Technological Tattletales and Constitutional Black Holes: Communications Intermediaries and Constitutional Constraints

*Lisa M. Austin**

In this Article I argue that the emerging public/private nexus of surveillance involves the augmentation of state power and calls for new models of constitutional constraint. The key phenomenon is the role played by communications intermediaries in collecting the information that the state subsequently accesses. These intermediaries are not just powerful companies engaged in collecting and analyzing the information of users and the information they hold are not just business records. The key feature of these companies is that, through their information practices and architecture, they mediate other relationships. I argue that this mediating function, and its underlying technological form, interacts with legal and social norms in ways that can lead to the erosion of constraints on state power. This Article maps two stories of erosion, rooted in two kinds of community displacement. The first involves the displacement of community participation in law enforcement and the emergence of "technological tattletales" where intermediaries cooperate with the state. Unlike citizen cooperation, this practice augments state power and undermines more traditional informal modes of constraint on state power. The second involves the displacement of national legal and political community. Communications intermediaries are often large multinational companies that operate in multiple jurisdictions and move their data to various datacenters across the world even as the individual data subject remains in one geographical location. Laws that treat nonresident aliens differently from residents and citizens can

---

* University of Toronto Faculty of Law. I would like to thank the participants of *The Constitution of Information* Conference, May 2015, for their comments on an earlier version of this Article.

create "constitutional black holes" where the communications data of an individual is not protected by any constitutional constraints.

Introduction

One of the functions of constitutions is to constrain power, particularly (although not necessarily exclusively) state power.[1] This is true of both the capital-C constitutional law of written bills of rights and the small-c constitutional law associated with many of the basic principles of the rule of law, including the core ideas that law cannot confer the authority to exercise power arbitrarily and that law must be able to guide actions.[2] Lawful access — the ability of law enforcement and intelligence agencies to access personal information in the course of their investigatory duties — engages both capital-C and small-c constitutional law in many liberal democracies. For example, constitutional texts, like Canada's *Charter of Rights and Freedoms*, protect individuals against unreasonable searches and seizures, which has been held to protect an interest in privacy.[3] However, the animating concerns of the jurisprudence are not just the value of privacy, but also the problems involved in unfettered police discretion — a classic rule of law preoccupation.[4] This Article argues that these constitutional constraints are being eroded in the Information State, due to the emerging public/private nexus of lawful access, and under the cover of maintaining the status quo.

Jack Balkin defines the Information State as a state involving a new mode of governance, governing through the "collection, collation, analysis, and

---

1 *See* Robin West, Re-Imagining Justice: Progressive Interpretations of Formal Equality, Rights, and the Rule of Law (2003) (arguing that constitutions should also be about obligations on states to take positive measures to protect individuals from private power). Similarly, the rule of law is not simply about state power but also the idea that law rules in a polity — which includes laws that protect against private power. Gerald J Postema, *Fidelity in Law's Commonwealth*, *in* Private Law and the Rule of Law 17 (Lisa M. Austin & Dennis Klimchuk eds., 2014).

2 Lisa M. Austin & Dennis Klimchuk, *Introduction*, *in* Private Law and the Rule of Law, *supra* note 1, at 1.

3 Canadian Charter of Rights and Freedoms, Part 1 of the Constitution Act, 1982, *being* Schedule B to the Canada Act, 1982, c 11 (U.K.). Section 8 provides that "everyone has the right to be secure against unreasonable search or seizure." Since *Hunter v. Southam*, [1984] 2 S.C.R. 145 (Can.), this has been held to protect a reasonable expectation of privacy.

4 Lisa M. Austin, *Getting Past Privacy? Surveillance, the Charter, and the Rule of Law*, 27 Can. J.L. & Soc'y 381 (2012).

production of information."[5] One way to think of the challenges posed by the emerging Information State, particularly in the context of lawful access, is to ask whether the state needs to find new ways of doing things that it has always been doing. If one takes this view, then a key focus is to ensure that law adapts to the changing context of communications technology in order to maintain a kind of constitutional status quo: rather than allowing technology to tip power into the hands of those who seek to both break and evade the law, the state tries to maintain its law enforcement capabilities. However, another way to think of the challenges posed by the Information State is to understand the state as doing *new* things and ask what this means from the perspective of constitutional constraints. And if you take this view of the Information State then the focus needs to shift back upon the state in order to ask whether *state* power is augmented, rather than diminished, in this new mode of governance, calling for new models of constitutional constraint.

In this Article I take this second perspective. The key phenomenon we need to look at when critically interrogating claims about the constitutional status quo is the new public/private nexus of surveillance. In this nexus, states do not collect information about individuals directly but instead access the information already collected and stored by what I call "communications intermediaries" — companies that provide the basic services through which we communicate with one another, which includes internet service providers (ISPs) as well as platform providers like Google. We cannot understand this new public/private nexus by simply looking at how state access to intermediaries is governed, or by looking at how the information practices of these private corporations are regulated.[6] These intermediaries are not just powerful companies engaged in collecting and analyzing the information of users and the information they hold are not just business records. The key feature of these companies is that, through their information practices and architecture, they *mediate* other relationships. Most obviously, they mediate the relationships between individuals — the various users who want to talk to one another, to share information and collaborate through the communication services.

It is because of this mediating function that intermediaries are so valuable to the state, for it allows the state to access the content of our communications as well as a treasure trove of other associated data, including what we do online and the nature of our social networks; collecting this information directly from individuals would be difficult and expensive. As Bruce Schneier stated after the Snowden revelations, "The NSA didn't build its eavesdropping

---

5 Jack M. Balkin, *The Constitution in the National Surveillance State*, 1 Minn. L. Rev. 1 (2008).

6 For example, Balkin argues that both of these are important. *Id.* at 20-21.

system from scratch; it got itself a copy of what the corporate world was already collecting."[7] What I show throughout this Article is that this mediating function, and its underlying technological form, interacts with legal and social norms in ways that can lead to the erosion of constraints on state power.[8] This erosion, however, is often hidden by claims that state practices are merely maintaining the legal status quo.

This Article maps out two stories of erosion, rooted in two kinds of community displacement created by the widespread use of communications intermediaries. The first story (discussed in Part I) involves the displacement of community participation in law enforcement. Instead of a world where law enforcement agents must convince members of the public to cooperate with investigations, we now have a world of "technological tattletales." The status quo argument is that cooperation from intermediaries is no different than other forms of citizen cooperation. However, I outline why the emergence of such technological tattletales raises rule of law concerns due to the way in which this practice augments state power while undermining more traditional informal modes of constraint on state power.

The second story (discussed in Part II) involves the displacement of national legal and political community. Communications intermediaries are often large multinational companies that operate in multiple jurisdictions and move their data to various datacenters across the world. While the private sector protections for this data might be relatively equivalent across these different jurisdictions, national differences regarding constraints on state access often differ. The status quo argument is that constitutional constraints should protect members of one's domestic political community, not nonresident aliens. However, I argue that this masks the way in which national differences can in fact create "constitutional black holes" where the communications data, including associated metadata, of an individual is not protected by *any* constitutional constraints.

Both of these displacements — the displacement of civic community and the displacement of political community — involve the displacement of modes of constraint on state power. In mapping both problems, I argue that it is difficult to see the problems unless we start to understand the mediating function of communications intermediaries and how this function interacts with social and legal norms in ways that disrupt our understanding of either public

---

7 Bruce Schneier, *'Stalker' Economy Here to Stay*, CNN (Nov. 26, 2013), http://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/index.html.

8 By technological form I do not mean to claim some kind of technological determinism — the form is often dictated by business practices and market forces as much as engineering design.

or private regulation. This Article does not aim to offer a clear resolution to the problems of either technological tattletales or constitutional black holes, but instead seeks to illustrate through these examples how difficult it is to come to terms with the public/private nexus of surveillance in the Information State, where power shifts in unexpected ways and where our standard tools do not yield obvious solutions.

I. Technological Tattletales

Law enforcement authorities increasingly seek access to information held by communications intermediaries. For example, in 2014 Google reported that data was requested for 99,202 users or accounts (from both law enforcement agencies and national security agencies).[9] In the same year, Microsoft reported that data was requested for 111,559 users or accounts (from law enforcement agencies), 37,000 to 38,998 accounts were impacted by national security orders seeking content, and 0 to 999 accounts were impacted by national security orders seeking non-content.[10] There is reason to believe that access requests made to internet service providers and cell phone providers occur even more frequently. One of Canada's top three providers, Rogers, reported that in 2014 it received 113,655 requests.[11]

There have been a variety of efforts to ensure that law enforcement authorities and national security agencies can gain access to information held by these communications intermediaries. My aim is not to catalogue these efforts and debates but to highlight a basic underlying displacement that we need to understand in order to assess this emerging private/public nexus. The typical justification for legislation requiring some new form of access is that it remedies a situation where "laws have not kept pace" with technology.[12] The idea is

---

9 *Transparency Report*, Google, http://www.google.com/transparencyreport/userdatarequests/?metric=targets (last visited Nov. 28, 2015). These are global numbers and include all criminal and national security requests.

