaming policies organized by the austerity regime authorities and the media, as an integral practice of austerity surveillance.

According to Lilian Mitrou (2012, pp. 247-248):

> by "naming" we understand the disclosure, publication and dissemination of the identity of a person, who is convicted or suspected of crime or tax evasion….The [stigmatizing] publicity serves as a means to degrade, shame, reprimand, reproach, censure, control…the person identified as offender, raising sentiments of guilt and shame…."Shaming" is a social process of purposefully expressing disapproval and/or contempt…provoking embarrassment, discomfort, anger and fear.

Shaming through publicly naming suspects, accused, and convicted persons as tax evaders by the Greek media throughout the austerity years aims at public condemnation and hopes to create deterrence effects.

Greece had very good legislation on the protection of personal data, which has been gradually but seriously amended to facilitate organized crime prevention, antiterrorism, and austerity policies, including tax evasion. In 2007, there was an amendment of Law 2472/97 on the protection of personal data, allowing the publication of the names of persons involved in criminal charges or convictions. Yet, the naming and shaming policies that had been introduced into Greek legislation in 2008 became an obligation of tax authorities against tax evaders since 2011 (Mitrou, 2012).

3.1.3. Humiliation and Defamation: Tax Evaders Are Frequently Considered Equal to Sex Offenders and Pedophiles

The implementation of these naming and shaming policies by the Greek authorities and the media has actually put tax evaders on the same level as serious criminals, sex offenders, and pedophiles, assuming that their public naming will deter other tax offenders. In the Greek social context, especially in local communities, public naming and shaming are serious policies to implement punishment, because the offenders fear "the look in the eyes of his intimates, family, friends, and colleagues, who know about their behavior." The community participates in the punishment process by disgracing, degrading, and stigmatizing the offender, imposing restrictions to his freedom, chances, and choices (Mitrou, 2012, p. 251).

The most blatant public and online stigmatization, a privacy violation, forced DNA collection, and imprisonment, was in May 2012, when the Greek authorities arrested 17 allegedly HIV-positive women who worked illegally as prostitutes, accusing them of intentionally causing serious bodily harm. The photographs of 12 of the women were published by TV channels and together with their names were posted on the Greek Police's website, causing an outcry of human rights advocates who said it was unclear whether the women were aware they had HIV.[5]

3.1.4. The Stigmatization Role of the Major Mass Media

The print and electronic mass media play a crucial role in the efficiency of surveillance (Monahan, 2010); especially in the naming and shaming process, they have overdone this during the austerity years in Greece, reproducing over and over the austerity regime's propaganda that most public servants and professionals are corrupted and are mainly responsible for the crisis. In very few cases when there is a celebrity arrest for tax evasion, this is presented in a very reviling way by the electronic media, advertising the "efficiency" of the austerity regime. Anchor men and women of the major TV channels have made a career as "tele-prosecutors," competing in the daily news programs to report in a very sensational way individual tax evasions cases, while they keep silence for huge tax evasion and offshore deposits of some of their colleagues and their bosses, the Greek "oligarchs," the media barons and owners of the TV channels, who are also contractors of public works, and/or ship-owners, etc. and have not bothered to pay their taxes (Kontoyiorgis, 2013).

3.2. Class Orientation and the Hypocrisy of the Greek Financial Big Brother

The Finance ministry, under the supervision of the Troika and the head of the European Commission's Task Force for Greece, Mr. Horst Reichenbach, was trying to track down tax evaders by cross-matching consumption data, unable though to identify those who have offshore accounts and money in Switzerland and in other tax-free paradises. Thus, the finance Big Brother is based on grassing and citizen informants, and exhausts its capacity to catch "small fishes."

There was also a proposed online publicity of income data of all Greek taxpayers, after the law 3842/2010, article 8 paragraph 20, that has permitted a total economic transparency, to enhance tax payments versus tax evasion, but this has not yet implemented, because the Greek Data Protection Authority (DPA) has prohibited the online posting of income data (Opinion 1/2011), suggesting less intrusive measures.

The fact that the Greek state with its financial surveillance is unable to arrest the enormous tax evaders

[5] See http://www.huffingtonpost.com/2012/05/03/greece-prostitutes-hiv-arrests_n_1473864.html

of the economic elite is illustrated in several lists with names of those who have deposited large funds in Switzerland and other offshore accounts, avoiding the payment of taxes in Greece.

3.2.1. The "*Lagarde* List"

The odyssey of the notorious "*Lagarde* list" exemplifies the typically lax and hypocritical attitude of all Greek governments and especially of this austerity regime toward real, very rich tax offenders. This list is a spreadsheet containing over 2,000 names of possible Greek tax evaders with undeclared large deposits at Swiss HSBC bank's Geneva branch, part of thousands of such customers' names, allegedly stolen by Herve Falciani, a computer technician of the bank, who attempted to sell them to several governments. It is named after former French finance minister Christine Lagarde, who passed it on to the Greek government in October 2010 to help them tackle tax evasion. The list was hidden by Greek officials, and it became known two years later when it was published by investigative journalist Costas Vaxevanis (2012). Former finance minister George Papaconstantinou was found guilty by the Special Court of tampering the spreadsheet and erasing names of his relatives on this list. Furthermore, the subsequent finance minister Evangelos Venizelos had forgotten the CD in his office for long time. To date, despite the public outcry, very few names on this list have been audited.[6]

There is also another list, from the Bank of Greece, of 54,000 people, who during the time of economic crisis took a total of €22 billion out of the country, and which seems will take many years to be investigated.

Another indicative example of hypocritical financial policy is the fact that on March 12, 2012, the pro-austerity government under the non-elected premiership of Eurobanker Loukas Papademos passed article 19 in an irrelevant law 4056/2012 about cattle breeding (!), abolishing a previous law 3399/2005 which established the information exchange between Greece and Anguilla, an offshore paradise, covering up huge tax evasion of several well-known Greek entrepreneurs (Akritidou, 2012, p. 28).

3.2.2. The "*Tiresias*" Black and White Lists

Let's compare now the above lists of mostly wealthy tax evaders with the *Tiresias* black and white lists. "Tiresias SA" is a private interbank company, named after the mythological blind prophet Tiresias; it collects and holds information on the economic behavior of all businesses and bank customers in Greece.[7] Legalized by Law 3746/2009, every bank customer is recorded and every payment delay of over 20 euros (!) is blacklisted for at least 5 years, regardless if this payment has been finally made. Hence, thousands of firms and individuals are blacklisted, stigmatized, and excluded by the Greek banking system, even for very small amounts of unpaid bills. There is also a *Tiresias* "white list" for all those bank customers with good credit, or those who have only once delayed a payment, or for those who are considered precarious for the future. Direct access to the *Tiresias* black and white lists is possible for everyone who pays a small fee, and the service is called a "check." *Tiresias*' lists' data are used by mushrooming private firms, which collect unpaid dues, exercising daily telephone bullying to debtors, pressing them to pay.[8]

Our comparison of the preferential treatment of the very wealthy tax evaders of the *Lagarde* list *vis a vis* the *Tiresias* black list, which names mostly petty entrepreneurs for bad credit, or thousands of defaulters who are unable to pay their commercial or house loans, elucidates the class discrimination of the Greek austerity regime and its expedient class-oriented surveillance.

3.3. Some Interesting Personal Testimonies

We now recount some personal testimonies from individuals experiencing austerity surveillance in Greece. As we have done with our research on anticommunist surveillance, where we had used in-depth conversational analysis (Samatas, 2004, 2005), we also analyze austerity surveillance here through "exploratory discussions" with a number of selected individuals who have either been watchers or watched, discussing and listening to their narrative "stories." From our narrative interviews with AS subjects, we cite here some characteristic excerpts, like the IRISS (2014) methodology.

After a malicious anonymous accusation against our dentist, who is an active citizen in voluntary organizations in our town, the SDOE visited his office and his house and for three days, looking for any evidence, even through family relics, to substantiate the accused illegal wealth, which there was none of to be found. The dentist, who after that event suffered a heart attack, told us:

> My grandfather had narrated to me notorious stories during the Nazi occupation of Greece when "Greek" collaborators having covered their face with hoods were regularly nailing and pointing out

[6] See http://greece.greekreporter.com/2015/02/09/86-names-missing-from-lagarde-list

[7] See http://www.tiresias.gr

[8] See more at http://www.balkaneu.com/tiresias-information-system-purchase information/#sthash.BIGoWA3p.dpuf
In the UK the private company "HR Blacklist" collects and files data against activists, union members, etc., selling them to employers, who exclude them from the labor market (Akritidou, 2012).

> persons to the German army to be executed based on real or false accusations of resistance. Nowadays, dishonorable "*roufianoi*" (informers) are doing a similar task, out of envy and malice…

A relative of a merchant who committed suicide after his bank auction, eviction, and confiscation of his house has told us:

> Listen to me good! He did not kill himself; the bank killed him! The f. bank gave him no chance to postpone payments of his loan, to pay later; they had started a fast track process to get his house and throw him and his family [of 3 kids] out of it. Do you wonder why I'm so glad every time those who are called "anarchists," "hooded," or you name them burn the bank's ATM?

A woman collecting rubbish leftovers from an outdoor vegetable market:

> I'm looking everywhere, even in rubbish bins, for some food or for something valuable to be sold; I'm ashamed to do this, but what else can I do? We all had a good household, but now we have become beggars.

This poor woman and the plethora of garbage pickers who flourish during this age of austerity are still lucky enough, because we don't have yet in Greece the CCTV monitoring the rubbish bins as they do in many UK neighborhoods (Haggerty, 2012, p. 241).

An SDOE financial prosecutor has stated:

> We don't have enough personnel to check the skyrocketing number of phone calls snitching tax evasions. Most of these calls are made by relatives against relatives, wives against their former husbands, accusations about inheritance, agricultural land, even accusations when someone appeared with a new car in the neighborhood. In short, snitching is developing as a national sport during the crisis.[9]

4. Austerity Surveillance in Greece Is Supplemented by a Variety of State Electronic Surveillance: Phone Taps, Communications Interceptions, Internet Tracking, etc.

