Telecom Responsibilization: Internet Governance, Surveillance, and New Roles for Intermediaries

Mike Zajko
University of Alberta

ABSTRACT This article foregrounds internet intermediaries as a class of actors central to many governance and surveillance strategies, and provides an overview of their emerging roles and responsibilities. While the growth of the internet has created challenges for state actors, state priorities have been unfolded onto the private institutions that provide many of the internet’s services. This article elaborates responsibilization strategies implicating internet intermediaries, and the goals that these actors can be aligned toward. These include enrolling telecom service providers in law enforcement and national security-oriented surveillance programs, as well as strategies to responsibilize service providers as copyright enforcers. But state interests are also responsive to pressures from civil society, so that “internet values” are increasingly channelled through the formal political processes shaping internet governance.

KEYWORDS Internet governance; Telecommunications policy; Surveillance; Copyright; Political theory

Introduction
Since Edward Snowden helped set off a cascade of reporting and debate in 2013 when he leaked classified information from the U.S. National Security Agency (NSA), many of us have been wondering about the institutions that we rely upon to communicate.
The companies behind our devices and online services connect us to one another, provide us with content, and facilitate transactions, but what other roles do they play? Do they spy on us, or guard our private information? What are their obligations, and to whom? All of this is just the latest and most explosive reminder of a gradual reconfiguration that has elevated communications service providers to a privileged relationship with their users. At the same time, state agencies have come to terms with the internet. In asserting themselves, they have demonstrated just where the “points of control” (Zittrain, 2003) in a digital society lie, as well as the continuing importance of territory in an era of transnational communication.

Through the territoriality and sovereign state power the internet was once thought to elide, authoritarian nations now have their authoritarian internets, and liberal democracies are struggling with old questions over the proper scope of surveillance, order, and policing transposed to the digital domain. A defining feature of the exercise of state power over digital networks has been the necessity of enrolling private institutions that own and operate the communications infrastructure and provide its services. This mode of governance is not without precedent, but its configuration is particular to today’s digital networks. It targets the key nodal institutions and draws on their newly elevated capacities. These institutions are the internet service providers (ISPs) and online service providers (OSPs), frequently referred to as “intermediaries.” Intermediaries are becoming increasingly important both as actors and sites of control. The relationships between intermediaries and those working to govern through them can be understood as forms of “responsibleization,” wherein one group of actors is asked or compelled by another to assist in a particular strategy. I will differentiate between three forms of responsibleization: the “unfolding” of state priorities onto intermediaries, an “enfolding” of the goals of non-state actors into the process of responsibleization (in which the mechanisms of state power are leveraged by non-state actors), and a private form of responsibleization that can operate without the need for state involvement. This article foregrounds internet intermediaries and their growing engagement in contemporary governance. It provides a synthetic overview of the governmental dynamics involved in shaping these intermediaries’ roles, and distinguishes strategies of responsibleization currently underway.

Nodal governance around the net

According to Tim Wu (2010), we should conceive of ongoing developments in the governance of the internet as part of a historical cycle through which a new communications medium passes from an open phase with little effective governance, to one that is increasingly controlled by a small number of actors. Although much of the cyber-optimism of the 1990s has now faded, it remains possible to argue that the internet is different enough from its media predecessors to resist this consolidating trend. However, the “founding myth” of the internet as a non-hierarchical network that routes around censorship must be tempered by an understanding of how vulnerable internet architecture is to control at particular points (Deibert & Rohozinski, 2010; DeNardis, 2014; Zittrain, 2003) or “organizational bottlenecks” (Mueller, 2010), which are occupied and operated by intermediaries (ISPs and OSPs).
These points of control and the internet intermediaries that operate them are a diverse category, inclusive of undersea cable operators, search engines, and social networking sites. This internet infrastructure can be “physical,” “virtual,” or some combination of the two (DeNardis, 2014, p.11). ISPs act as bottlenecks because they control the physical infrastructure that connects individuals to the global internet. OSPs can be gatekeepers to valuable online resources, such as those provided by Google and Facebook. However, the distinction between infrastructure-based ISPs and online services is often blurry, with ISPs hosting content, and OSPs maintaining vast physical infrastructures (Edwards, 2011, pp. 4–5). What these intermediaries have in common is the ability to monitor and control information flows by virtue of their strategic position. Consequently, these diverse intermediaries are often subject to the same regulatory regimes and sets of responsibilities (see Edwards, 2011).