10 *Law Enforcement Requests Report*, Microsoft Transparency Hub, https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/lerr/ (last visited Nov. 28, 2015); *U.S. National Security Orders Report*, Microsoft Transparency Hub, https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/fisa/ (last visited Nov. 28, 2015).

11 *2014 Rogers Transparency Report*, Rogers, http://www.rogers.com/cms/pdf/en/2014-Rogers-Transparency-Report.pdf (last visited Feb. 9, 2016). The report does not disclose how many accounts/users were affected by these requests.

12 *Summary of Submissions to the Lawful Access Consultation (2005)*, Gov't of Can., Dep't of Justice, http://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html (last modified Jan. 7, 2015).

that we already have laws that permit things like wiretaps and we need to "update" them in order to accommodate new information and communications technology. The problem with this analogy between phone technology and twenty-first century information and communications technology is that access to information stored by communications intermediaries is not about real-time interception of a conversation but access to a record of multiple modes of communication, past and present, including interactions on kinds of social media and including associated metadata that can be used to map your social networks and physical habits. This is not just a new version of tapping your phone. The more apt analogy is between authorities seeking the assistance of community members to provide them with information about suspects and authorities now seeking the assistance of communications intermediaries. By community I mean to simply point to the role of ordinary citizens in the course of their everyday lives and activities within their neighborhoods, social circles, and local community organizations (for example, schools, religious organizations, volunteer groups); the information that your community might know about you now has a digital copy stored by intermediaries.

The questions, then, are these: what is the difference between community cooperation with law enforcement investigations and intermediary cooperation with law enforcement investigations? When the community is displaced in favor of the communications intermediary, does this augment state power or maintain the status quo in the face of new technologies? For the purposes of simplicity, in discussing these questions I focus on the law enforcement context and not the national security context, although both are important in the new private/public nexus of state surveillance.

A. Differences Between Community Cooperation and Intermediary Cooperation

The police routinely ask citizens for information pertinent to their investigations and they do not need to get a warrant to do so. Should they have to get a warrant to request information from communications intermediaries? Why not leave the issue of cooperation to the discretion of the intermediary, just as we leave cooperation to the discretion of the citizen? This Section argues that there are several important differences between citizen cooperation and intermediary cooperation and that these differences are relevant to understanding what kinds of constraints operate in relation to state power.

The first important difference concerns the nature of the information at issue. Information held within communities is different from information held by communications intermediaries. For one thing, information within a community is often decentralized, as different "pieces" of information are held

by different people within the community. Access to these pieces is mediated by many different human factors such as memory and the myriad factors that affect how, when and why an individual might be willing to cooperate with state authorities. Because this information is held by other people who must be contacted and interacted with, it usually requires time and effort by law enforcement agents to gather. Information held by a communication intermediary is often centralized — all of an individual's communications with a wide variety of people over a period of time could be potentially available from the intermediary. This information is not filtered through human memory and motivation but can be produced as a copy of its original form. Moreover, this information has metadata associated with it, which permits forms of analysis that are difficult, if not impossible, with unstructured data.[13] The time and costs involved in accessing this data from intermediaries can be low compared with more traditional investigative techniques.

One can sum up these differences by saying that community cooperation involves many more practical constraints than intermediary cooperation.[14] The question then is why we should care about the erasure of these practical constraints, especially since the result is the availability of more usable information, more easily, and more cheaply. But practical constraints help to condition the exercise of state power. When they are erased we need to attend to the resulting augmentation of state power and address whether new forms of constraint are advisable. From this perspective of constraints on state power, citizen cooperation and intermediary cooperation are not equivalent; where the social world used to provide de facto forms of protection, there is at least a question of whether the law needs to impose new norms in order to return to the status quo.

The second way in which citizen cooperation and intermediary cooperation are different lies in the question of whether the police are simply doing what anyone else is free to do or are gaining special access to information. To understand why this is a question, consider search and seizure's roots in the law of trespass. In the Anglo-American traditions of countries like the United States and Canada, the modern trajectory of search and seizure law is often thought to have started with the protection of property and then shifted to the

---

13 This can shift methods away from those that rely on local knowledge and judgment towards data-intensive techniques, and there are questions about whether that is actually so effective. *See* Lisa M. Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)*, *in* A World Without Privacy? What Can/Should Law Do 131 (Austin Sarat ed., 2014).

14 Lisa M. Austin, *Towards a Public Law of Privacy: Meeting the Big Data Challenge*, 71 Sup. Ct. L. Rev. 527 (2015).

protection of privacy.[15] This suggests that the focus is on the type of interest protection — property and privacy. Another way to look at this jurisprudence, however, is to see it as dominated by a concern to place limits on discretionary authority.[16] One way of placing such limits is to ensure that public authorities follow the ordinary laws unless they have special authorization to depart from this. If it is generally against the law to enter another person's home without their permission (trespass) then the police must seek special legal authorization to do so (a warrant). Although things get a great deal murkier when attention shifts from property (with clear laws and boundaries) to privacy (and the reasonable expectation of privacy test), there continues to be a general intuition that if the police are simply doing what others are free to do (for example, observing someone in public), then there is no need for special authorization.

We can apply this insight to the case of community cooperation. Individuals are free to ask each other questions about their neighbors and about events they have witnessed within their neighborhoods. When police ask questions they are only doing what citizens in general are free to do. However, the situation is different with communications intermediaries. There are often various legal impediments to an individual's seeking information about a neighbor from an intermediary. For example, in Canada this would be a prohibited disclosure unless it had been consented to by that individual. If providing that information to the police is a permitted disclosure, then this allows the police to get access to that information in a manner that ordinary citizens are not permitted to do. In this way, the police have greater power than ordinary citizens and this has traditionally been thought to engage the need for justification and, often, special justice authorization such as the warrant requirement.

Despite the seeming similarity between citizen cooperation and intermediary cooperation, these two differences show that in the context of intermediary cooperation state power is augmented. Treating them the same obscures this shift in power dynamics and prevents us from asking questions about constraints.

However, the issue is not simply one of practical constraints or special access by the state. When state surveillance practices bypass community involvement, citizen agency is also bypassed. An important aspect to community cooperation with state authorities in information gathering is that citizens

---

15 Hunter v. Southam, [1984] 2 S.C.R. 145 (Can.).

16 Austin, *supra* note 4; Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547 (1999); M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. Rev. 85 (2010).

exercise *agency*. They are not simply sources of information — they also exercise their own capacity to decide whether to cooperate, and on what terms. Citizen agency introduces citizen discretion into law enforcement. In what follows I want to outline why this discretion can sometimes play an important rule of law function in constraining state power, and also why this discretion can sometimes be problematic from a rule of law perspective. Once the contours of citizen discretion are clearer, then we can understand the impact on state power when this citizen discretion shifts to intermediary discretion or even to no discretion, such as when intermediaries are compelled to cooperate with state authorities.

B. Citizen Agency, Discretion and the Rule of Law

Rule of law narratives often focus on the role of law enforcement or the courts and overlook the role of citizens.[17] However, citizens play a role in upholding the rule of law in at least three ways. The first is by following the law, which I refer to as "self-constraint." When individuals exercise self-constraint, and obey the law, then they very obviously contribute to a society where law rules. Although many accounts of the rule of law list the guidance function of law as one that is separate from the idea that law constrains arbitrary power, the two are linked. If law cannot guide individual action, then the self-application of the law and self-constraint become impossible. This undermines the ability of the law to constrain the arbitrary power of individuals in relation to other individuals. The second way that citizens help to uphold the rule of law is through what I call "other-constraint." The most obvious example of this is when citizens assist in law enforcement efforts that hold others to account in obeying the law. The third role for citizens is in "state-constraint," or holding the state to account in its exercise of authority. There are a number of obvious ways in which citizens do this, through voting and through exercising their free speech rights. However, as I outline below, there are also a number of nonobvious ways that are important. This Section deals primarily with the second citizen function, that of other-constraint. However, I argue that the context of citizen cooperation can also affect the functions of self-constraint and state-constraint.

Citizen cooperation involves citizen discretion and the first thing to get clear is why discretion is an issue in the law enforcement context. Search and seizure jurisprudence has often been concerned with constraining police discretion, and in scholarship on the increasing administrative nature of the criminal justice system there has been much discussion of prosecutorial

---

17 *But see* Postema, *supra* note 1.

discretion.[18] There is far less attention paid to the issue of citizen discretion with respect to cooperation with investigations and the impact this has on the justice system. But the basic concern about discretion in the administration of justice remains the same across all of these cases. That concern is to prevent individuals from acting upon personal prejudices, vendettas, and private beliefs rather than public purposes.