Phone taps, lawful with due process and unlawful by state agencies and private surveillants, have been significantly increased all over the world (Landau, 2010; Marx, 2002), and especially in Greece during the financial crisis under the austerity regime. This is an indication of the insecurity of the austerity regime and the inability of the pertinent data and communications protection authorities to control the galaxy of private interceptions and the personal data market. Therefore, we consider phone taps a significant supplementary mechanism of the austerity surveillance.

According to the Hellenic Authority for Communication Security and Privacy (ADAE), in 2012 state authorities' waivers of confidentiality for telephone conversations due to national security, that is without a due process to justify the reason, numbered 2,634, more than those waivers following the due process, which were 2,055. These figures show that within two years of the beginning of the crisis, the "lawful" telephone interceptions were ten times more.

According to ADAE, the Greek Police and the National Intelligence Service (EYP) had over 50,000 phones tapped in 2012. The mobile phone companies have reported security problems with their networks. Also, there are accusations by political parties that their headquarters' phones are tapped (Karanicas, 2015; Lambropoulos, 2012).

Further, in 2013 the request for authorities' waivers of confidentiality for telephone conversations, due to national security, were 4,141, double that of 2012, and more than all waivers during the pre-crisis period of 2005−2009, plus 2,700 phone taps for clearing serious crimes (see Table 1).[10]

Table 1. EYP's waivers of telephone conversations' privacy.

Year	For Serious Crimes	For National Security	Total
2005	144	55	199
2008	607	302	909
2010	2281	1169	3450
2011	1743	3472	5215
2012	2055	2634	4689
2013	2700	4141	6841

Source: This list is based on a combination of data from www.adae.gr and Efimeros (2014).

Social media are also targeted by the Greek Police and EYP; they have requested in the first six months of 2013 the personal data of 141 *Facebook* users; according to journalist sources, *Facebook* gave data for 66 of them.[11]

Another controversial case is the well-publicized "Cyber Crime Unit of the Greek Police," which has successfully averted lots incidents of suicide, cyber bulling, and has arrested pedophiles. However, the problem with this unit is that to fulfill its goals it continuously tracks the entire cyberspace, and to act efficiently and on time it cannot follow legal due process; this is a fact not admitted to by the Greek police.

[9] For similar statements, see www.tovima.gr/opinions/article/?aid=709572

[10] www.adae.gr and Efimeros (2014).

[11] www.in.gr (Aug. 28, 2013).

Moreover, the police surveillance has been intensive and coercive against citizens and activists, even toward school students and whole families participating in the anti-gold mining movement and protests, which have been taking place in the gold-mining area, Skouries, in northern Greece.

In addition, there is cell phone interception by the Greek authorities, as *Vodafone* has acknowledged. According to *The Guardian*'s list, based on the Vodafone report, "Law Enforcement Disclosure Report," published June 6, 2014, Vodafone in Greece in 2013 received from Greek agencies a total of 8,602 metadata and content requests through the corporate telecom system, a proportionately very high amount of government surveillance (Garside, 2014).

5. The Greek Austerity Regime Is Under Surveillance by the Troika and Allies

The implementation of the austerity memoranda implied a direct Troika supervision of the state financial ministries; e.g. the secretariat of fiscal revenues is considered an informal fiefdom of the Troika. There is a direct intervention by the special Task Force under Mr. Reichenbach, having in most ministries about 400 representatives (Kotzias, 2013, pp. 332-342). As it was also confirmed by Mr. Fotis Kouvelis, the former president of the "Democratic Left,", a party which was a member of the coalition government under the ND Antonis Samaras premiership, there are Greek informers within the state apparatus providing detailed data to the Troika's technocrats about all contentious issues. This Troika's inside information has given lenders an advantage in the negotiation with the Greek government.[12]

In addition to Troika's supervision, there is continuous surveillance of the Greek austerity regime by European and American allies.[13] According to the newspaper *Ta Nea* (Karanicas, 2014, pp. 1, 14-15), Greece is among the 196 countries that are currently being monitored by the German Federal Intelligence Service (BND) since April 2010. Based on relevant documents of a dispute between a German lawyer and BND, a Europarliament study, and a *Spiegel* magazine report, *Ta Nea* revealed that BND has been monitoring Greece through three telecommunication companies, OTEGlobe, Forthnet, and Cyprus' CYTA, which are currently cooperating with DE-CIX, the largest telecom provider in Germany (Karanicas, 2014).

[12] See http://www.capital.gr/story/2281975

[13] In June of 2013, Edward Snowden revealed documents showing how the American NSA is bugging its European allies, the EU headquarters, 38 embassies, and UN missions, including the Greek ones, using an extraordinary range of spying methods (MacAskill & Borger, 2013).

6. The Austerity Surveillance's Impact and Implications

6.1. Detrimental Personal and Social Impact

A decent society and a democratic liberal state should respect and protect citizens from humiliation and stigmatization. Shaming hurts the ethical and psychological integrity of a person, contrary to the human rights and the values of a state of justice. In contrast to Greek culture, which celebrates a good neighborhood with open doors, community solidarity, social cohesion, and harbors disgust toward police informers due to Greece's authoritarian past, the Greek austerity authorities encourage the public to report anyone they perceive to be living beyond their means, or suspected of benefit fraud, illegal wealth, corruption, etc.

However, the austerity surveillance by the public exposure of personal economic data and the encouraging of one citizen watching and reporting on another, is a very controversial policy supported by the state, which may imply related crimes, like extortion, blackmail, robberies, etc. Further, when honest taxpayers are urged by the state to report suspected neighbors of offending their tax obligations, this state admits its institutional failure and inability to check tax evasion. Citizens' grassing is constructing a society of informers, with social cohesion seriously eroded and where the privacy rights and liberties of the people next door are infringed upon. Public naming and shaming of a person accused of or convicted for a crime is degrading and humiliating, injuring social dignity and reputation, threatening relationships, social status, employment, and life chances (Mitrou, 2012, pp. 253-254). The accused, the arrestees, and the suspects of tax evasion, who are not yet convicted, should not be deprived of their rights.

Furthermore, the online naming and shaming implies a perpetual online stigmatization, undermining the right to oblivion, i.e. the right to forget and to be forgotten. As Mitrou (2012, p. 255) points out, "due to the Internet's perfect and perpetual memory it is becoming harder and harder for people to escape their past." Moreover, the efficiency of shaming publicity, aimed to humiliate and stigmatize the offenders, seems to be questionable and undermines the reintegration of the offender into society as it is very unlikely that shaming would lead extreme offenders to change behavior, it punishes and ostracizes even minor offenders such as tax evaders, pushing them into a permanent underclass.

This community stigmatization is one of the most serious latent factors of the dramatic increase of suicides, especially in the Greek countryside. According to a research study, due to the austerity measures there was a 35.7 percent increase in total suicides in Greece during 2011−2013 (Branas et. al., 2015).

Regarding the efficiency of citizens' grassing in the UK, only one in every six calls received by the organization "Crimestoppers" has provided genuine information on benefit fraud, and there was a meagre overall success rate of 1.32 percent (Rowlands, 2013). There is not yet an estimate of the success rate of these grassing reports in Greece. We should report here that when we discussed the issue of the aforementioned hotlines with an informal focus group of various people around us, most ignored the existence of these hotlines; only two out of 12 of them, a lawyer and a public servant, knew their function, but no one knew the exact numbers of a single hotline.

6.2. Rapid Decline of the Best Privacy Protection Record

The constitutional, legislative, and institutional protection of privacy in Greece, as well as civil society's resistance against the Olympic CCTV cameras (Samatas, 2007, 2008), were reflected in the results of an international survey. In fact**,** Greece was recognized in 2006 as the highest privacy protection-ranking country (!) by the Electronic Privacy Information Center (EPIC) and Privacy International (PI) global study on "Privacy & Human Rights Report surveys developments in 47 countries" (2006). However, the phone-tapping during and long after the Athens 2004 Olympics (Samatas, 2010, 2014), and the easy mobile phone and internet interceptions by authorities and private intruders, have resulted in Greece's low record (1) in the category of "communication interceptions" in this survey. Unfortunately, Greece ever since, especially during this last period, under the draconian austerity regime against society and democracy, has definitely lost its "champion" position in privacy and data protection, joining countries with a high record in violations in these issues. Especially the Greek record concerning the serious issue of "personal data breaches" was and still is far worse, due to the illegal commerce of personal data, which is a very profitable business in Greece (Samatas, 2004, pp. 128-130).[14]

6.3. AS Has Reinforced the Mutual Mistrust between the Greek State and its Citizens

Every legitimate "institutional surveillance" (Lianos, 2003) presupposes trust in the state's public and private institutions. This institutional trust has never really existed in Greece, especially during the austerity regime, which in the name of security and its fight against tax evasion violates privacy and personal data of all Greek citizens.

In sharp contrast to other Europeans, there is an embedded mistrust and lack of institutional confidence that Greek citizens have expressed even before the crisis for any state and police surveillance as well as any kind of data collection by the state authorities, even 40 years after the collapse of the military dictatorship in 1974 (Samatas, 2004). For example, according to the findings of the *Flash Eurobarometer* survey on data protection in the 27 EU member states, conducted in January 2008: while, in the eyes of most EU citizens (72 percent), the fight against international terrorism is an acceptable reason to restrict data protection rights, Greeks express the highest suspicion about any provisions that would allow authorities to relax data protection laws, even if this served to combat terrorism.

Furthermore, according to the *Special Eurobarometer* (European Commission, 2011) exploring the "Attitudes on Data Protection and Electronic Identity in the European Union," Greek respondents appeared to have the lowest level of trust in most institutions and corporations and the highest levels of concerns in most examined categories. In particular, 83 percent of them stated that the government asks for more and more personal information, which was the highest figure among all countries, while 77 percent consider the disclosing of personal information a serious issue. Also, regarding concerns about tracking via mobile phone or mobile Internet, Greeks had once again the highest concern (65 percent). Further, more than half of the Greek respondents appeared to be concerned that their behavior is being recorded in a public space (54 percent).