Intermediaries are primarily defined by their role as conduits for users, whether they conduct data packets in the case of ISPs, currency in the case of online payment providers, or access to an organized Web in the case of search engines. Typically, intermediaries also engage in some form of gatekeeping by restricting or regulating access. As components of the internet, they are susceptible to control by others. However, as institutions, these intermediaries are actors in their own right, as they enter into or contest relationships with other actors. While the corporate giants of the internet, such as Google and Facebook, are private actors that exercise considerable regulatory independence over their domains, many states are pursuing varying forms and degrees of internet governance, and asserting their sovereignty even over and against such “internet sovereigns” (see Deibert, Palfrey, Rohozinski, & Zittrain, 2012, p. 17; MacKinnon, 2012).

Jack Goldsmith and Tim Wu (2006) have documented “the Internet’s transformation from a technology that resists territorial law to one that facilitates its enforcement” (p. 10), and Ronald Deibert and Rafal Rohozinski (2010) have argued that “securing cyberspace has definitely entailed a ‘return of the state’ ... [although] not in ways that suggest a return to the traditional Westphalian paradigm of state sovereignty” (p. 30). Numerous states around the world are developing and refining the exercise of state power through the internet by way of surveillance and content filtering. Where such strategies differ from the traditional exercise of state sovereignty is through the importance placed on responsibilizing private actors. To the extent that private actors dominate much of the telecom infrastructure, including key network nodes where surveillance and control are most effective, their cooperation with state strategies becomes crucially important (Deibert et al., 2012). Furthermore, as the uses of our networks multiply, and as internet-based threats and pathologies gain more attention, intermediaries become seen as the instrument for a diverse array of governance strategies.

ISPs and OSPs have been enlisted as guardians of public morality, national security, and our individual privacy. Since the internet became available to the public in the mid-1990s we have seen proposals and legal efforts in numerous countries to make intermediaries responsible for controlling pornography, racist materials, blasphemy, defamation, cyber-bullying, “anti-social” speech, and intellectual property rights (Frydman & Rorive, 2002; OpenNet Initiative, n.d.). ISPs are now envisioned as being on the front lines of cyber conflicts, with the capacity to play defence against interna-
tional threats—if only we could agree on an appropriate set of responsibilities for them (Greenberg, 2010). Tellingly, in the wake of the Snowden disclosures in the U.S., President Obama tried to reform one of the most controversial mass surveillance programs of the National Security Agency (NSA) by transferring some of the responsibility for maintaining it to private telecom companies (Obama, 2014). The logic of such an approach seems to be that a loss of trust in government agencies can be addressed by making intermediaries more responsible as stewards of our personal information.

Intermediaries can conceivably govern communications toward the various ends listed above, but this does not mean all such proposals are practical or effective. In reality, intermediaries are far better suited for some responsibilities than others. For example, a great deal of surveillance capability is already embedded in the operations of ISPs and OSPs, which have their own reasons for monitoring how their services are being used. This makes it relatively straightforward to task these intermediaries with collecting, intercepting, or forwarding certain kinds of data. In contrast, determining what constitutes an infringement of copyright or a defamatory statement is effectively a judicial responsibility, and delegating this judgment to intermediaries creates enormous challenges and burdens.

The vision of social order that intermediaries are enlisted to serve varies according to territory, but the difficulties of governing the internet have led both liberal and authoritarian states to pursue responsibilization as a strategy. However, the main focus of this article will be on responsibilization as a strategy of liberal governance, which presumes both state sovereignty and a civil society “outside” the state (Dean, 2007). How these two domains are interlaced calls our attention to the formal political sphere and its capacities for governing a society that is permeable by state power. Conversely, it also shows the permeability of formal politics and the state in the liberal order, which leaves the door open to dramatic episodes of contention over appropriate forms of governance.

**Responsibilization of internet intermediaries as an extension of state power**

This analysis is based on a theory of the state derived from Mitchell Dean (2007), who builds on and extends the work of Michel Foucault. Many have cited Foucault as doing away with privileged notions of state power in political theory, and his writings have inspired scholars to examine the myriad “networks” of power relations and non-state actors involved in contemporary governance. However, Dean (2007) is critical of this trend away from “hoary old ideas of politics and territorial states to a cultural and network form of government” (p. 14). Instead, he argues that the challenge for social theory is to rethink and “recover” sovereignty, but in a way that incorporates Foucault’s insights about multiple and heterogeneous forms of power. The picture of the territorial state that results from Dean’s (2007) analysis is that of “a fragile and precarious achievement” (p. 55), produced and shaped by a multiplicity of forces, and governing through or alongside non-state institutions. In liberal societies, government is expected to operate through semi-autonomous domains external to the state, such as “the economy” or “civil society” (Dean, 2007, p. 98). Yet, this liberal political order presumes the existence of territorially bounded sovereign power. This sovereign power can be
derogated, delegated to non-state actors, or contested, but its effectiveness and supremacy is brought into stark relief on a regular basis, particularly when the state addresses threats to society or national security (Dean, 2007, pp. 105–106).