How this operates in relation to citizen discretion can be illuminated by reflection upon our moral censure of "tattling." Those with young kids might be familiar with the difficulty of teaching them when it is acceptable — and even desirable — to tell on another person and when it is not. Nobody likes a "tattletale" and yet there are circumstances where telling is indeed the right thing to do. Some of the anti-bullying education efforts make the distinction between "telling" and "tattling" in terms of what the objective of the action is.[19] For example, if the objective is the safety of oneself or others, then it is "telling." If the objective is to get someone else in trouble, then it is "tattling." We might say that "telling" is motivated by pursuing some objective idea of the good, or the good of others, and "tattling" is motivated by selfish interests, which may include the interest in harming another.

"Snitching" carries with it many of the connotations of "tattling" but typically refers to an individual within a criminal group who informs on other members of the group in order to receive leniency from the state.[20] A snitch tells on others who were involved in their crime and does so in order to further their own self-interest. With snitching, there is a kind of double problem involving discretion: prosecutorial discretion is supplanted by informant discretion, which is motivated by self-interest, and informant discretion is overseen by police who exercise broad discretion in their handling of these informants, with little public oversight.[21]

The negative connotations associated with snitching and tattling are not just about the pursuit of self-interest over public interest but also have to do with the violation of group loyalty involved. Instead of promoting the values of friendship, trust and solidarity, from the perspective of the criminal group the snitch participates in disloyalty, treachery and betrayal.[22] As Michael Rich

---

18 William Stuntz, The Collapse of American Criminal Justice (2013).

19 *See The Difference Between Telling and Tattling*, Together Against Bullying, http://www.togetheragainstbullying.org/the-difference-between-telling-and-tattling (last visited Nov. 28, 2015).

20 Alexandra Natapoff, *Snitching: The Institutional and Communal Consequences*, 73 U. Cin. L. Rev. 645 (2004).

21 *Id.* at 674.

22 Malin Akerström, *Snitches on Snitching*, 26 Soc'y 22 (1989).

points out, loyalty and disloyalty are about relationships. The duties of loyalty, therefore, are not simply about putting aside self-interest but about conforming to the norms of particular relationships, such as marriage, friendship, ethnic group, neighborhood, etc.[23] This dynamic of group loyalty that generates the moral opprobrium associated with the word "snitch" is not confined to the context of "honor among thieves." It is this same dynamic that can motivate officers within the police forces or the military to protect one another even when a member of their group has violated norms they have been sworn to uphold.[24] Disloyalty is something that generally attracts moral opprobrium but is sometimes justified, depending on many contextual factors about which different people might have different views.[25] These factors can include the seriousness of the behavior at issue, and whether the problem is something that could be dealt with in a manner "internal" to the community/relationship.[26]

As Alexandra Natapoff points out, the widespread use of informants can have a disproportionate negative effect on communities where they are used in large numbers, such as poor, racialized communities with high incidents of drug crimes.[27] In such a context both interpersonal trust and institutional trust are affected — interpersonal because one has reason to potentially distrust a large number of people within one's social circle, and institutional because of the message that "the state secretly permits criminals to evade punishment by snitching on friends and family."[28] This complex relationship between social trust and cooperation is important. As Dan Kahan argues, when citizens trust each other and the state then they are more likely to themselves follow the law.[29] Research has shown that perceptions of police legitimacy and trust in institutions are correlated both with compliance with the law and with cooperation with the police more generally.[30]

---

23 Michael L. Rich, *Lessons of Disloyalty in the World of Criminal Informants*, 49 Am. Crim. L. Rev. 1493, 1501-02 (2012).

24 Bret D. Asbury, *Anti-Snitching Norms and Community Loyalty*, 89 Or. L. Rev. 1257 (2011).

25 Rich, *supra* note 23, at 1508.

26 *Id.* at 1517-18 (suggesting that snitching norms in high-crime neighborhoods are partly motivated by an insularity that leads the community to view crime as an internal problem and not one for police intervention).

27 Natapoff, *supra* note 20, at 646.

28 *Id.* at 684.

29 Dan M. Kahan, *The Logic of Reciprocity: Trust, Collective Action, and Law*, 102 Mich. L. Rev. 71 (2003).

30 Tom R. Tyler, Why People Obey the Law (2006); Tom R. Tyler & Jeffrey Fagan, *Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in Their Communities?*, 6 Ohio St. J. Crim. L. 231 (2008).

Sometimes the label "snitching" is applied to the more general phenomenon of citizen cooperation, where the person who shares information is not necessarily involved in criminal activities and does not necessarily receive a personal benefit, such as leniency, from informing police. For example, in the United States the "Stop Snitching" movement was popularized by the "Stop Snitchin'" DVDs.[31] Despite what many saw as its message of witness intimidation, these DVDs contributed to a movement within many communities — particularly poor, black communities — to not cooperate with police. Bret Asbury suggests that one way to understand this is to see that even in this more general context of snitching, the primary moral issue is one of community loyalty. According to Asbury, "[t]here is a fundamental disconnect between these communities and the police, and Stop Snitching represents the culmination of the historical uneasiness that has existed between them, an uneasiness that persists today and plays a pivotal role in deterring witnesses from helping the police solve crimes."[32]

Those who refuse to snitch privilege loyalty to their community over loyalty to the state, for various reasons. Some might be concerns for the effects of incarceration on the accused's family and community, particularly in communities where incarceration rates are high and create many social problems.[33] Other concerns might include the general lack of trust a community might have in the police to look after their interests, and a perceived illegitimacy in the justice system more generally.

In this broader context of citizen cooperation, there can also be concerns regarding the motivations that individuals have to cooperate with the state, and not just concerns about their noncooperation. For example, the influential report of Canada's Task Force on Privacy and Computers noted, in 1972, the public concern surrounding the information-gathering practices of corporations and governmental institutions, particularly "the practice of some investigators who make unauthorized inquiries among the friends and neighbours of a subject, a technique that renders the final dossier vulnerable to hearsay, and to gossip which may be founded in prejudice and malice."[34]

When Canada later adopted its Privacy Act, one of its requirements was that government institutions "shall, wherever possible, collect personal information

---

31 These were coproduced by rapper Ronnie Thomas ("Skinney Suge"). Thomas was later convicted and imprisoned on gang-related racketeering charges. *See Producer of 'Stop Snitching' Witness Intimidation Videos Sentenced to Prison*, Baltimore Sun (June 25, 2010), http://articles.baltimoresun.com/2010-06-25/news/bs-md-stop-snitching-sentence-20100625_1_snitching-skinny-suge-videos.

32 Asbury, *supra* note 24, at 1262.

33 *Id.* at 1299.

34 Privacy and Computers: Report of the Task Force Established by the Department of Communications/Department of Justice 113 (1972).

that is intended to be used for an administrative purpose directly from the individual to whom it relates."[35] The Privacy Act's solution for dealing with the problem of secondhand information by requiring collection directly from the individual is not workable in the law enforcement context, as information collection there is usually contrary to the self-interest of the individual, protected by rights against self-incrimination, and likely to be inaccurate. In the context of an individual receiving government benefits — the administrative context of the social welfare state — providing accurate information is in the individual's self-interest.

Crimestoppers offers an interesting example of a system of information gathering in the law enforcement context that seeks to address the concern about inaccurate information motivated by the personal prejudices and ill-will of the informer. These local or regional programs are run in many different jurisdictions, including both Canada and the United States. Crimestoppers pays for anonymous crime tips, engaging financial self-interest as at least one motivation rather than a sense of general moral or civic responsibility. However, they only pay for "good" information ("information clear enough and specific enough to lead to an arrest or indictment"[36]) and the programs are funded privately and often controlled by civilian directors.[37]

What conclusions can we draw from this? It is not the case that citizen cooperation is always good or that the lack of citizen cooperation is always bad. The issue is not the cooperation *per se* but what informs the exercise of discretion to cooperate or not. When citizens cooperate from a perspective of civic duty, then they fulfill an important rule of law function by helping the state in its role in constraining exercises of private power (other-constraint). The decision to cooperate helps to ensure that legal violations are investigated and prosecuted. When citizens cooperate out of self-interest or personal vendettas, then this can be just as distorting to the administration of justice as problematic exercises of discretion on the part of public officials. When citizens refuse to cooperate out of resistance to perceived patterns of illegitimate state activity, then they are also fulfilling an important rule of law function by helping to constrain the problematic exercise of state power (state-constraint). A lack of cooperation that is motivated by problematic personal beliefs — such as discriminatory views — can also lead to situations where the rule

---

35 Privacy Act, R.S.C., 1985, c. P-21, s. 5(1). There are several exceptions to this, such as when it would lead to the collection of inaccurate information or where it would undermine the purpose for which the information was collected.

36 Erdwin H. Pfuhl, *Crimestoppers: The Legitimation of Snitching*, 9 Just. Q. 505, 508 (1992).

37 *Id.* at 509.

of law fails.[38] Moreover, many of the factors that help to ensure cooperation are also the factors important to ensuring general social trust in the legal system, which is also correlated with individuals themselves following the law (self-constraint). In other words, where the state is seen to exercise power legitimately, citizens will exercise self-constraint and other-constraint, but where it is not then citizens will not, which itself acts as a constraint on state power. Citizen cooperation and noncooperation alike can undermine rule of law values when either the one or the other is motivated by the pursuit of personal gain or prejudices rather than public values.