This traditional mistrust of Greeks of their state institutions, and especially of state surveillance, due to the country's authoritarian past, is a key issue in understanding the lack of any legitimacy of austerity surveillance in Greece.[15]

6.4. The AS Acts without Democratic Control and Accountability

"Austerity surveillance," as a basic control mechanism, which together with many other draconian austerity mechanisms and policies make up the austerity regime, create a coercive and insecure surveillance society

[14] The Greek DPA has lately punished (DPA decision 100/2014) two marketing companies (PANNER and AddOne) that have illegally collected personal data of almost all Greek taxpayers, smuggled from the Secretariat of Information Systems of the Finance Ministry (Giannarou, Souliotis, & Hadzinikolaou, 2013). For such *data aggregator* companies, selling personal profiles in the USA, and considered "the little-known overlords of the surveillance society," see Gilliom and Monahan (2013, p.43).

[15] In fact, most Greek citizens have expressed mistrust before the crisis of almost all political, governmental, and judicial institutions, the police, the church, mass media, etc., except for the President of the Republic, the Fire Department, and the National Weather Forecast (*Public Issue* survey 2008 at http://www.publicissue.gr/wp-content/uploads/2008/12/institutions_2.pdf).

without democratic control and accountability. This regime, which in the Greek case was based on a coalition government of the right-wing New Democracy (ND) party and the center-left PASOK party, reflects a "post-political" era of professionalized "governance" beyond left and right, and favors all those who accept the austerity propaganda that everyone in the public sector—not the power elite—is corrupt and responsible for the crisis. The most favorable type of citizens are "snitches," who eagerly consider it their duty to watch and snitch to the officials on others' misbehavior, trying to gain personal advantage (Haggerty, 2012, p. 237).

We can correlate security with austerity policies and agree with Huysmans (2014), who argues that democracy becomes "at stake" as security and austerity policies threaten to hollow out human rights, compromise privacy, and outflank rights to question, challenge, and scrutinize.

6.5. "Sousveillance" and Resistance

6.5.1. Sousveillance and Shaming against the Austerity Regime's Elite

One very resilient reaction against the austerity regime is "sousveillance," surveillance from below, conducted mainly by young users of social media against the pro-austerity government, MPs, journalists, Eurocrats, German leaders, etc. The electronic social media are full of such fierce, hateful defamation and mocking comments, frequently like a cyber bullying against all of the pro-austerity personas by anonymous or pseudonymous commentators. Even beyond the social media platforms, there has been frequent physical harassment of governmental ministers and MPs by indignant citizens in public spaces. However, the worst impact is an alarming increase of the far right, neofascist party of "Golden Dawn," which came in third in the elections of January 2015.

The coercive austerity regime and its AS have caused a variety of everyday resistance efforts in Greece by private individuals, activists, NGO's, opposition parties, etc. One extreme but explicit type of surveillance resistance is the following one.

6.5.2. Vandalism of Police CCTV Cameras

According to official police data, through the end of November 2006, 180 CCTV cameras and/or their electronic operations boxes had been burned by radical groups (*IOS*, 2007). Police CCTV vandalism has continued, and by the end of 2013, 60 percent of all police CCTV cameras in the Athens metropolitan area were not working because they were vandalized, and there are no repair funds. Further, since the riots of 2008 up to the present, police and bank CCTV cameras are widely vandalized in the Athens metropolitan area. Also, in January 2015, 27 police CCTV cameras in Athens were destroyed by sympathizers of prisoners accused of being terrorists. Therefore, the police often relies on footage from private CCTV cameras, which are mushrooming everywhere in Greece. Thus, we have an extensive surveillance "creep" (Lyon 2007, p. 52) of data to the police taken by the private CCTV cameras, which seems not to bother Greeks, as much as the police cameras do (Samatas, 2008, 2011).

7. Concluding Remarks: Assessment and Prospects

We have tried to elucidate here the features, functions, and impact of the "austerity surveillance" (AS) used by the extreme austerity regime in Greece. As we have sketched it, AS is a specific kind of coercive surveillance, based mainly on "coveillance," i.e., citizen informers' grassing, naming, and shaming, public stigmatization and punishment, as a domination and disciplinary control mechanism of the Greek population. It functions under the Troika's supervision in a post-democratic and neoliberal setting, violating human rights and shredding social cohesion. Moreover, AS has a class orientation against the lower economic classes, while covering up the elite. Its neoliberal, antidemocratic, and unjust nature deprives AS of any legitimacy and citizens' trust.

AS in current Greece is not an original type of surveillance; we observe some basic similarities of this type of AS with past anticommunist surveillance (Samatas, 2004); while the Greek anticommunist state and regime used an authoritarian repressive surveillance apparatus, targeting leftists, communists, sympathizers, and anti-regime opponents, and was far more repressive and exclusionary (Samatas, 2004), the austerity regime, and its AS, targets public employees, professional groups (e.g. medical doctors), and petty store owners as tax evaders, as well as the poor welfare recipients. AS also has similarities to antiterrorist surveillance in the USA (Goldstein, 2002; Lyon, 2003), and "marginalizing surveillance" of welfare recipients (Monahan, 2010, p. 10). In fact, as we have mentioned, several features of AS are imported from other advanced surveillance societies, such as that of the UK (Rowlands, 2013). All these surveillance types, including the totalitarian one like that of the Stasi in East Germany (Funder, 2003; Schmeidel, 2008), are cultivating and using citizens as spies.

We could agree that Greece is being used by the Troika as an austerity laboratory (Douzinas, 2013), using austerity surveillance to produce discipline and control for further potential use beyond the Greek case, in other over-indebted countries. However, the Greek austerity regime and its AS have failed; Greeks have rejected their victimization. The election victory of the anti-austerity government on January 25, 2015 and the "No" victory on the referendum of July 5,

2015, against the new austerity measures, illustrate that the austerity regime and austerity surveillance have failed to fulfill their basic mission to make Greek people fearful and disciplined, under an austerity straightjacket. Moreover, these draconian policies have contributed to their resistance and defiance, even if this puts Greece at risk of being kicked out of the Eurozone.

Although we do not have space to analyze them here, there are two basic reasons in our view that AS has failed like the anticommunist one has in the past. The first reason is the anti-surveillance culture in the country, due to the authoritarian past of Greece (Samatas, 2011); the second significant reason is the powerful Greek "bonding" social capital, that is, according to Daniel P. Aldrich (2012), the relationships a person has with family and friends, which make it also the strongest form of social capital. Therefore, we declare our disbelief of the efficiency of AS and on the magnitude of citizens' snitching and their results, despite the regime's propaganda.

Financial crimes and corruption (Lambropoulou, 2011) are real serious problems of the Greek state and society, rooted since the founding of the modern Greek state. Coercive austerity surveillance has not and cannot resolve these problems. Greece urgently needs an efficient state apparatus and a legitimate surveillance mechanism, trusted by citizens, one working with justice and accountability, respect for human and democratic rights, and without discrimination against the poor and needy.

Let's finish by interpreting the aforementioned *Panoptes* myth in this time of austerity, considering the new Greek anti-austerity government, which came to power on January 25, 2015, and the prime minister Alexis Tsipras as the Hermes who had the mandate of the Greek people (Zeus) to kill *Panoptes* (austerity surveillance) in order to liberate Io (Greece), displeasing Hera (the Eurozone and/or Chancellor Angela Merkel). For the time being, Hermes (Tsipras) has been defeated and humiliated by the Eurozone. Despite this fact, the Greek people have given him a second chance, winning the elections of September 20, 2015. It seems he has two choices now: either to buy time, trying a more feasible project and even a more useful one by softening the austerity measures for the lower classes and taming *Panoptes* with democratic control, targeting the real rich "big fishes" of tax evasion; and then there is also the realist option for Hermes (Tsipras) to ignore his initial mandate to kill *Panoptes* (and austerity) and simply become a populist manager, reproducing a kind of softer "leftist" austerity *Panoptes* control mechanism, satisfying the lenders and deceiving the Greek people. We'll see…

Acknowledgements

The author would like to acknowledge the inspiring effect for this article of Lilian Mitrou's article (2012) "Naming and shaming in Greece: Social control as law enforcement tool" in C. W. Webster, G. Galdon, N. Zurawski, K. Boersma, B. Sagvari, C. Backman, & C. Leleux (Eds.), *Living in surveillance societies: The state of surveillance* (pp. 247-258). UK: University of Stirling. Also, he thanks the three anonymous referees and the guest editors for their constructive comments.

Conflict of Interests

The author declares no conflict of interests.

References

Aldrich, D. P. (2012). *Building resilience: Social capital in post-disaster recovery*. Chicago: The University of Chicago Press.

Akritidou, R. (2012). Spies in the workplace. *Hotdoc*. 17, December, pp. 57-60.

Branas, C., Kastanaki, A. E., Michalodimitrakis, M., Tzougas, J., Kranioti, E. F., Theodorakis, P. N., Carr, B. G., & Wiebe, D. J. (2015). The impact of economic austerity and prosperity events on suicide in Greece: A 30-year interrupted time-series analysis. *BMJ Open*, 5(1). Retrieved from http://bmjopen.bmj.com/content/5/1/e005619

Chrysogonos, K. (2013). *The circumvention of the Constitution*. Athens: Livani.

Crouch, C. (2004). *Post-democracy*. Cambridge: Polity.

Douzinas, K. (2013). *Philosophy and resistance in the crisis: Greece and the future of Europe*. Cambridge: Polity.