Under the logic of liberal “governmentality,” responsibilization is an appealing strategy because it minimizes direct interventions by the state, drawing instead on the governing capacities of non-state actors, and aligning them with state goals. Many discussions of responsibilization have presented it as an aspect of neoliberal governance, corresponding with the devolution of state responsibilities and regulatory powers onto private actors (Burchell, 1996). But responsibilization need not be the result of a shrinking neoliberal state handing over powers and responsibilities to the private sector. Instead, we should appreciate how responsibilization has been used as a technique of governance to extend state power throughout society, by aligning its newly ascended points of control with the maintenance of a particular social order.

My argument that responsibilization can extend state power is similar to that made by David Garland (1996), who discusses responsibilization as an adaptive strategy of crime control compatible with increased regulation and a broader reach for state agencies. Responsibilization is not a way for the state to “pass the buck” to other actors, but encompasses “ways of acting at a distance, of activating the governmental powers of ‘private’ agencies, of co-ordinating interests and setting up chains of co-operative action” (Garland, 1996, p. 454). Keiji Uchimura (2005) has drawn on Garland’s (1996) work to discuss the responsibilization of telecom companies as a means of countering “cybercrime,” but we should understand that responsibilization can address many activities other than crime. Around the world, internet filtering targets a wide range of content, and internet surveillance programs can be even broader in scope. This kind of governance is in line with a more expansive, earlier notion of “police” that included concerns over morality, public order, political dissent, and trade (Dean, 2007). And indeed, while internet intermediaries are a relatively new class of actors with some unique responsibilities, we should not think there is something fundamentally new about responsibilization or the existence of close relationships between private telecom companies and state agencies.

As Dwayne Winseck and Robert Pike (2007) demonstrate in their account of the development of telecom networks in the late nineteenth and early twentieth centuries, the relationship between governments and private companies in the construction and regulation of telecom infrastructure has frequently included close cooperation, interdependence, and the interpenetration of actors and interests. Often, governments relied on (at least ostensibly) private companies to meet their surveillance and security needs (Winseck & Pike, 2007). The distinction between state and private actors has rarely been clear-cut, and intermediaries such as telecom companies and financial institutions have been enrolled in state surveillance programs long before the internet.

If intermediary responsibilization did not begin with the internet and is not just a consequence of neoliberalism, then what is its driver? Why have states as different as the U.K. and China turned to internet intermediaries to implement their respective visions of social order? The answer to these questions is relatively simple: while the governments of the U.K. and China may differ in the kinds of order they seek, the pro-
liferation and growing importance of digital networks in countries around the world entails a similar reconfiguration in the means of communication. This reconfiguration elevates internet intermediaries to a privileged position over digital records and digital flows. Governing these intermediaries then appears as the solution to both old and new problems.

A particularly new development has been the increasing integration and lack of distinction between our online and offline activities, and the level of detail at which these activities can be monitored. Steadily, as our economic transactions, social relationships, and media consumption acquire an online component, those who desire to monitor or control these activities look to where they can achieve the greatest access and influence. The capability of today’s mobile devices to locate their owners in time and space and to monitor their communications far exceeds the tools of twentieth-century tyrants (Deibert & Rohozinski, 2012). Social networking profiles includes personal information as well as an already mapped network of contacts. While sorting through the glut of available information is often given as a leading challenge facing today’s intelligence agencies, this glut also speaks to the ease of collecting volumes of personal data through our digital networks. The responsibilization of intermediaries to collect and provide access to this data constitutes a dramatic extension of state power, rather than simply a devolution of state responsibilities into private hands.