C. Shifting Constraints

What happens when this community discretion to cooperate with authorities shifts and is replaced by intermediary discretion? The first thing to note is that intermediary discretion is situated within a context that makes intermediaries more powerful than ordinary citizens. The nature of the information held by intermediaries is not mediated by the frailties of human memory or individual relationships, and is centralized, digitized, and structured data. A decision to share information with state authorities can therefore potentially offer the state more information, more useful information, and more accurate information than when information is dispersed within a community. The impact of this power shift on rule of law values depends on the way in which this power is exercised.

What is the motivation for intermediary cooperation and to what extent is this motivation congruent with public values rather than private interest or prejudice? There is evidence that in some charged contexts, like child exploitation investigations, intermediaries are motivated by a general civic duty.[39] The difficulty lies in moving beyond these specific cases to other types of criminal activity, and to other types of customer information that does not necessarily immediately identify an individual offender. One court in Canada recently suggested that a communications intermediary has a general interest in preventing its services from being used for illegal purposes. In *R. v. Ward*, a case concerning whether the police required a warrant to obtain subscriber

---

38 One might describe the "public practice of illegality" characteristic of the era of Jim Crow segregation in the American South in these terms. *See* Gerald J. Postema, *Law's Ethos: Reflections on a Public Practice of Illegality*, 90 B.U. L. Rev. 1847, 1850 (2010).

39 Lisa M. Austin & Andrea Slane, *What's in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations*, 57 Crim. L.Q. 487 (2011).

information from an ISP who was willing to voluntarily provide it, the Ontario Court of Appeal stated:

> Like any service provider, Bell Sympatico has a legitimate interest in preventing the criminal misuse of its services, particularly in circumstances where the misuse effectively constituted the *actus reus* of a crime. The interest may be seen as purely as self-interest or, perhaps more appropriately, as a form of "civic engagement" reflecting a corporate commitment to assist in law enforcement's struggle to rid the Internet of child pornography.[40]

On its face, this does not look like a sweeping statement, especially since the case in question concerned a child pornography investigation. However, the heart of the comment lies with the close connection between the ISP services and the commission of the crime and not with the particular nature of the crime.[41] As we shift more and more of our activities online, there are many more crimes that will involve a close connection with the services of an ISP. And as Big Data techniques become more ubiquitous, monitoring for criminal misuse can potentially involve a great deal of customer data. Can intermediaries simply decide to monitor for criminal misuse and share that information with the police?

If the idea is that civic duty and corporate interest align in preventing criminal misuse of services, then perhaps intermediary cooperation is free of the kinds of personal interest or prejudice that raises questions with other "snitches." However, it also seems to be free of other kinds of constraining social norms, such as the loyalty characteristic of various social relations. As outlined in the previous Section, tattling on a friend or family member is a kind of disloyalty that attracts our moral censure, but in some contexts other social values take precedence. Individuals might rightly break the bonds of loyalty in the context of serious crimes, for example, but are judged much more harshly and negatively when they inform about less serious crimes or when the matter could be resolved in a manner that does not involve the police. In this way, social norms regarding what is appropriate in different relationships operate informally to constrain breaches of loyalty except in cases of very serious criminal or immoral behavior. It is not socially acceptable to simply always tell on another, even if one has no "private" motive for doing so. Do intermediaries have a sense of loyalty to their customers? It is difficult to see how this is the case when the relationship is often regulated by terms of service

---

40 R. v. Ward, 2012 ONCA 660 ¶ 97 (Can.).

41 *See also id.* ¶ 102 (emphasizing the "direct connection" between the services and the commission of the crime).

that stipulate that the customers will not use the services for illegal activities, can be monitored for such, and that information can be shared with the state. Indeed, some Canadian courts have pointed to such agreements as evidence that individuals have a diminished expectation of privacy in the information they share with intermediaries because they have consented to such terms.[42]

Do intermediaries have a general sense of civic duty that provides a source of constraint on state actions? As we saw with citizens generally, basic perceptions of the legitimacy of state power affect citizen willingness to cooperate with police. It is not clear that intermediaries are a substitute for this citizen role. Decision makers within these corporations have to exercise their discretion in line with corporate interests and policies and not with their own views. These companies are not necessarily situated within the particular communities that feel the impact of the police investigations they cooperate with.

If there are effectively few constraints on intermediary cooperation, then another problem arises concerning the potential scope of information available. Alan Westin argued that one of the "distinguishing characteristics of life in a free society" is "having privacy for permissible deviations."[43] By this, he meant that there are a number of norms and laws in society that society only punishes the most extreme transgressions of which and largely tolerates most violations. He cautioned that "[i]f there were no privacy to permit society to ignore these deviations — if all transgressions were known — most persons in society would be under organizational discipline or in jail, or could be manipulated by threats of such action."[44] When information that would otherwise be dispersed within a community gets centralized by an intermediary and then is easily available to the state, we come close to such a situation where all transgressions are known. This is a shift that we need to understand more fully and also put into the context of another important shift — the increasing move towards crime *prevention*. But if all transgressions are known, or even predicted with great frequency, then it becomes burdensome to determine who to charge and prosecute. What this situation does is shift the source of discretion again, from intermediary discretion towards greater police and prosecutorial discretion. The issue then is to determine whether there should be new forms of constraint in these areas.

In a post-Snowden world, however, intermediaries increasingly understand that their business interests align strongly with protecting customer privacy. This suggests that intermediaries should be as much concerned with their role in constraining the state as they have been with their role in cooperating

---

42 *See* Austin & Slane, *supra* note 39.

43 Alan Westin, Privacy and Freedom 35 (1967).

44 *Id.*

with the state (and constraining others who might violate the law). One way to do this is to only comply with court orders and not otherwise voluntarily provide information to the state. This would achieve several objectives. The first is that it would reduce the effect that service policies and agreements might have in reducing an expectation of privacy. A production order does not indicate that the information sought has no privacy interest attached to it — it affirms that it is generally private but that when special authorization is given (preferably by a court) then this privacy is overridden in the name of state objectives of law enforcement. A court cannot logically point to a policy that affirms that an intermediary will comply with court orders and from this infer that this means there is a diminished expectation of privacy in the information generally.

The second effect is that intermediary discretion would be displaced by court oversight. If fewer norms constrain intermediary cooperation than constrain citizen cooperation, and if intermediaries are more powerful than ordinary citizens, then this shift to court oversight could be a welcome rebalancing. Canada has largely taken this route with its recent Supreme Court decision in *R. v. Spencer*.[45] In that case, the Court held that the police need a warrant to access basic subscriber information even when an ISP is willing to provide it voluntarily in response to a police request. There are also new warrant and production order provisions in Canada that allow for state access to different forms of metadata held by third parties.[46]

However, this state access still takes place in a context of reduced constraints in at least two ways. The first way is that access to information held by intermediaries involves fewer practical restraints than access to information within the community more generally. If the information at issue is centralized, digital, unmediated by "human" factors, and structured, then it is potentially far more useful and revealing than information dispersed within a community. Even if the police require a warrant to access it, it is unclear that such warrants are as constraining as previous practical constraints.

The second way, which concerns the standards on which warrants and production orders are granted, is perhaps even more important. Despite a growing consensus within the privacy community that metadata can be as revealing as content data, most legal systems still reflect the idea that metadata attracts a lower expectation of privacy. In Canada, for example, a production order can be granted for transmission data on the grounds that there are

---

45 R. v. Spencer, [2014] S.C.C. 43 (Can.).

46 There are potential constitutional questions about these orders and whether they infringe upon a reasonable expectation of privacy, but a discussion of these questions is beyond the scope of this Article.

"reasonable grounds to suspect" an offence has or will be committed and that the transmission data "will assist in the investigation."[47] This is much lower than the usual standard of "reasonable grounds to believe" that the data "will afford evidence respecting the commission of the offence."[48] Even if state access to metadata is mediated by court oversight, if the process does not properly track the privacy interest at stake then too much access will be granted. This takes us back to the scope problem flagged earlier — if the state effectively gets easier access to more information about us then we come closer to a situation where all transgressions are either known or knowable. This raises important questions regarding how police and prosecutorial discretion should operate and with what kind of oversight and accountability.

In sum, if we return to the initial question of whether there is a difference between community cooperation and intermediary cooperation, the answer is clearly yes. There are numerous ways in which intermediary cooperation operates with fewer practical and informal constraints than community cooperation.

II. Constitutional Black Holes

As just outlined, one aspect of communications intermediaries is that they displace the role of communities in law enforcement. Another important community displacement is that of national political community. Communications intermediaries, given their technical architecture and business practices, facilitate data crossing national borders. This makes that data subject to the laws of those other jurisdictions, including laws governing access to that information for law enforcement or national security purposes.