Efimeros, K. (2014). Research for the unlawful phone taps [in Greek]. Retrieved from http://www.thepressproject.gr/article/71708/Ereuna-gia-tis-paranomes-parakolouthiseis

Elafros, Y. (2015, March 15). Tele-accusations as a sport: Over 40.000 the annual "snitches" for tax evaders [in Greek]. *Kathimerini*. Retrieved from http://www.kathimerini.gr/807457/article/epikairothta/ellada/spor-oi-thlekataggelies

Electronic Privacy Information Center (EPIC), & Privacy International (PI). (2006). *Leading surveillance societies in the EU and the world* (Feb. 11, 2006). Retrieved from http://www.privacyinternational.org/survey/phr2005/aboutphrtable.pdf

European Commission. (2011). *Attitudes on data protection and electronic identity in the European Union* (Special Eurobarometer 359). Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Fuchs, C. (2012). Political economy and surveillance theory. *Critical Sociology*, *39*(5), 671-687.

Funder, A. (2003). *Stasiland: True stories from behind the Berlin Wall*. London: Granta.

Garside, J. (2014, June 6). Vodafone reveals existence

of secret wires that allow state surveillance. *The Guardian*. Retrieved from http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance

Giannarou, L., Souliotis, Y., & Hadzinikolaou, P. (2013, January 24). Personal data a multimillion-euro business (pp. 21, 41). Retrieved from http://www.kathimerini.gr

Gilliom, J., & Monahan, T. (2013). *Supervision: An introduction to the surveillance society*. Chicago: The University of Chicago Press.

Goldstein, R. (2002, July 15). US Planning to recruit one in 24 Americans as Citizen Spies. *Sydney Morning Herald.* Retrieved from http://www.smh.com.au/articles/2002/07/14/1026185141232.html

Haggerty, K. (2012). Surveillance, crime and the police. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 236-243). Oxon, UK: Routledge.

Haggerty, K., & Samatas, M. (Eds.) (2010). *Surveillance and democracy*. Oxon, UK: Routledge.

Huysmans, J. (2014). *Security unbound: Enacting democratic limits*. London: Routledge.

IOS. (2007). Why are cameras burned? *Sunday Eleftherotypia.* January 7.

IRISS (Increasing Resilience in Surveillance Societies). (2014). *Deliverable D4.2: Conduct the observation/interviews. Doing privacy in everyday encounters with surveillance*. Retrieved from http://irissproject.eu/wp-content/uploads/2015/01/IRISS_DEL_4_2_Conduct_the_Observations_Interviews_2014_FINAL.pdf

Landau, S. (2010). *Surveillance or Security? The risks posed by new Wiretapping technologies*. Boston: MIT Press.

Karanicas, C. (2014, June 14). How Germany watches Greeks through the internet. *Ta Nea.* pp. 14-15.

Karanicas, C. (2015, January 20). Bugs on the political parties [in Greek]. *Ta Nea*. p. 21.

Kontoyiorgis, G. (2013). *The oligarchs*. Athens: Patakis.

Kotzias, N. (2013). *Greece: A debt colony* [in Greek]. Athens: Patakis.

Lambropoulou, E. (2011). Corruption. In L. Cheliotis & S. Xenakis (Eds), *Crime and punishment in contemporary Greece* (pp. 171-195) Bern: Peter Lang.

Lambropoulos, V. (2012, August 28). 50.000 citizens' phones are taped [in Greek]. *To Vima*.

Lazzarato, M. (2012). *The making of the indebted man*. New York: The MIT Press/Semiotext.

Lianos, M. (2003). Social control after Foucault. *Surveillance and Society*, *1*(3), 412-430. Retrieved from http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3348/3310

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

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

MacAskill, E., & Borger, J. (2013). New NSA leaks show how US is bugging its European allies. Retrieved from http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies

Margomenou, M. (2014, October 5). A town of 70.000 makes accusations against friends and relatives [in Greek]. *I Kathimerini*. p. 25.

Marx, G. T. (2002). What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance & Society*, *1*(1), 9-29.

Mitrou, L. (2012). Naming and shaming in Greece: Social control as law enforcement tool. In C. W. Webster, G. Galdon, N. Zurawski, K. Boersma, B. Sagvari, C. Backman, & C. Leleux (Eds.), *Living in surveillance societies: The state of surveillance* (pp. 247-258). UK: University of Stirling.

Monahan, T. (2010). *Surveillance in the time of insecurity*. New Brunswick, NJ: Rutgers University Press.

Rowlands, M. (2013). Grassing for austerity: A duty to inform? *Statewatch Journal*, *23*(2).

Samatas, M. (2004). *Surveillance in Greece: From anticommunist to consumer surveillance*. New York: Pella.

Samatas, M. (2005). Studying surveillance in Greece: Methodological and other problems related to an authoritarian surveillance culture. *Surveillance & Society*, *3*(2/3), 181-197.

Samatas, M. (2007). Security and surveillance in the Athens 2004 Olympics: Some lessons from a troubled story. *International Criminal Justice Review*, *17*(3), 220-238.

Samatas, M. (2008). From thought-control to traffic-control: CCTV politics of expansion and resistance in post-Olympics Greece. In M. Deflem & J. T. Ulmer (Eds.), *Surveillance and governance: Crime control and beyond* (pp.345-369). Bingley, UK: Emerald Group.

Samatas, M. (2010). The Greek Olympic phone tapping scandal: A defenseless state and a week democracy. In K. Haggerty & M. Samatas, (Eds.), *Surveillance and democracy* (pp. 213-230). Oxon, UK: Routledge.

Samatas, M. (2011). Surveillance, modernisation and controversy in contemporary Greece. In L. K. Cheliotis & S. Xenakis (Eds.), *Crime & punishment in contemporary Greece: International comparative perspectives* (pp. 421-442). Oxford, UK: Peter Lang.

Samatas, M. (2014). *The "super-panopticon" scandal of the Athens 2004 Olympics and its legacy*. New York: Pella.

Schaefer, A., & Streeck, W. (Eds.) (2013). *Politics in the age of austerity*. Cambridge: Polity.

Schmeidel, J. C. (2008). *Stasi*. London: Routledge.

Stavrakakis, Y. (2013). Post democracy. *Atlas of transformation.* Retrieved from http://monumentotransformation.org/atlas-of-transformation/html/p/postdemocracy/postdemocracy-yannis-stavrakakis.html

Stavrakakis, Y. (2014) Debt society: The power of morality and the immorality of power. *Chronos*. Retrieved from http://www.chronosmag.eu/index.php/y-stavrakakis-my-country-is-the-colony-of-a-larger-colony.html

Tsimitakis, M. (2012) Greece: A debt colony, shackled to its lenders. *Al Jazeera*. Retrieved from http://www.aljazeera.com/indepth/opinion%20/2012/12/20121219740297362221.html

Vaxevanis, C. (2012). All names in the Lagarde List. *HotDoc*, issue 13, October. Retrieved from http://hotdoc.gr/store/issues/issue-13

Webster, W., & Leleux, G. (2014). Engagement and security. In *IRISS*: *Increasing Resilience in Surveillance Societies* (D4.2: Conduct the observation/interviews) (pp. 152-169). Retrieved from http://irissproject.eu/wpcontent/uploads/2015/01/IRISS_DEL_4_2_Conduct_the_Observations_Interviews_2014_FINAL.pdf

About the Author

Dr. Minas Samatas

Minas Samatas is Professor of Political Sociology at the Sociology Department of the University of Crete, Greece. He has an M.A. and a Ph.D. in sociology from the New School for Social Research (New York), and is the author of *Surveillance in Greece: From anticommunist to consumer surveillance* (2004), and *The "super-panopticon" scandal of the Athens 2004 Olympics and its legacy* (2014), and co-editor with Kevin Haggerty of *Surveillance and democracy* (2010).

COGITATIO

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 3, Pages 81-90
Doi: 10.17645/mac.v3i3.305

Article

Interveillance: A New Culture of Recognition and Mediatization

André Jansson

Department of Geography, Media and Communication, Karlstad University, 651 88 Karlstad, Sweden;
E-Mail: andre.jansson@kau.se

Submitted: 30 April 2015 | In Revised Form: 7 July 2015 | Accepted: 23 July 2015 |
Published: 20 October 2015

Abstract
The everyday uses of networked media technologies, especially social media, have revolutionized the classical model of top-down surveillance. This article sketches the contours of an emerging culture of interveillance where non-hierarchical and non-systematic monitoring practices are part of everyday life. It also introduces a critical perspective on how the industrial logics of dominant social media, through which interveillance practices are normalized, resonate with social forces already at play in individualized societies. The argument is developed in three steps. Firstly, it is argued that the concept of interveillance is needed, and must be distinguished from surveillance, in order to critically assess the everyday mutual sharing and disclosure of private information (of many different kinds). Secondly, it is argued that the culture of interveillance responds to the social deficit of recognition that characterizes highly individualized societies. Finally, it is argued that the culture of interveillance constitutes a defining instance and even represents a new stage of the meta-process of mediatization. The dialectical nature of interveillance integrates *and* reinforces the overarching ambiguities of mediatization, whereby the opportunities for individuals and groups to achieve growing freedom and autonomy are paralleled by limitations and dependences vis-à-vis media.

Keywords
identity; interveillance; mediatization; recognition; social media; surveillance

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

1. Introduction

In the last decade we have seen the arrival of what might be considered a new stage in the history of mediatization. The parallel expansion of social media, mobile media devices and various lifestyle applications constitutes more than a technological shift. It also denotes a social and cultural shift through which more and more areas of social life become saturated with and dependent on processes of mediation. There are today mobile applications for almost any kind of lifestyle practice, through which activities can be measured, stored and shared. At first sight the growing tendency to monitor, quantify and comment on one's own life as well as those of others may seem like a media-invoked transformation following certain technologically enabled and commercially driven logics of social media industries (van Dijck & Poell, 2013). However, the emergence and significance of such logics should also be understood in relation to social forces that have long prevailed in modern society and can be traced to broader structural transformations, above all individualization.

