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.