For example, many platform providers are multinational corporations who embrace cloud computing and operate multiple data centers in multiple jurisdictions, so one user's information might be in multiple centers, allowing for ready availability and data recovery. A consumer in Canada who signs up with Google for a Gmail account will have their communications data travel to, and be stored in, data centers in the United States and even around the globe. Enterprise clients who sign up for cloud-based services can have all their communications data stored in the United States — even communication between two Canadian employees who work in the same building.[49] Service

---

47 Criminal Code, R.S.C., 1985, c. C-46, s. 487.016 (Can.).

48 *Id.* s. 487.014.

49 For example, many Canadian universities have outsourced their email to either Microsoft or Google. In such a situation, even when email communication is between individuals within that university, or with someone who is at another Canadian university, that email will both transit the United States and be stored

providers also facilitate information crossing borders. This is perhaps an obvious aspect of international communications but it can occur with entirely domestic communications as well. Within Canada, researchers have documented "boomerang routes" where communications that originate and terminate within Canada nonetheless pass through the United States, a result that is largely due to the business practices of carriers. As Andrew Clement and Jonathan Obar outline, "carriers are selective about who they exchange traffic with directly: the larger ones typically are reluctant to exchange traffic with their smaller competitors and have an incentive to make it difficult for them to reach destinations outside their immediate networks."[50]

The important question is whether data crossing national borders augments state power in the context of lawful access such that we should rethink our models of constraint. Cross-border data concerns are, after all, nothing new. However, as outlined below, there are many reasons to think that the kind of information practices that are now ubiquitous have features that in fact lead to the erosion of constitutional constraints.

A. Legal Loopholes and National Boundaries

There remains a strong territorial basis for the application of national laws, especially in the context of lawful access and the application of constitutional constraints on this access.[51] The status quo response to data crossing borders, therefore, is that the lawful access rules of the jurisdiction where the data is located should apply. Internet communications might be global, but national laws apply. This basic claim surfaces frequently, in different contexts. For

---

there as a function of using these services. In this way communications that are entirely between Canadians who themselves are within Canada are nonetheless within the boundaries of the United States. *See* Heidi Bohaker, Lisa Austin, Andrew Clement & Stephanie Perrin, Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World (2015), http://ecommoutsourcing.ischool.utoronto.ca/wp-content/uploads/BohakerAustinClementPerrin_SeeingThroughTheCloud-PublicReport-15Sept2015.pdf.

50 Andrew Clement & Jonathan A. Obar, *Canadian Internet "Boomerang" Traffic and Mass NSA Suveillance*, *in* Law, Privacy and Surveillance in Canada in the Post-Snowden Era 13, 21 (Michael Geist ed., 2015).

51 Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326 (2015). There are separate issues with respect to the question of the extraterritorial application of warrant authority — this is not about applying constitutional constraints to the exercise of state power, but about the territorial boundaries of the exercise of that power.

example, the Canada and U.S. "Beyond the Border" plan calls for increased information sharing at the border, while at the same time talking of "respecting our separate constitutional and legal frameworks that protect privacy."[52]

Part of the perceived problem, however, is that national laws offer different levels of protection. For example, Canadian constitutional norms regarding privacy are more protective than U.S. constitutional norms, particularly when dealing with communications intermediaries and the new public/private nexus of lawful access. For example, Canada has long rejected the U.S. third party doctrine, which holds that once data is shared with a third party then it no longer attracts a reasonable expectation of privacy. The Supreme Court of Canada has also recently held that access to basic subscriber information requires a warrant. Under the status quo argument, given the many different ways and high likelihood that data will cross borders, Canadians risk having their communications data accessed under lower standards within the United States; they are no longer protected by their own national norms.

This community displacement is different from the more familiar situation of individuals who seek to do business in another country in order to take advantage of the laws of that country. The paradigm case for this latter situation would be banking, where individuals might want to benefit from laws in a particular jurisdiction and so do business there. In such a case, an individual very much understands the legal implications of doing business in another jurisdiction — that is the very point. If for some reason lawful access laws in the country-of-business are less protective than lawful access laws in the country-of-residence, then one might still conclude that this was a state of affairs chosen by the individual and that one cannot choose some legal benefits but disclaim any accompanying legal disadvantages. In contrast, subscribers to communications intermediaries are choosing services based on price and features and often do not understand the legal implications of their choice. The practices of intermediaries in sending data from one data center to another, often crossing jurisdictional boundaries, is itself dictated by technological and economic imperatives and has little to do with choosing to be subject to particular legal regimes.[53] Furthermore, the amount and type of data now at issue and the number of individuals implicated is huge and growing.

However, the issue is not just that data in other jurisdictions is subject to a different national law, or that it might as a result receive a lower level

---

52 White House, United States, Canada Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness Action Plan 27 (2011), https://www.whitehouse.gov/sites/default/files/us-canada_btb_action_plan3.pdf.

53 With the obvious exception of service providers who advertise local data storage as a feature of their service.

of privacy protection, depending upon national laws. The issue is that the data might fall into a legal loophole. To understand this claim, two other crucial contextual elements must be layered atop this story of information dispersion: first, the increased cooperation and coordination between states in relation to both law enforcement and national security and, second, the fact that some countries treat nonresident aliens differently under their laws than residents. Taken together, this leads to a situation where communication data is dispersed globally, where national authorities are acting transnationally, but where the checks and balances on state power — including constitutional privacy norms — remain dependent on ideas of nationality and territoriality. The result is legal loopholes where constitutional constraints on state actions that infringe privacy are severely weakened.

For example, in his testimony before the European Parliament, Edward Snowden remarked that the cooperation between the NSA and EU states created a "European bazaar" of surveillance. He elaborated:

> [A]n EU member state like Denmark may give the NSA access to a tapping center on the (unenforceable) condition that NSA doesn't search it for Danes, and Germany may give the NSA access to another on the condition that it doesn't search for Germans. Yet the two tapping sites may be two points on the same cable, so the NSA simply captures the communications of the German citizens as they transit Denmark, and the Danish citizens as they transit Germany, all the while considering it entirely in accordance with their agreements. Ultimately, each EU national government's spy services are independently hawking domestic accesses to the NSA, GCHQ, FRA, and the like without having any awareness of how their individual contribution is enabling the greater patchwork of mass surveillance against ordinary citizens as a whole.[54]

The basic legal loophole in this international data flow basically looks like this: nation A can collect data within their own territory that is about citizens from nation B, on lower standards than apply to citizens from nation A, and the norms of nation B do not reach into nation A to protect the citizens of nation B. The result is the ratcheting down of protection under the patina of liberal-democratic constraints because states are indeed applying their own laws.[55]

---

54 Edward Snowden, Testimony to European Parliament (Mar. 7, 2014), http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.

55 This exploitation of extraterritoriality in relation to internet communications is of a piece with other controversial U.S. extraterritorial strategies in relation to terrorism. *See* Kal Raustiala, Does the Constitution Follow the Flag? The

In the rest of this Article, I take constitutional law and the U.S.-Canada border as a case study and map out how the basic structure of this legal loophole in fact constructs a constitutional *black hole*. When data about Canadian persons crosses the Canada-U.S. border, it can be subject to lawful access on U.S. legal standards and the U.S. constitutional position is that the Fourth Amendment does not apply to nonresident aliens. The Canadian constitutional position is that the *Canadian Charter of Rights and Freedoms* (the *Charter*) does not apply to extraterritorial searches and seizures. This data therefore falls within a constitutional black hole, where the constitutional norms of neither jurisdiction apply to state access. Far from the status quo, this is the erasure of constitutional constraints.

B. Constitutional Black Holes

In this Section I want to map out a very specific constitutional black hole to show how it can arise through the seemingly rational application of domestic legal doctrine and yet operate to undermine rights quite dramatically when bodies and data are in different locations. The basic scenario I have in mind concerns Canadian data that is situated within the United States. By "Canadian data" I mean personal information concerning a Canadian citizen or resident; and by "situated within the United States" I mean that it either transits or is stored within the geographical boundaries of the United States. Given basic technological and economic facts regarding the infrastructure of the internet in North America, this is the more likely factual scenario than U.S. data transiting or being stored within Canada. The key factual point is that while the data is within the United States, the person remains within Canada and so, from the U.S. perspective, is a nonresident alien. As I outline below, in such a situation the constitutional norms of *neither* state apply: these communications fall into a constitutional black hole.