In this mainly theoretical essay, the key idea that will be elaborated on is that we (that is, those of us who live in societies marked by digital media abundance) are immersed in a *culture of interveillance*. This perspective provides a way of capturing the social embeddedness of contemporary surveillance processes, typically governed by commercial forces, while at the same time recognizing the non-hierarchical and non-systematic nature of most social monitoring processes

occurring in everyday life. It is also a way of pointing out what is new about contemporary mediatization; how the industrial logics of dominant social media resonate with the everyday social characteristics of individualized modern society. Mediatization is basically understood as a historical meta-process whereby a variety of social realms, in organizational settings as well as everyday life, become increasingly adapted to and dependent upon media technologies and institutions (see, e.g., Couldry & Hepp, 2013; Krotz, 2007; Lundby, 2014).

Starting out from these fundamental assumptions, my aim is to explore three interconnected arguments, each constituting a separate section of the text. Firstly, it will be argued that the concept of interveillance is needed in order to critically assess the everyday mutual sharing and disclosure of private information (of many different kinds) that constitutes an increasing share of all media practices. The concept is needed not only for defining particular forms of mediated interaction, namely those forms marked by digital connectivity (van Dijck, 2012, 2013), but also more indirectly in order to preserve the conceptual specificity and critical potential of the term surveillance. In the first part of the essay the properties of interveillance will be discussed in relation to related concepts, notably lateral surveillance (Andrejevic, 2005) and social surveillance (Marwick, 2012).

Secondly, it will be argued that the culture of interveillance responds to the *social deficit of recognition* that characterizes highly individualized societies. Interveillance breeds in the soils of an other-directed social landscape that had already been diagnosed in the mid 20th century by sociologists like David Riesman (1950) and later by Giddens (1991) and Beck and Beck-Gernsheim (2002), amongst others. The second part of the essay will, through an engagement with Axel Honneth's (2012) theory of recognition, discuss the ways in which dominant forms of social media and accompanying representational spaces of interveillance largely reinforce this sense of lack, while at the same time circulating promises of mutual recognition and individual growth. This is to say that the culture of interveillance holds a dialectical character where striving for recognition coalesces with social simulations that bind individuals closer to technological and commercial structures of dependence.

Thirdly, by way of conclusion, it will be argued that the culture of interveillance constitutes a defining instance of contemporary mediatization. The dialectical nature of interveillance integrates *and* reinforces the overarching ambiguities of mediatization, whereby the opportunities for individuals and groups to achieve growing freedom and autonomy are paralleled by limitations and dependences vis-à-vis media. Interveillance constitutes an entry point for grasping how new forms of normalized media dependence are replacing and displacing pre-established patterns tied to the mass media era. Interveillance gives us an analytical tool for conducting critical analyses of how the dialectics of mediatization are played out and socially constructed at the level of everyday life.

This article should also make an epistemological contribution to the mediatization debate. Whereas mediatization research has been accused of being media-centric, that is, explaining social transformations too much in terms of media change (see Deacon & Stanyer, 2014), my analysis adheres to the broadly accepted view of mediatization as concerned with the *interplay* between media, culture and society (see, e.g., Hepp, 2013; Hepp, Hjarvard, & Lundby, 2015; Krotz, 2007). Through the concept of interveillance, which articulates the fundamental role of long-term social transformations like individualization in *conditioning media change*, the aim is to stress the continuously contested and socially moulded nature of mediatization (Jansson, forthcoming). In addition, the dialectical understanding of mediatization paves the way for rethinking mediatization as a research programme for *immanent critique*. Mediatization is at its strongest when it captures the inherent and continuously evolving social contradictions and ambivalences that mark out media saturated societies, notably in terms of liberating versus constraining forces. Accordingly, the dialectical perspective needs to move beyond and build bridges between the predominant social-constructivist and institutionalist frameworks (see Couldry & Hepp, 2013). In the more confined analysis of interveillance the combination of recognition theory (Honneth, 2012) and theorizations of emerging "social media logics" (van Dijck & Poell, 2013) constitutes one such bridge.

2. Interveillance and the Social Relocation of Media

One thing that distinguishes our contemporary media landscape from what it looked like just one or two decades ago is the *social location* of media. In addition to their traditional position between people and various organizational entities (including media institutions) that characterized the mass media landscape (see Hjarvard, 2013, pp. 23-27), media technologies are now to a greater extent located *between people*. This is not to say that interpersonal media are all new; telephony and the postal system have been crucial to the history of modernity. Nor is it to say that today's networked media, enabling various forms of many-to-many communication, have replaced mass media; rather these forms co-exist and interact in various ways, giving rise to increasingly complex media landscapes. If we are to understand the consequences of mediatization at the level of social life, that is, how various lifestyle sectors (Giddens, 1991) are successively made dependent on and adapted to certain technologies and institutions of mediation (Jansson, 2013), we must account for this multi-layeredness while at the same time disentangling what is succinctly new about the current situation.

A relevant framework for identifying the novelty of our networked media landscape is suggested by van Dijck and Poell (2013), who introduce four elements of what they call "social media logic": *programmability*, *popularity*, *connectivity* and *datafication*. Whereas the whole idea of any coherent "media logic(s)" should be treated with great caution, it is fair to argue that there exist processes at *the industrial level* of media circulation that are built into the very techno-economic architecture. As Hepp (2013, p. 46) points out in a critique of media logic(s), "in the functionalities of media logic we no longer see the acting subjects, the meaningfulness of their action, as well as all the other problems of power in communication". This is important. In adopting van Dijck and Poell's (2013) notion of social media logics it should not be inferred that mediatization follows any clear-cut *social* logic(s), but that there are certain industrial mechanisms that follow calculated orders, notably algorithms, for profit maximisation. These mechanisms respond to and reinforce the social behaviour of media users, and can be located in a particular area of the digital media landscape, which may be called *dominant social media*. Such media may take the form of websites or mobile applications and involve social networking sites (e.g., Facebook, LinkedIn), video sharing sites (e.g., YouTube), blogs and microblogs (e.g., Twitter, Weibo), as well as social media extensions of various lifestyle applications (e.g., RunKeeper, Nike+). What they have in common is that they turn "platformed sociality" (van Dijck, 2013, p. 4) into economic value through the development and implementation of industrial logics (see also Gillespie, 2010; Striphas, 2015).

This is not the place for going deeper into each of the four elements suggested by van Dijck and Poell (2013). Instead, two general points will be advanced, related foremost to popularity and connectivity that are particularly important for describing how industrial logics play into the on-going social relocation of media, which will also lead us further to the question of interveillance. Firstly, van Dijck and Poell (2013, pp. 6-7) stress that the implementation of various measurements of *popularity*, such as the Like-mechanism, constitutes the extension of economic drivers that were already at place in commercial mass media settings in the shape of, for instance, top lists and ratings. The difference today is that individual media users may also take part in this competition for popularity, where the automated generation of friend stats on Facebook and follower counts on Twitter becomes, for instance, a means of expressing social integration and success. At the same time, media users are turned into (unpaid) "prosumers" of media content and the social media industry is given raw material for generating economic turnover through advertising sales (see also Fuchs, 2014, Ch. 5).

Secondly, van Dijck and Poell (2013, pp. 8-9) introduce a crucial distinction between *connectivity* and *connectedness*. Whereas connectedness is all about the meaningful social connections between individuals and groups—which social media promote and which various media have enhanced and extended in different ways since their very origin—connectivity refers to "the socio-technological affordance of networked platforms to connect content to user activities and advertisers" (van Dijck & Poell, 2013, p. 8). This means that the social practices that these platforms mediate are actually not as free and open-ended as one might think, but partly governed and exploited via the algorithms of the techno-economic architecture (see also Striphas, 2015). In everyday life the distinction between connectivity and connectedness becomes difficult to identify since, for instance, many close relations may also be exploited and reproduced via automated connective processes, and vice versa. The important point is precisely this accentuated fuzziness between connectedness and connectivity—the fact that social relations are to a certain extent *premediated* and *simulated* through automated patterns of connectivity. These concepts will be further explored below.

Accordingly, the elements of popularity and connectivity reinforce one another; connectivity operates as a support for reaching the goal of popularity. In more straightforward terms, this development can be described as an escalating commoditization of social life, which today expands beyond the confines of particular groups and particular forms of communication (see, e.g., Fuchs, 2014, Ch. 5). In transmedia environments, where information flows smoothly between different platforms and devices, almost any kind of everyday practice can be measured, recorded and circulated/shared, and thus commoditized, as information either through embedded social functionalities of applications such as RunKeeper, or through external sharing via, for example, Facebook or Instagram. The industrial logics of social media stimulate their users/prosumers to think of their peers, whether close friends or more distant acquaintances, as audiences of their own lifestyle performances (see Marwick, 2013; Marwick & boyd, 2011; Turkle, 2011). In this way, dominant social media are part of gradually normalizing new forms of reflexivity and new ways of relating to the social world. As we will see, however, the identification of "social media logics" at the industrial level should not lead us to adopt a media-centric view of social transformations.

Surveillance is part and parcel of these alterations. Whilst mass media institutions have long conducted or consulted various kinds of audience research in order to increase the popularity of media products and sell audience segments to advertisers, digital media platforms enable datafication and automated, or interactive, surveillance (see Andrejevic, 2007). Datafication implies that media industries as well as other commer-

cial actors are able to retrieve advanced profiles of the market and automatically target their advertising, even on a real-time basis, through instantaneous analysis of user generated data streams (Striphas, 2015; Trottier, 2011; Trottier & Lyon, 2012). Digital transmedia technologies thus revolutionize the classical model of top-down surveillance, defined as the systematic collation and analysis of information in order to exercise power over a certain population or territory (see, e.g., Giddens, 1987, pp. 14-15; Lyon, 2007, p. 14). Furthermore, several researchers have pointed out that surveillance expands beyond administrative settings (economy and state) and in various ways has come to saturate social life in the form of peer-to-peer monitoring (e.g., Andrejevic, 2005). This tendency should be seen in light of the aforementioned relocation process, through which individuals and groups start relating to themselves more and more as manageable symbolic entities, even brands (see Marwick, 2013).