**Types of responsibilization: Unfolding, enfolding, and private**

Hereto responsibilization is treated as a fairly broad concept that can encompass a variety of practices and relationships. I will now differentiate three basic forms of responsibilization, as distinguished by the role of the state and its relation with civil society. The first is the sort of responsibilization that is initiated and directed by the state: unfolding state priorities onto private actors. Such “unfolding responsibilization” is based on conventional mechanisms of liberal rule, but its objectives are not determined by the demands of civil society. Unfolding responsibilization works to orient actors and networks toward goals such as national security, public order, moral governance, and crime control. It is achieved through legislation and sovereign violence, but may also involve moral suasion and associating national goals with patriotic and civic duty. For example, the “warrantless wiretapping” carried out by the NSA following 9/11 relied in large part on the voluntary cooperation of telecom companies. Rather than being compelled by law, these companies accepted legal risks in order to aid national security efforts (NSA, 2009).^5^)

In the second form of responsibilization, private actors are aligned with goals or priorities originating outside the state, but which have successfully shaped state interests and thereby leveraged the mechanisms of sovereignty. Such “enfolded responsibilization” is possible because of the permeability of the formal political sphere in liberal rule, so that the state is by no means the only possible origin or motivator of responsibilization. To the extent that mechanisms and apparatuses of the state are susceptible to the influence of private actors and institutions, the state can serve as a channel for interests that become enfolded as state priorities.^6^ Once this occurs, these interests can then be unfolded back upon civil society, promoting broad deployment through the weight of state power. The prime example of this kind of responsibilization
is copyright enforcement. Copyright owners have successfully lobbied states to impose copyright enforcement obligations on intermediaries, and even shaped the foreign policies of nations such as the U.S., which has pressured other nations to extend similar intermediary responsibilities (Mueller, 2010).

It is also possible to conceive a third type of responsibilization that effectively avoids the state-private sector nexus, and refers to how some private actors are able to responsibilize others directly. This includes some institutions’ ability to set standards in a particular field, or the ability of dominant actors to demand that their dependents behave in certain ways. Relevant examples of this type are the responsibilities that some ISPs expect from any networks wishing to interconnect with them, as specified in interconnection or “peering” agreements. These can require companies to manage spam or other “malicious” activity coming from customers (Norton, 2010). Larger, more established ISPs can bargain for exclusive and burdensome terms, as long as these do not violate responsibilities imposed on them by the state to promote competition (in many countries this includes an obligation for “incumbent” ISPs to provide wholesale internet access to smaller competitors). While this private form of responsibilization seems to elide the state, it more accurately indicates a particular relationship to the state—in which the state takes a “hands-off” approach to some aspects of internet governance.

What these three forms distinguish are three separate relationships between responsibilizing actors and the mechanisms of state power. In the first (unfolding), the state initiates responsibilization, while in the second (enfolding) the state becomes a channel and means of leverage for other responsibilizing actors. In the third, private responsibilization occurs outside of the formal political sphere but under conditions enabled by state power (or its restraint). State agencies unfold responsibilization when they desire to govern digital flows, but are incapable or unwilling to do so directly. Instead, they choose to govern the conduct of intermediaries toward this end. Enfolded responsibilization is attempted by private actors who also seek to govern these digital flows, but do not have an adequate basis for exerting influence over intermediaries. They must therefore mobilize state intervention to reconfigure intermediary responsibilities. When such efforts are blocked or face resistance, private responsibilization strategies may still be pursued, but these are unlikely to have much success unless intermediaries derive some benefit from compliance. Purely private responsibilization is most effective when both parties have something to gain. Otherwise, any expansion of intermediary responsibilities requires a credible threat of state intervention.

Table 1 summarizes the above-mentioned forms of responsibilization. Black arrows show responsibilization originating in the civil domain.

While private responsibilization may in time become more relevant, the continued effectiveness of state sovereignty means that responsibilization still occurs primarily through state power. The concept of responsibilization depends on one actor enrolling, devolving onto, or capturing another. This is not the most appropriate way to describe the loose and cooperative associations that define much of internet governance in its broader sense (Mueller, 2010). The internet’s coordination of standards, protocols, and strategies often arises out of the shared interests and concerns of its operators. Peering
agreements between ISPs are reciprocal, and bad actors that violate community norms can be excluded. Responsibilization, on the other hand, occurs when actors accept extrinsic responsibilities and modify their practices accordingly. They may be convinced or compelled to do so, and to bear the associated costs. State power includes mechanisms for such intervention, and is already oriented toward collective ambitions such as national security and public order. Because of this, it is the strategies of responsibilization that originate in or involve the state that currently require greatest attention.