The argument for why Canadian constitutional norms do not apply in such a scenario is that this would be an impermissible extraterritorial application of the *Charter*. The application of the *Charter* is objectionable when it intrudes

---

Evolution of Territoriality in American Law (2009). As Raustiala has outlined, post 9/11 the United States was engaged in "a significant effort to keep what was perceived as critical intelligence gathering and detention outside the reach of American law. The favourable precedents under U.S. law with regard to the extraterritorial rights of aliens provided a strong inducement to move as much counterterrorism as possible offshore." *Id.* at 207. This included the highly criticized attempts to relocate detention and interrogation through Guantanamo Bay and extraordinary rendition.

upon the state sovereignty of a foreign territory.[56] Because of this, the *Charter* does not apply to legal proceedings in foreign countries, or to the actions of foreign officers. Nor does it apply to actions of foreign officers taken pursuant to a request from Canadian authorities, because to impose *Charter* standards on these officers would interfere with U.S. state sovereignty.[57]

The *Charter* can sometimes apply to the actions of Canadian authorities within foreign territories. For example, in *Cook* the Supreme Court of Canada held that the *Charter* applies when Canadian police officers interview a suspect arrested and detained in the United States on the basis of an extradition request made by Canadian authorities. The fact that the offence was committed in Canada and was to be prosecuted in Canada, and that the interview was conducted solely by Canadian officers pursuant to their investigatory powers, was central to finding no objectionable extraterritorial effect.[58]

However, the search and seizure context is one where the Canadian Supreme Court has repeatedly denied the extraterritorial application of the *Charter*, even when applied to Canadian authorities. For example, in *Schrieber*, the Supreme Court held that the *Charter* did not apply to a Canadian request for assistance from Swiss authorities in relation to a Canadian criminal investigation.[59] The question was whether Canadian standards regarding the issuing of a search warrant had to be met before sending a letter of request to the Swiss government if Swiss authorities were the ones to seize the banking documents and records. A majority of the Court said no. More recently, in *R. v. Hape* the Supreme Court indicated that Canadian law never applies to extraterritorial searches and seizures.[60] According to Justice LeBel, for the majority:

> Searches and seizures, because of their coerciveness and intrusiveness, are by nature vastly different from police interrogations. The power to invade the private sphere of persons and property, and seize personal items and information, is paradigmatic of state sovereignty. These actions can be authorized only by the territorial state. From a theoretical standpoint, the *Charter* cannot be applied because its application would necessarily entail an exercise of the enforcement jurisdiction that lies at the heart of territoriality. As a result of the principles of sovereign

56 R. v. Cook, [1998] 2 S.C.R. 597 (Can.)
57 *See* R. v. Terry, [1996] 2 S.C.R. 207, ¶ 19 (Can.).
58 *Cook*, [1998] 2 S.C.R. at 628.
59 Schreiber v. Canada (Att. Gen.), [1998] 1 S.C.R. 841 (Can.).
60 R. v. Hape, [2007] S.C.C. 26 (Can.).

> equality, non-intervention and comity, Canadian law and standards cannot apply to searches and seizures conducted in another state's territory.[61]

The *Charter* could come into play when dealing with fair trial considerations. However, according to Justice LeBel, a search in a foreign territory that if undertaken in Canada would violate the *Charter* is unlikely to trigger a *Charter* remedy.[62]

In sum, then, the Canadian Supreme Court has held that the *Charter* has no application to a search or seizure undertaken in a foreign territory, has no application to a Canadian request that foreign authorities initiate a search in a foreign territory, and most likely will not trigger a *Charter* remedy at trial if a search or seizure undertaken in a foreign territory is not *Charter* compliant.

This leaves the search or seizure of Canadian data situated within the United States to be dealt with according to U.S. constitutional norms. The leading U.S. Supreme Court decision on extraterritoriality in the search and seizure context is the 1990 decision *Verdugo-Urquidez*.[63] It concerned the question of whether the Fourth Amendment applied to the search of the Mexican residence of a Mexican citizen who had been apprehended by Mexican police and transported to the United States, where he was arrested for drug smuggling. The U.S. Supreme Court held that the Fourth Amendment did not apply to aliens in foreign territory (although Mr. Verdugo-Urquidez was actually in U.S. custody within the United States at the time of the search).

Although *Verdugo-Urquidez* concerned a search in a foreign territory, it is taken to stand for the proposition that the Fourth Amendment does not apply to nonresident aliens, even if the impugned government activity is *within* U.S. territory. This unquestioned interpretation is itself notable. For example, both the Privacy and Civil Liberties Oversight Board (PCLOB) and the President's Review Group, who reviewed surveillance programs like the notorious PRISM program which involved NSA access to information stored by U.S. communications intermediaries, endorsed this interpretation. The legal authority for the PRISM program was section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA), added by the 2008 FISA Amendments Act, which treats non-U.S. persons differently from U.S. persons.[64] According to the PCLOB, this differential treatment does not raise constitutional concerns since "foreigners located outside of the United States" lack Fourth Amendment

---

61 *Id.* ¶ 87.

62 *Id.* ¶ 91.

63 United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

64 FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2463 (current section 702 of FISA is codified in 50 U.S.C. § 1881a (2012)).

rights.[65] Similarly, the President's Review Group argued that the *Verdugo-Urquidez* case is a "definitive" answer to the question of whether section 702, to the extent that it concerns non-U.S. persons located outside of the United States, violates the Fourth Amendment. The answer is "no," because such non-U.S. persons have no Fourth Amendment rights.[66]

If we put the Canadian and U.S. positions together, and contemplate what they mean in relation to the global internet, several conclusions can be drawn. First, if communications data is within U.S. territory but the person to whom the data relates is a nonresident alien, then the U.S. Fourth Amendment will not apply. Therefore, the United States can collect those communications on lower standards than it would have to apply to citizens or residents. Second, if Canadian authorities want access to those communications then the Canadian *Charter* does not apply. If authorities request that information then, as in *Schreiber*, there are no constitutional restraints on that request and only U.S. legal standards apply.

In this way, Canadian authorities can get access to data collected within another jurisdiction on standards that, if applied *within* Canada, would be unconstitutional. This is not a circumvention of Canadian law at all because the issue is not about applying the law within Canada, but the extent to which Canadian norms apply *outside* of Canada. Canadian authorities are legally permitted to get access to this data in foreign territory in situations where *Charter* norms do not apply. Moreover, U.S. authorities can get access to this data on standards that would be unconstitutional within Canada (according to Canadian constitutional norms) and also unconstitutional if applied to U.S. persons within the United States (according to U.S. constitutional norms). The information falls within a constitutional black hole.

This situation can generate some very absurd consequences in some factual contexts. Even when Canadian authorities are asserting jurisdiction over people within Canada regarding crimes committed within Canada, which are to be tried within Canada, and are in no way engaged in cooperating in transborder criminal investigations, the *Charter* does not constrain their access to Canadian data transiting or stored within the United States. It is one thing to say the *Charter* does not apply in relation to the search or seizure of banking or other business records where an individual has deliberately chosen to do business in another country partly in order to take advantage of foreign

---

65 Privacy & Civil Liberties Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 86 (2014) (citing *Verdugo-Urquidez*, 494 U.S.).

66 President's Review Grp., Liberty and Security in a Changing World 151 (2013).

laws; it is quite another when the jurisdictional split between data and bodies applies to a large number of people within the country, most of whom have no idea of either the technological or legal consequences of their use of the services of communications intermediaries.

C. Closing Gaps, Creating Sinkholes

If such black holes are created through the jurisdictional split between bodies and data, combined with the application of domestic norms premised on the location of either bodies or data, then there are two main options to close such holes: we can close the jurisdictional division of bodies and data or we can end differential legal treatment by treating the privacy rights of all people in the same way no matter where their bodies or their data are located. What might this look like?

The question really comes down to how to treat the significance of national political community in the context of the global internet. While the report of the President's Review Group provides one of the most striking defenses of the status quo, it also points to a number of ways to close the gap between bodies and data.[67] The President's Review Group defended the differential treatment of non-U.S. persons by appealing to the idea of political community. According to the Review Group, the "driving force" behind the original enactment of FISA was to protect Americans against the manipulation of "domestic political activity in a manner that threatened to undermine the core processes of American democracy."[68] The idea is that "persons who participate directly in its own system of self-governance" require *special* protection from surveillance from that government.[69] In other words, citizens and residents are given extra protection that non-U.S. persons do not require. Indeed, by preserving the United States' own democracy through such special protections, this even contributes "to sustaining democratic ideals abroad."[70]

There is merit to this argument, but it is dangerous when it ignores two things: whether the data of non-U.S. persons receives an adequate level of protection, and the special concerns of non-U.S. persons in relation to the exercise of U.S. power against them. This is particularly important in the context of antiterrorism efforts and the U.S. exploitation of extraterritoriality, where concerns about government abuse in relation to non-nationals has repeatedly arisen. Both the increased assertion of the extraterritoriality of U.S. law and

---

67 *Id.*
68 *Id.* at 154.
69 *Id.*
70 *Id.*

the denial of the extraterritorial application of the U.S. Constitution have together formed a part of the U.S. strategy to "offshore" counterterrorism efforts, playing a key role in setting up bases like Guantanamo Bay and also in relation to extraordinary rendition practices.[71] Indeed, one of the most high-profile cases of extraordinary rendition involved a Canadian — Maher Arar. Due to problematic information-sharing practices between Canadian and U.S. authorities, Maher Arar was detained in the United States by U.S. authorities while transiting through a U.S. airport and sent to Syria, where he was tortured.[72] Examples like these make the President's Review Group's focus on domestic abuse by governments, and its claims that this promotes democracy, ring hollow.