These diagnoses of technologically- and industrially-driven social change should certainly inform a critical view of mediatization. However, they suffer from a recurring dilemma when it comes to conceptual stringency. When applying the term surveillance to the analysis and understanding of more horizontal processes of information gathering and disclosure one runs the risk of misnaming and simplifying aspects of social life that are dense with social and cultural ambivalences. For instance, the concept of lateral surveillance, introduced by Andrejevic (2005), refers to "peer-to-peer monitoring, understood as the use of surveillance tools by individuals, rather than by agents of institutions, public or private, to keep track of one another" (Andrejevic, 2005, p. 488). The basic argument is that the expanding availability of new online technologies has also fostered a socio-cultural climate where people get accustomed to checking up on others in order to avoid risk, for example in relation to new romantic interests. Whereas Andrejevic points to a significant new area of communicational practice, it is difficult to distinguish to what extent and in which particular cases this type of peer-to-peer monitoring falls under the original definition of surveillance. The kinds of "check-ups" that Andrejevic discusses are often far from systematic and may be more acquainted with everyday social phenomena driven by affection and curiosity, even a desire for knowledge. They also, literally, contradict the hierarchical relations that originally used to define surveillance. Albrechtslund (2008), who proposes the concept of participatory surveillance for analyzing similar monitoring practices, even sees this as a potential source of social empowerment among "ordinary" or disadvantaged groups of people—a conclusion that contradicts Andrejevic's more critical view.

Similarly, Marwick's (2012) notion of social surveillance, which refers to the social media practices of "closely examining content created by others and looking at one's own content through other people's eyes" (Marwick, 2012, p. 378), problematizes the power dynamics associated with surveillance. Her point is that even though social surveillance is marked by reciprocity—that is, when people give away information they expect to get something back—it can still be framed by the notion of surveillance, because it leads to self-management among social media users through the "internalization of the surveilled gaze" (Marwick, 2012, p. 381). Even sharing Marwick's understanding of how social surveillance is entangled with everyday power relations, informed by Foucault's (1977) notion of capillaries of power, two main problems may be detected. Firstly, much empirical research shows that the kinds of practices that Marwick highlights are not often systematically undertaken, but rather occur within the realm of more or less floating everyday routines (see, e.g., Christensen, 2014; Humphreys, 2011; Jansson, 2014a). When self-monitoring practices escalate into well thought out strategies for improving one's reputation or performance, such as among amateur bloggers and in certain media related professions or among adherents of the Quantified Self movement, one might probably speak of systematic procedures, and thus surveillance in the stricter sense. But these groups constitute quite exceptional cases and thus contradict Marwick's depiction of social surveillance as a widespread phenomenon related to social media in general.

Secondly, when speaking of the internalization of the surveilled gaze, what Marwick outlines is largely a technologically driven cultivation process, akin to Andrejevic's thoughts on how the spread of new surveillance tools instils new forms of behaviour among ordinary people. Also if we would agree on the idea that monitoring practices enabled by dominant social media are to be seen as a particular kind of surveillance we should be cautious about placing all social media use under the same rubric. Whereas the industrial logics of social media, and the elements of connectivity and popularity in particular, may sustain a drive towards more open-ended forms bonding, as identified already in Wittel's (2001) analyses of network sociality, studies also show that social media (just like other technologies) are appropriated in culturally specific ways (e.g., Christensen, 2014; Jansson, 2014a).

We thus need a concept that allows for complex analyses of the social processes related to mediated monitoring and control—without emptying out the original meaning and critical potential of the term surveillance. What may be termed interveillance resembles closely the phenomena outlined by Andrejevic, Albrechtslund and Marwick.[1] Interveillance includes the

[1] Another concept that has been juxtaposed with surveillance is sousveillance, coined by artist Steve Mann. However, sousveillance should be seen as a deliberate reaction to surveillance processes, involving highly reflexive and technologically

kinds of everyday check-ups that Andrejevic discusses, as well as Albrechtslund's more expressively oriented practices and the anticipation of other people's mediated gazes. Interveillance also includes the normalization of horizontal networking practices that Marwick refers to. Interveillance means that social agents to a growing extent come to understand and define the relations between themselves and others via automatically generated recommendations of contacts and commodities (connectivity) and quantified simulations of social status (popularity). Interveillance practices are thus inseparable from societal surveillance processes, foremost algorithmically based commercial surveillance (datafication), but they are not systematic and hierarchical *per se*. Rather, they are driven by the fundamental social needs through which identities are (re)created and manifested, and thus take on a relatively non-reflexive and volatile character (see Table 1).

Table 1. Analytical distinctions between surveillance and interveillance.

	Surveillance	*Interveillance*
Driving force	Control of people and spaces	Identity development
Mode of practice	Systematic procedures	Everyday routines
Power relation	Hierarchical, formal	Multi-layered, informal
Direction of flows	Mainly one-way, vertical	Mainly two-way, horizontal

Furthermore, to the extent that interveillance practices become part of everyday life, they do not look the same and do not involve the same media in all social groups and in all walks of life. This means that if we want to grasp the culture of interveillance as a broader and socially complex transformation we have to combine media-centric models of altered "media logics", understood as industrial modes of accumulation as discussed above, with historically contextualized understandings of socio-cultural structures and their transformation. In the following section attention will turn to Honneth's (2012) theory of recognition in order to outline a critical perspective through which the social nature and historical development of interveillance can be further explicated and problematized. Through this elaboration a more general account will be developed of mediatization as a dialectical process that integrates interveillance as a key feature and increasingly prominent social force behind the current escalation of everyday media dependence.

advanced political actions and artistic interventions that aim to strengthen the power and communion of "ordinary citizens". While partly related, the concept covers a different set of practices and different social dynamics than the horizontal forms of everyday monitoring discussed here.

3. Interveillance and Simulated Recognition

First of all we must specify what recognition means and why it has become a critical issue in modern society. Honneth (2012), who takes his key from psychoanalytical theory, sees recognition as a basic requirement for the individual to establish a sense of security in his or her capability of thinking, reflecting and acting independently of other individuals. Such a sense of autonomy cannot emerge without the positive attention from significant others, who contribute to both social integration and a sense of individual worth on behalf of the individual. The individual's desire to belong to groups is thus not merely a reflection of integrative forces, but should be understood as a quest for *autonomy through recognition*. One of the predicaments of Honneth's theory of recognition is that "groups should be understood, whatever their size or type, as a social mechanism that serves the interests or needs of the individual by helping him or her to achieve personal stability and growth" (Honneth, 2012, p. 203). However, the membership of groups gives no guarantee for recognition in the true sense of the word, since groups may also involve repressive tendencies that rather lead to conformism and the dissolution of autonomy.

In Honneth's positive definition of the term, recognition "should be understood as a genus comprising various forms of practical attitudes whose primary intention consists in a particular act of affirming another person or group" (Honneth, 2012, pp. 80-81). The concept thus contains three basic premises: recognition should be (1) positively affirmative, (2) actualized through concrete action (rather than just symbolical in nature), and (3) explicitly intended (rather than emerging as a social side effect or means for reaching other goals). It is also stated that the basic attitude of recognition can take the form of different "sub-species", notably love, legal respect and esteem. Against such pure stances of recognition Honneth poses ideological forms of recognition that rather exploit the individual's psychosocial needs in order to install attitudes that reproduce certain structures of domination. One example is the way in which societies of different epochs have endorsed certain attributes among certain groups (based on gender, sexuality, ethnicity, and so on) as part of the reproduction of hegemonic orders for the division of labour: "We could easily cite past examples that demonstrate just how often public displays of recognition merely serve to create and maintain an individual relation-to-self that is seamlessly integrated into a system based on the prevailing division of labour" (Honneth, 2012, p. 77). Such ideological forms of recognition are false, Honneth argues, because they fail to promote personal autonomy.

Recognition theory has so far gained very little attention within media studies, and vice versa.[2] In my view, Honneth's thinking around recognition lays the ground for a broader social critique of how the expansion of interveillance resonates with structural transformations. His analyses point especially to the negative consequences of an extended individualization process, including forces that under the auspices of supporting autonomy and recognition actually operate in the opposite direction. Whereas individualization in its positive fulfilment sets individuals free from oppressive structures and normalizes the pluralization of choice it also leads to a state of increased psychological anxiety and vulnerability among individuals, which in turn can be seen as "*one*, if not *the*, central motive behind group formation today" (Honneth, 2012, p. 207). Since modern society, as opposed to more traditional formations, does not provide one unified standard (such as religiously grounded ethics) in relation to which the individual may estimate the value of his or her achievements, it becomes increasingly important for the individual to achieve recognition within the peer group. Furthermore, media institutions, labour markets and a multitude of commercial and political actors promote individuals to actively work on their identities and learn how to present their personalities in ways that are as beneficial as possible for reaching certain goals in society or in their careers. Honneth (2004, 2012, Ch. 9) calls this *organized self-realization*, which implies that self-realization becomes ideologically normalized as a biographical goal. Genuinely dialogical processes of recognition are undermined and replaced by standardized patterns of identity-seeking and simulated forms of recognition that serve the goal of legitimizing and further integrating individuals into the capitalist system. Authenticity and autonomy transmute into their opposites, simulation and conformism, and individuals may ultimately find their lives devoid of meaning.

We can now discern the connection to interveillance. What Honneth outlines is a dialectical transformation whereby the individual quest for recognition and autonomy rather leads to the legitimation of and dependence on various technological and economic systems (see also, e.g., Beck & Beck-Gernsheim, 2002; Boltanski & Chiapello, 1999/2007; Giddens, 1991). Honneth does not pay much attention to media technologies and institutions, however. To the extent they are mentioned, they are taken as a compound institution, "electronic media" (Honneth, 2012, p. 162), that operates as a machinery for normalizing desirable formats of self-realization through for example advertising and popular fiction, which play the role of legitimizing certain ideological forms of recognition. This diagnosis resonates in interesting ways with Riesman's (1950/2001) account of how other-directedness spread as the dominant mode of social conformity in post-war America, involving reflexive forms of lifestyle management among the urban middle classes. The desire to achieve mutual recognition among peers was channelled through standardized consumption practices whose symbolic meanings were socially implanted via mass media.