Nonetheless, a focus on the relevance of political community is helpful to understanding the basic contours of options to close the jurisdictional gap between bodies and data. The first way is to apply the protections of the political community of the person in question to the data.[73] For example, if a Canadian remains within Canada but their data is within the United States then Canadian constitutional constraints would apply to lawful access of this data. The second way is to apply the protections of the political community where the data resides to the data in question. In the same example, U.S. constitutional constraints would apply to lawful access of Canadian data. The final way to close the gap is to treat national political community as no longer relevant and to apply international norms to lawful access of the data in question. I briefly discuss each of these options and indicate why the first one is the most promising way to close constitutional black holes.

1. Political Community of the Person Is Primary

The first option is to treat the national political community of the person as primary and allow that person's data to receive the protective norms of that community. Indeed, Microsoft has recently proposed this in wake of the

---

71 Raustiala, *supra* note 55, at 207. This included the highly criticized attempts to relocate detention and interrogation through Guantanamo Bay and extraordinary rendition.

72 *The Unfinished Case of Maher Arar*, N.Y. Times (Feb. 17, 2009), http://www.nytimes.com/2009/02/18/opinion/18wed2.html?_r=2&ref=opinion; *see also* Comm'n of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Report of the Events Relating to Maher Arar: Analysis and Recommendations (2006).

73 The protections of the political community usually extend beyond citizens to include residents and others who might be considered to have the right kind of relationship. In this discussion I refer to citizens for the sake of simplicity.

collapse of the U.S.-EU Safe Harbor Agreement. According to a recent blog post by Microsoft's President and Chief Legal Officer, Brad Smith, we should ensure that "people's legal rights move with their data." If the United States wants access "to personal information that is stored in the United States and belongs to an EU national" then it can only do so in conformity with EU law.[74]

In some ways, this position would in fact better reflect the facts of *Verdugo-Urquidez* than the idea that no national political norms apply. On the facts of *Verdugo-Urquidez*, even though the Fourth Amendment did not apply to the search in Mexico, *Mexican* law did apply. Mexican law applied to the Mexican authorities and the U.S. authorities acted with the cooperation and authorization of Mexican authorities. Maintaining this understanding of constitutional constraints in the context of the global internet, where bodies and data are often in different jurisdictions, means that we have to treat lawful access to data as if it occurred within the national jurisdiction of the person to whom it pertains, subject to the constitutional constraints of their own political community. So, on this model of one's own law following one's data, if U.S. authorities want access to Canadian data stored within the United States, they should only do this with the cooperation of Canadian authorities within the terms of Canadian law. A revised Mutual Legal Assistance Treaty (MLAT) process could accomplish this, for when U.S. authorities seek assistance from Canadian authorities through the MLAT process, Canadian constitutional norms apply.[75] How the MLAT process could be revised to deal with legitimate concerns regarding delays, and the relative roles of intermediaries and authorities, would all have to be worked out and the details are not trivial.

There are three virtues to this proposal. First, it avoids the situation of commercial decisions that are opaque to individual consumers and prevent them from determining the constitutional level of privacy protection that they receive. People can choose their service and platform providers based on price and features and still be protected by their own political community when it comes to the question of lawful access. For example, this would give Canadians greater protection than the U.S. Fourth Amendment affords, given the fact that Canadian constitutional privacy norms are stronger than American ones.

---

74 Brad Smith, *The Collapse of the US-EU Safe Harbor: Solving the New Privacy Rubik's Cube*, EU Pol'y Blog (Oct. 20, 2015), http://blogs.microsoft.com/eupolicy/2015/10/20/the-collapse-of-the-u-s-eu-safe-harbor-solving-the-new-privacy-rubiks-cube/.

75 Peter Swire & Justin Hemmings, *Stakeholders in Reform of the Global System for Mutual Legal Assistance* (Georgia Tech Scheller College of Bus., Working Paper Series, Working Paper No. 2015-32, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2696163.

The second virtue to this proposal is that it is consistent with some of the underlying concerns animating the community arguments against extraterritorial application of constitutional norms. Subject to some of the concerns I discuss shortly below, there is something unique to the relationship between the state and the people it governs and who make up its political community. However, that unique relationship does not imply that a state can get access to the information of nonresident aliens on any standard it chooses. Rather, it should dictate a reciprocal respect for the political community of nonresident aliens. *This* is the way to foster respect for democratic ideals internationally.

The third virtue of this proposal is that it is consistent with the way in which people experience the internet; it is a better phenomenological fit. People do not think of their information traversing various geographies and jurisdictions — they simply act and interact "online." Even when they click "I agree" to various agreements that might have them consent to having their data stored in a number of different jurisdictions, most people are only vaguely aware of this, at best. We still experience ourselves as within our home legal jurisdiction, despite our data traversing and residing in the "cloud."

There are two main objections to this proposal. The first is practical: how would anyone know the nationality of the person to whom the data pertains? Whether this is feasible or not depends upon the underlying practices of communications intermediaries and whether they are willing to design their technology and business practices in a way to make this feasible. Take a fairly straightforward example — an enterprise-level client who wants to use U.S.-based cloud services for eCommunications. If these communications use end-to-end encryption then the way for authorities to get access to them is either through the client or through the communications intermediary, and both of these would be able to determine nationality.

Another serious objection to this proposal is that it looks like it involves interfering with state sovereignty. In the example given, data could be within U.S. territory but U.S. authorities would not be able to access it according to the standards set out in U.S. law. This is why the implementation of this proposal would require multilateral treaties where states agreed to the process outlined.

2. Political Community Where the Data Resides Is Primary

A different way to close the jurisdictional gap between bodies and data is to treat the political community where the data resides as primary and apply its constitutional constraints to lawful access to the data without regard to the fact that the person the data concerns is in another jurisdiction. This would mean that when a Canadian remains within Canada but their data is within the United States then U.S. law would treat the situation *as if* the Canadian

was also physically present within the United States. Another way to put it is that U.S. law would treat the fact that the data pertains to a nonresident alien as irrelevant. This would mean that the U.S. Fourth Amendment would apply to any search or seizure of the data.

This is actually a possible, although unlikely, interpretation of *Verdugo-Urquidez*. The major factual difference between *Verdugo-Urquidez* and the situation when bodies and data are in different jurisdictions is that in the latter case the search (or seizure) takes place within U.S. territory. The question therefore is the extent to which the result in *Verdugo-Urquidez* is driven by the extraterritoriality of the search itself (the search was in Mexico) or by the fact that Mr. Verdugo-Urquidez was a nonresident alien. If it is the former, then this case is of questionable authority for the proposition that the search or seizure *within the United States* of the data of nonresident aliens is not subject to the Fourth Amendment.

Justice Renquist wrote the decision of the court (joined by Justices White, O'Connor and Scalia) and stressed that the Fourth Amendment protects "the people," which refers "to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."[76] This suggests that the most important fact is not the extraterritoriality of the search, but that the search concerns a nonresident alien. However, Justices Kennedy and Stevens wrote separate concurring judgements that focused on the extraterritoriality of the search. Justice Kennedy went so far as to say that "[i]f the search had occurred in a residence within the United States, I have little doubt that the full protections of the Fourth Amendment would apply."[77] Moreover, Justices Brennan (with Justice Marshall joining) and Blackman, in separate dissents, argued that the Fourth Amendment should apply to nonresident aliens when the United States investigates and seeks to hold them accountable under U.S. law. If we put together the two dissenting opinions with the two concurring opinions, we have five justices who either are prepared to find that the Fourth Amendment applies to nonresident aliens when they are subject to domestic U.S. criminal law, or that the lack of application depends upon the fact that the search in question took place in a foreign jurisdiction. It is only four justices who explicitly agree with the "community" argument, which is the argument that provides the strongest basis for the proposition that the Fourth Amendment does not apply to domestic searches or seizures of nonresident alien data.

That said, there would likely be strong opposition in the United States to extending Fourth Amendment protection in this way, given the ease with

---

76 United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990).

77 *Id.* at 278.

which people in other countries can make use of U.S.-based internet services. According to Orin Kerr, such an extension would alter the balance of Fourth Amendment rights:

> Anyone who feared or expected surveillance from the United States could use United States-based services strategically in order to obtain Fourth Amendment rights and limit US Government surveillance powers. As a practical matter, the US Government would be forced to satisfy the hurdles of Fourth Amendment protection all around the world.[78]

In contrast, the previous proposal that would allow a person's law to follow their data would only apply where there were multilateral treaties in place — so states could agree to the practice for allies and trading partners while maintaining their ability to treat other nationals differently.

Jennifer Daskal offers an interesting variant on this argument to extend Fourth Amendment protection. Instead of the universal approach, she argues for a "presumptive approach" where the Fourth Amendment presumptively applies "absent a determination that all parties to the communication are non-U.S. persons."[79] The problem with this proposal, from a non-U.S. perspective, is the same problem as with the proposal to simply extend the Fourth Amendment to everyone: this might result in a lower standard of protection than the individual's own political community would provide. For example, a Canadian person who gets either actual Fourth Amendment rights or de facto Fourth Amendment rights gets a lower level of constitutional protection than a Canadian person who is protected by the Canadian *Charter*, given the differences in privacy jurisprudence. The data would not fall within a constitutional *black* hole, but it would still fall into a *sink*hole with less protection.

One way to alleviate the depth of this sinkhole is to revisit the Canadian position concerning the extraterritoriality of the *Charter*, particularly with respect to its application to Canadian authorities. The approach needed is that advocated by Justice Iacobucci's dissent in *Schreiber*. He argued that if the actions of Canadian authorities in requesting foreign assistance did not attract *Charter* scrutiny, then the respondent's interest falls "between two stools."[80] It would fall between two stools because the respondent's privacy interest

---

78 Orin Kerr, *The Fourth Amendment and the Global Internet*, 67 Stan. L. Rev. 285, 307 (2015).

79 Daskal, *supra* note 51, at 386. This addresses the problem of U.S. persons whose communications might be collected without Fourth Amendment protections if the person they communicate with is a non-U.S. person, and it provides more de facto protection to non-U.S. persons because where nationality is unclear, the Fourth Amendment applies.

80 Schreiber v. Canada (Att. Gen.), [1998] 1 S.C.R. 841, ¶ 58 (Can.).

would not be protected under Swiss law (there was no assurance of judicial preauthorization) or Canadian law. According to Justice Iacobucci, applying the *Charter* to the letter of request does not involve an extraterritorial application of the *Charter*, as the actual search and seizure would still be carried out under Swiss law.[81] This is a better approach than the one adopted by the Court in *Hape*.[82] The mistake in *Hape* seems to be the idea that if Canadians receive Canadian authorization for a search this means somehow that a court is giving permission for the search to take place within the foreign territory — something that it cannot do. But we could instead understand the court to authorize Canadians to participate in the search on the understanding that the search will have to take place with the additional permission of foreign authorities under foreign law. The basic point is that Canadian authorities should only initiate such a search where they can meet Canadian standards, even though foreign authorities are not required to meet those standards. However, this would only alleviate the sinkhole insofar as Canadian authorities are involved in initiating the search and would leave it in place in other circumstances.

3. National Political Community Is Irrelevant, International Norms Should Apply

The final option for eradicating the constitutional black hole is to insist that communications data be subject to the same privacy norms no matter where the data is located or the nationality of the person concerned. An example of such a strategy would be to look to international human rights norms to fill in the gap.[83] In other words, the strategy is to bypass the relevance of national political community in favor of international norms.

However, there are two main problems with invoking international human rights as a solution. The first is that the substantive international norms might not be as strong as domestic constitutional norms. Then we could have a situation where, for example, Canadian data stored in Canada would be subject to Canadian constitutional norms but Canadian data stored in the United States would only be subject to the weaker international baseline. While no longer a black hole, it remains a sinkhole.

The second problem is that the issue of the jurisdictional split between data and bodies can be replicated, albeit in a new form, with respect to

---

81 *Id.* ¶ 59.

82 R. v. Hape, [2007] S.C.C. 26 (Can.).

83 The Canadian Supreme Court has held that even though the Charter does not constrain Canadian officers' participation in cooperation with transborder criminal investigations, principles of international law and human rights might. *See id.* ¶ 90.

international human rights norms. One version of this arises because even though international human rights norms apply to all individuals, there is still a question of when a particular state has an obligation in relation to a particular individual. For example, Article 2(1) of the International Covenant on Civil and Political Rights (ICCPR) provides that "[e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant."[84] The U.S. position is that there is no extraterritorial application of the ICCPR and that it only applies to individuals who are *both* within U.S. territory *and* subject to U.S. jurisdiction.[85] The UN Human Rights Committee has disagreed with this position, arguing that "a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party."[86] However, even this latter test would still seem to apply to persons — whether they are in the power or effective control of a state — and not to their data. In other words, it remains an open question as to how international human rights might apply to the situation where data and persons are in different places.[87]

Another version of the problem arises if the substantive international norms might still accept differences based on either geography or nationality that could still be exploited given the global nature of communications. That is, human rights might establish a baseline but also might accept that extra protections above that baseline are justified for citizens and residents of a state but not nonresidents. For example, in the United Kingdom it was recently held that treating the collection of "internal" and "external" communications on different standards, as are found in the Regulation of Investigatory Powers Act,[88] is not a violation of the European Convention on Human Rights (ECHR).[89] External

---

84 International Covenant on Civil and Political Rights, art. 2(1), Dec. 16, 1966, 999 U.N.T.S. 171.

85 Beth Van Schaack, *The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now Is the Time for Change*, 90 Int'l L. Stud. 20 (2014).

86 Human Rights Comm., General Comment 31 ¶ 10, U.N. Doc. A/59/40 (2004).

87 *See* Am. Civil Liberties Union, Informational Privacy in the Digital Age (2015), http://www.ncbi.nlm.nih.gov/pubmed/23682396; Daniel Joyce, *Privacy in the Digital Era: Human Rights Online?*, 16 Melb. J. Int'l L. 270 (2015); Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 Harv. Int'l L.J. 81 (2015).

88 Regulation of Investigatory Powers Act 2000, c. 23.

89 Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November

communications, defined as those that are sent or received outside of the British Islands, can be intercepted on a general, or untargeted warrant, rather than a targeted warrant and these warrants are not issued by a judge.[90] These general warrants did not violate the ECHR. Moreover, the fact that people located within the United Kingdom received additional safeguards regarding their communications that were intercepted under these general warrants than people living outside of the United Kingdom was not discriminatory and in violation of Article 14 of the Convention.[91] The worry is that instead of helping to close the legal loopholes that are exploited to collect information on low standards, international human rights norms could be made to be complicit in replicating these loopholes.

4. The State Alone Cannot Protect National Political Community

The best solution for actually closing, and preventing, the kind of constitutional black hole described in this Article is the first one discussed in Subsection II.C.1. above — the protections afforded by a person's political community should follow their data wherever it happens to be located. This solution is the one that best preserves the relevance of one's national political community. The interesting thing about this solution, however, is that it is not one that can be implemented by any particular state government. Instead, it depends upon both international agreements and the willingness of communications intermediaries to develop their technical architecture and business practices in such a way as to make this solution feasible. In this way, the future effectiveness of state-based constitutionalism as applied to communications depends upon both the private and international spheres.

Conclusion

The new public/private nexus for lawful access in the Information State involves two community displacements — the displacement of civic community and the displacement of national political community. Both of these displacements involve the erosion of both formal and informal constitutional constraints on lawful access. However, as this Article has tried to outline through various examples, we can neither understand the erosion of these constraints nor pose solutions by focusing on traditional public or private regulatory models.

1950, ETS 5; *see* Liberty v. United Kingdom, [2104] UKIPTrib13_77-H (U.K.), http://www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

90 *Liberty*, [2014] UKIPTrib13_77-H ¶ 65.

91 *Id.* ¶ 148.

Balkin has argued that we cannot simply think about information policy in terms of individual rights, but have to also think about institutions, technological design, and infrastructure.[92] Moreover, "knowledge and information policy . . . is increasingly the product of coordination between state power and private power."[93] Balkin focuses much of his attention on free expression and the infrastructure that might support it. However, we must also attend to the reality that many of our "actions" now are mediated through online communicative acts. This is the way in which we assemble, organize, discuss, research, and engage in many more mundane daily tasks. We can absorb these actions into "speech" and think about them through the rubric of freedom of expression, or we can seek ways to understand more fully the relationship between communication and what might in other times have been actions categorized under separate rights and freedoms. But even more than understanding the role of communications in relation to various entrenched constitutional rights, we need to understand the special role that communications have in relation to more basic rule of law concerns. For example, Lon Fuller, who outlined a very influential theory of procedural rule of law norms, wrote:

> If I were asked . . . to discern one central indisputable principle of what may be called substantive natural law — Natural Law with capital letters — I would find it in the injunction: Open up, maintain, and preserve the integrity of channels of communication by which men convey to one another the way they perceive, feel, and desire.[94]

Communication, he argued, is "the principle that supports and infuses all human aspiration."

Ultimately what we need is to look at information and communications systems and not just specific practices, and we need to do so from the perspective of fostering trust in these systems. We need to do so in a manner that is sensitive to shifting power dynamics in the Information State, that is skeptical of claims to update law based on old paradigms, and that is rooted in an appreciation of the centrality of communications to human life.

---

92 Jack Balkin, *The First Amendment Is an Information Policy*, 41 Hofstra L. Rev. 1 (2012).

93 *Id.* at 8.

94 Lon Fuller, The Morality of Law 186 (rev. ed. 1969).