The mass media system thus operates both as a map and a guidebook of the social terrain; a system that establishes and negotiates the codes through which patterns of interpersonal recognition (and misrecognition) evolve. This means that mass media not only mediate but also, and perhaps more significantly, *premediate* social expectations and experiences of individual actors (Grusin, 2010), turning the process of (mass) mediation *per se* into a force of symbolic legitimation. What (and who) is mediated is what counts as important. As Couldry (2003) suggests, the symbolic power of media (taken in the broad, institutional sense) rests on a dominant mythology that constructs *the* media as an institution that circulates symbolic material possessing exceptional social, cultural, economic and/or political significance. This mythology functions as a stabilizing factor in relation to the social anxieties articulated through organized self-realization, and legitimizes people's ritualized dependence on mass media as a *structure of premediated recognition*.

Today we must rethink these relations. The widespread usage of social media, mobile devices and numerous transmedia applications has in recent years come to play into the social functions of mass media, both challenging and extending them. A growing share of media users, especially younger groups, orient their media habits towards interactive platforms, such as Facebook and YouTube, that circulate user-generated flows as well as content emanating from mass media industries.[3] As Gillespie (2010, p. 347) argues, these platforms have become the "curators of public discourse". They both enable and demand continuous monitoring and updating, and thus feed off precisely

[2] On the whole, recognition theory attains a strong political and social philosophical bias. In a recent volume entitled *Recognition Theory as Social Research* (O'Neill & Smith, 2012), in spite of the broad scope of the book, none of the eleven chapters addresses the pervasive role of media for shaping contemporary relations of recognition. In media and communication studies the work by Nancy Fraser (e.g., 2000, 2001) has gained substantial attention among scholars studying for instance the politics of identity and migration. The most significant work that has brought together questions of recognition and mediation is Boltanski's (1996/1999) book *Distant Suffering*. This work deals chiefly with spectatorship, however, and is linked to questions of pity and self-justification in the age of mass mediated humanitarian spectacles.

[3] In Sweden, for instance, one of the leading countries in this development, more than 50 per cent of young Internet users (ages 12–18 years) use YouTube every day and more than 50 per cent of Internet users between 20 and 45 years old use YouTube every week (Findahl, 2014).

those psychosocial needs and desires that characterize other-directed life environments, while at the same time extending the pre-established mythology of institutionalized mediation as a marker of socio-cultural status. Accordingly, dominant social media build their success upon the promises of providing solutions to recognition deficit, but contribute at the same time to the reinforcement of interveillance culture through the circulation of *simulated forms of recognition*, which now exist alongside various premediated forms.

This is *not* to say that all forms of interaction that occur via dominant social media resonate with the industrially invoked logics of popularity scores and simulations of connectedness, or that all forms of recognition on these platforms are of an ideological nature. It is *not* to say that connective practices, such as liking, commenting and (geo)tagging, are always to be seen as mere expressions of interveillance and cannot be part of deeper relations of recognition, such as love, friendship or identity politics, or make up community maintaining flows of phatic communication (see, e.g., Ling, 2008; Miller, 2008). However, the architecture of dominant social media and the interfaces through which interveillance unfolds sustain open-ended processes of simulation where the distinction between connectivity and connectedness is collapsed (van Dijck, 2013). For instance, whereas algorithmic systems keep track of how many connections (friends, followers, etc.) different users have and how many confirmative acts certain posts generate, these functionalities contradict the dialogical aspects that mark pure forms of recognition and make it possible for each actor to hermeneutically assess and build trust in the intentionality and practical relevance of other communicators' symbolic acts (cf. Striphas, 2015). On the contrary, social media relations are typically marked by *uncertainty* as to what intentions and what level of involvement may hide behind the digital interface, that is, what is "actually" going on.

This mediated social uncertainty, which can be identified in areas as diverse as political action (e.g., related to microblogging) and intimate relations (e.g., dating sites), is exactly what characterizes and reinforces the culture of interveillance. In interveillance there is never any affirmative dialogue. In interveillance, recognition is continuously at stake, but never achieved.

In this section, an explanation has been provided of how the expanding industrial logics of social media interact with long-term social transformations of individualized societies. The overarching point is that dominant social media contribute to the normalization of simulated forms of recognition, which establishes interveillance as a ritualized part of everyday life and makes certain media devices and applications ritually indispensable to social life. At the same time, however, we should embrace the fact that the overall consequences of interveillance are ambiguous and take on different (often contradictory) appearances in different contexts. We should also take into account that interveillance is intertwined with and inseparable from deeper forms of mutual recognition and emancipatory forms of communication that take place between peers through a variety of media (e.g., Caughlin & Sharabi, 2013; Jiang & Hancock, 2013; Linke, 2011).

When raising critical questions concerning the social and existential costs of our connected lives we should thus move beyond simplified views of social fragmentation and media power. Rather, the type of social and cultural critique that should be considered is of an *immanent* nature (see, e.g., Fornäs, 2013). The purpose of immanent critique is precisely to grasp the contradictions and ambiguities that characterize social transformations on both individual and structural levels, and explore how these levels are interrelated. In the following section I will discuss the ways in which the culture of interveillance may signify a new stage within the broader dialectical meta-process of mediatization.

4. Interveillance and the Dialectics of Mediatization

Two main points have so far been advanced. Firstly, it has been described how interveillance is related to the social relocation of media, including the growing prominence of dominant social media, and argued that we need to maintain analytical distinctions between interveillance and surveillance (Table 1). Secondly, it has been argued that the emerging culture of interveillance, and its variations, can only be sufficiently understood if we account for how the industrial logics of social media resonate with social forces already at play in individualized societies, above all the increasingly open-ended quest for recognition. This is where we find the fundamental energy that drives and entertains the commercial machineries of dominant social media, which in turn occupy an increasingly significant role in normalizing partly new ways of defining social relations and senses of self (notably in terms of connectivity and popularity). *The culture of interveillance thus arises through the mutual operation of social and techno-economic forces. It denotes a cultural condition where identity creation is saturated with monitoring practices based on simulations of connectedness and recognition, thus reproducing the ambiguities of recognition they were intended to stabilize.*

What follows from this is my third and concluding point; the culture of interveillance both integrates and reinforces the dialectics of mediatization. The term mediatization refers to something more than just the general development and appropriation of *more* media within *more* areas of social life. While such quantitative elements are indeed part and parcel of the mediatization meta-process, as Hepp (2013) points out, we can only estimate the real force of mediatization once we are able to detect substantial social and cultural trans-

formations tied to the establishment of new media technologies as *cultural forms* (Williams, 1974; see also Hjarvard & Nybro Petersen, 2013). When this happens, as it did with radio and television during the broadcasting era, media are experienced as more or less indispensable and social life becomes difficult to manage, and indeed to imagine, without them. During a long period of the 20th century, and still today, modern life was spatially and temporally ordered in relation to the material and cultural properties of these media (see, e.g., Scannell, 1996; Spigel, 1992). While broadcasting, taken as one institution, enabled new forms of social extension and functioned as a (pre)mediator of recognition, as discussed above, it also established (more or less context specific) dependencies vis-à-vis certain flows of information and certain technologies.

In a similar manner, the culture of interveillance encompasses the normalization of a new set of everyday media routines and the taken-for-grantedness of certain media ensembles—such as, smartphones, tablets, Wi-Fi networks and social media accounts. Interveillance practices, as we have seen, are thoroughly interwoven with other kinds of everyday practices and are rarely systematic or strategic in nature. They come to surface as "something one just does", while on the move or while waiting, during free time or while pursuing other routines. They are also interwoven with other online activities (news gathering, shopping, gaming, and so forth), which together contribute to the social construction of media as *indispensable things* (Jansson, 2014b). There are several empirical studies showing that a life without mobile media devices and various social media applications would be more or less unthinkable to many social groups today and that people even develop counter-routines in order to cope with their experiences of being increasingly "addicted" to keeping an eye on various information flows and updates, responses to things they have posted online and the fluctuations of social media scores (e.g., Bengtsson, 2015; Hall & Baym, 2012; Paasonen, 2014).

Dependencies may also be of a more formal, transactional nature. As we have already seen, the basically horizontal processes of interveillance are structurally integrated with vertical processes of automated commercial surveillance. This means that each user of an online service has to subscribe to terms and conditions that allow the service provider to aggregate, store and analyze data flows in order to build consumer segments for targeted online advertising, that is, to maintain the industrial logics. The kinds of recognition that may stem from such personalized services and publicity offers are ideological in the sense that they contribute to the legitimation of the dominant system itself rather than to individual autonomy (following Honneth, 2012). Whereas this means that many social media sites (such as Facebook and YouTube) to some extent occupy the same symbolically orienting function as the mass media, being part of the premediation of social relations and identities, they are at the same time transforming these conditions through turning individual media users, or prosumers, into agents of their own surveillance. They are explicitly complying with substantial privacy restraints, whose character and implications they often find obscure and/or difficult to penetrate (Andrejevic, 2007, 2014). Previous research shows that most media users feel less anxious in relation to this type of systematic surveillance than in relation to interveillance practices (see Marwick, 2012; Taddicken, 2012; Jansson, 2012) but also tend to overlook the actual terms of use that they sign (Best, 2010; Andrejevic, 2014). What may seem like a space of recognition is thus literally turned into a space of transactional dependence and "infinite debt" (Andrejevic, 2014), which in turn reproduces the functional dependence vis-à-vis various technological systems and infrastructures.

Mediatization is thus a complex transformative force that integrates *both* a liberating potential, the prospects of greater autonomy and new avenues towards social recognition enabled by media, *and* new forms of dependence that in different ways restrict the prospects of liberation. The dialectical relations between these two sides vary over time and depend on socio-cultural as well as media-specific factors that have to be identified empirically. The point that has been outlined in this essay, via the concept of interveillance, is just one yet increasingly prominent expression of the dialectics of mediatization. We may even say that this represents a new face, or a new stage, of mediatization. In this analysis the fact that mediatization processes are characterized by a complex, and contextually dependent, interplay between industrial logics and more enduring social transformations has been highlighted. If we want to formulate an immanent critique of why a growing share of the world's population allows their lives and identities to get entangled with increasingly complex technological and commercial structures of surveillance we should take this interplay into consideration—and thus also transcend the divide between institutional and social-constructivist perspectives on mediatization.

Acknowledgments

This article is part of the ongoing research project "Cosmopolitanism from the Margins: Mediations of Expressivity, Social Space and Cultural Citizenship", funded by the Swedish Research Council (2012–2015). The author would like to thank Miyase Christensen, Karin Fast and Johan Lindell for valuable discussions and comments on earlier versions of this text, as well as the anonymous reviewers for their very constructive critique.

Conflict of Interests

The author declares no conflict of interests.

References

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday* 13(3).

Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance and Society*, *2*(4), 479-497.

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

Andrejevic, M. (2014). The infinite debt of surveillance in the digital economy. In A. Jansson & M. Christensen (Eds.), *Media, surveillance and identity: Social perspectives* (pp. 91-108). New York: Peter Lang.

Beck, U., & Beck-Gernsheim, E. (2002). *Individualization: Institutionalized individualism and its social and political consequences.* London: Sage.

Bengtsson, S. (2015). *An ethics of ambiguity in a culture of connectivity?* Paper presented at the international research workshop Mediatisation of Culture and Everyday Life, 23-24 April 2015, Stockholm, Sweden.

Best, K. (2010). Living in the control society: Surveillance, users and digital screen technologies. *International Journal of Cultural Studies*, *13*(1), 5-24.

Boltanski, L. (1996/1999). *Distant suffering: Morality, media and politics.* Cambridge: Cambridge University Press.

Boltanski, L., & Chiapello, E. (1999/2007). *The new spirit of capitalism*. London: Verso.

Caughlin, J. P., & Sharabi, L. L. (2013). A communicative interdependence perspective of close relationships: The connections between mediated and unmediated interactions matter, *Journal of Communication*, *63*(5), 873-893.

Christensen, M. (2014). Complicit surveillance and mediatized geographies of visibility. In A. Jansson & M. Christensen (Eds.), *Media, surveillance and identity: Social perspectives* (pp. 15-31). New York: Peter Lang.

Couldry, N. (2003). *Media rituals: A critical approach*. London: Routledge.

Couldry, N., & Hepp, A. (2013). Conceptualizing mediatization: Contexts, traditions, arguments. *Communication Theory*, *13*(3), 191-202.

Deacon, D., & Stanyer, J. (2014). Mediatization: Key concept or conceptual bandwagon? *Media, Culture & Society*, *36*(7), 1032-1044.

Findahl, O. (2014). *Svenskarna och Internet 2014*. Stockholm: SE (Stiftelsen för Internetinfrastruktur).

Fornäs, J. (2013). The dialectics of communicative and immanent critique in cultural studies. *TripleC*, *11*(2), 504-514.

Foucault, M. (1977). *Discipline and punish*. New York: Knopf Doubleday Publishing Group.

Fraser, N. (2000). Rethinking recognition. *New Left Review*, *3*(May-June 2000), 107-120.

Fraser, N. (2001). Recognition without ethics? *Theory, Culture and Society*, *18*(2-3), 21-42.

Fuchs, C. (2014). *Social media: A critical introduction*. London: Sage.

Giddens, A. (1987). *The nation-state and violence: Volume two of a contemporary critique of historical materialism*. Berkeley: University of California Press.

Giddens, A. (1991). *Modernity and self-identity: Self and society in the late modern age*. Cambridge: Polity Press.

Gillespie, T. (2010). The politics of "platforms". *New Media & Society*, *12*(3), 347-364.

Grusin, R. (2010). *Premediation: Affect and mediality after 9/11*. Basingstoke: Palgrave Macmillan.

Hall, J. A., & Baym, N. K. (2012). Calling and texting (too much): Mobile maintenance expectations, (over)dependence, entrapment, and friendship satisfaction. *New Media and Society*, *14*(2), 316-331.

Hepp, A. (2013). *Cultures of mediatization*. Cambridge: Polity Press.

Hepp, A., Hjarvard, S., & Lundby, K. (2015). Mediatization: Theorizing the interplay between media, culture and society. *Media, Culture & Society*, *37*(2), 314-324.

Hjarvard, S. (2013). *The mediatization of culture and society*. London: Routledge.

Hjarvard, S., & Nybro Petersen, L. (2013). Mediatization and cultural change. *MedieKultur*, *54*, 1-7.

Honneth, A. (2004). Organized self-realization: Some paradoxes of individualization, *European Journal of Social Theory*, *7*(4), 463-478.

Honneth, A. (2012). *The I in the we: Studies in the theory of recognition*. London: Polity Press.

Humphreys, L. (2011). Who's watching whom? A study of interactive technology and surveillance. *Journal of Communication*, *61*(4), 575-595.

Jansson, A. (2012). Perceptions of surveillance: Reflexivity and trust in a mediatized world (the Case of Sweden). *European Journal of Communication*, *27*(4), 410-427.

Jansson, A. (2013). Mediatization and social space: Reconstructing mediatization for the transmedia age. *Communication Theory*, *23*(3), 279-296.

Jansson, A. (2014a). Textures of interveillance: A sociomaterial approach to the integration of transmedia technologies in domestic life. In A. Jansson & M. Christensen (Eds.), *Media, surveillance and identity: Social perspectives* (pp. 145-162). New York: Peter Lang.

Jansson, A. (2014b). Indispensible things: On mediatization, space and materiality. In K. Lundby (Ed.), *Mediatization of communication (Handbook of communication sciences, vol. 22)* (pp. 273-295). Berlin:

De Gruyter Mouton.
Jansson, A. (forthcoming). The moulding of mediatization: The stratified indispensability of media in close relationships, *Communications.*
Jiang, L. C., & Hancock, J. T. (2013). Absence makes the communication grow fonder: Geographic separation, interpersonal media, and intimacy in dating relationships, *Journal of Communication*, *63*(3), 556-577.
Krotz, F. (2007). The meta-process of "mediatization" as a conceptual frame. *Global Media and Communication*, *3*(3), 256-260.
Ling, R. (2008). *New tech, new ties: How mobile communication is reshaping social cohesion*. Cambridge, MA: MIT Press.
Linke, C. (2011). Being a couple in a media world: The mediatization of everyday communication in couple relationships. *Communications*, *36*(1), 91-111.
Lundby, K. (2014). Mediatization of communication. In K. Lundby (Ed.), *Mediatization of communication (Handbook of communication sciences, vol. 22)* (pp. 3-35). Berlin: De Gruyter Mouton.
Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge: Polity Press.
Marwick, A. E. (2012). The public domain: Social surveillance in everyday life. *Surveillance & Society*, *9*(4), 378-393.
Marwick, A. E. (2013). *Status update: Celebrity, publicity and branding in the social media age*. New Haven, CT: Yale University Press.
Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media and Society*, *13*(1), 114-133.
Miller, V. (2008). New media, networking and phatic culture. *Convergence*, *14*(4), 387-400.
O'Neill, S., & Smith, N. H. (Eds.) (2012). *Recognition theory as social research: Investigating the dynamics of social conflict*. Basingstoke: Palgrave Macmillan.
Paasonen, S. (2014). As networks fail: Affect, technology, and the notion of the user. *Television & New Media*. doi:10.1177/1527476414552906
Riesman, D. (1950/2001). *The lonely crowd*. New Haven: Yale University Press.
Scannell, P. (1996). *Radio, television and modern life*. Oxford: Blackwell.
Spigel, L. (1992). *Make room for TV: Television and the family ideal in postwar America*. Chicago: University of Chicago Press.
Striphas, T. (2015). Algorithmic culture. *European Journal of Cultural Studies*, *18*(4-5), 395-412.
Taddicken, M. (2012). Privacy, surveillance, and self-disclosure in the social web: Exploring the user's perspective via focus groups. In C. Fuchs, K. Boersma, A Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media* (pp. 255-271). London: Routledge.
Trottier, D. (2011). A research agenda for social media surveillance. *Fast Capitalism*, *8*(1).
Trottier, D., & Lyon, D. (2012). Key features of social media surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media* (pp. 89-105). London: Routledge.
Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other*. New York: Basic Books.
van Dijck, J. (2012). Facebook as a tool for producing sociality and connectivity. *Television and New Media*, *13*(2), 160-176.
van Dijck, J. (2013). *The culture of connectivity: A critical history of social media*. Oxford: Oxford University Press.
van Dijck, J., & Poell, T. (2013). Understanding social media logic. *Media and Communication*, *1*(1), 2-14.
Williams, R. (1974). *Television: Technology and cultural form*. London: Fontana.
Wittel, A. (2001). Toward a network sociality. *Theory, Culture & Society*, *18*(6), 51-76.

About the Author

Dr. André Jansson
André Jansson is Professor of Media and Communication Studies at Karlstad University, Sweden. His research deals primarily with questions of mediatization, identity and social space. His most recent books are *Cosmopolitanism and the media* (2015, co-authored with Miyase Christensen) and *Media, surveillance and identity* (2014, co-edited with Miyase Christensen). Recent articles have appeared in journals like *Communication Theory*, *International Journal of Cultural Studies, MedieKultur*, *New Media and Society* and *Space and Culture*.

Media and Communication (ISSN: 2183-2439)

Media and Communication is an international open access journal dedicated to a wide variety of basic and applied research in communication and its related fields. It aims at providing a research forum on the social and cultural relevance of media and communication processes.

www.cogitatiopress.com/mediaandcommunication

COGITATIO