Internet governance and liberal police

To better understand responsibilization we need to consider the dynamics of the forces involved. The differentiation between unfolding and enfolding given above is based in considerable part on Dean’s (2007) understanding of liberal governance and its attendant “liberal police.” Dean uses “police” to refer broadly to the maintenance of good order and administration. This is closer to the term’s earlier usage in cameralist police science (Polizeiwissenschaft), but liberal police is distinguished by its emphasis on techniques and agencies located in civil society. Rather than aspiring to a comprehensive set of regulations based on detailed knowledge, liberal rule restricts the role of state actors directly ensuring good order and encourages governance through non-state agencies. The resulting liberal police “is anchored in civil society and attempts to guarantee the security of its processes” (Dean, 2007, p. 113), but this diffusion enables rather than restricts its comprehensiveness. Furthermore, liberal rule remains quite compatible with authoritarian and despotic techniques of government, which it recurrently applies to social disorders, pathologies, and problem populations (Dean, 2007). In Dean’s (2007) political theory, sovereignty is “an aspiration, a more or less accomplished fact” (p. 140), but he is deeply skeptical of those heralding the decline of the sovereign state, or political analyses that deny the “extant operation” (p. 133) of sovereignty, with its links to violence and territory. This affirmation of both sovereignty and territory echoes an important lesson learned by many observers of internet governance in recent years. While transnational communication has never been easier, the institutions and material infrastructure that underpin it must respect borders and respond to local pressures (Goldsmith & Wu, 2006).

<table>
<thead>
<tr>
<th>Type of Responsibilization</th>
<th>Logic</th>
<th>Domain of Origin</th>
<th>Figure</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>State-Directed</td>
<td>Unfolding</td>
<td>State</td>
<td></td>
<td>Lawful Intercept</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mandated Filtering</td>
</tr>
<tr>
<td>State-Leveraged</td>
<td>Enfolding</td>
<td>Civil</td>
<td></td>
<td>Copyright Enforcement</td>
</tr>
<tr>
<td>Private</td>
<td>Bargaining</td>
<td>Civil</td>
<td></td>
<td>Internconnection Agreements</td>
</tr>
</tbody>
</table>
For Dean (2007), civil society serves as “a convenient shorthand for all that liberal government must take into account that is exterior to the formal governmental domain of the state” (p. 110), including private industry. Civil society and state governance become linked through liberal police, which “works by two distinct but related operations: an ‘unfolding’ of the (formally) political sphere into civil society and an ‘enfolding’ of the regulations of civil society into the political” (Dean, 2007, p. 116, see Figure 1). Responsibilization can thereby follow the logic of the state unfolding into civil society as a “joining up” of state and non-state actors. But responsibilization is also preceded by the enfolding of civil society into government, as a result of which the “values, expectations and conducts of civil society, real or ideal, form the means and objectives of governmental programmes” (Dean, 2007, p. 116). Since civil society encompasses a diverse terrain of values and interests, once a particular set becomes enfolded into formal politics, the state can unfold these interests and goals (through sovereign force if necessary) onto members of civil society that might not otherwise pursue them. The state therefore acts as a mechanism by which some techniques and values found in civil society are able to be deployed more broadly, allowing some members of civil society to responsibilize others.

Figure 1: Liberal government of internet intermediaries (adapted from Dean, 2007, p. 117)

While Dean’s (2007) argument concerns liberal governance, it retains a great deal of applicability to contemporary authoritarian or non-liberal states, as both must govern through a multiplicity of sites and forces beyond the direct control of authorities. This is not to suggest an equivalence between liberal and authoritarian states, but Dean helps us understand corresponding tendencies and pressures found in both. In general, modern governmental rationalities are concerned with the conditions of social and political
order. They presuppose a sovereign power that can determine what constitutes this order, and maintain it against threats or social pathologies (Dean, 2007). Authoritarian states may exercise greater autonomy and be less responsive to civil society, but the idea of a “total state” now seems to be little more than a North Korean fantasy.

Sovereignty represents an ongoing, and never finalized, accomplishment of supremacy, which can in turn be dispersed or delegated to various agents (Dean, 2007). This allows us to consider the multiplicity of sites involved in governance (and indeed the multiplicity of the state), as well as the contestation of sovereignty. There are numerous ways in which state sovereignty can be resisted or circumvented through the use of transnational networks, and any attentive analysis to the relationship between networks and states (see Mueller, 2010) must recognize these challenges to state power. It can be argued that I am overemphasizing the importance of state sovereignty in internet governance, given the internet’s overall decentralization and numerous failed attempts by state actors to exert effective control. The internet’s balkanization (Theurer, 2012) remains more of a fear than a description of reality, but it is a fear that has grown more plausible over time. As states debate the legitimate bounds of internet governance and their own role in a transnational order, the means of domestic internet control have been considerably refined and extended. No state has been able to achieve full domestic control over communications, but many have established effective regimes of governance.

Unfolding security and enfolding copyright
This article now outlines some examples to flesh out the distinctions provided in the preceding section, and elaborates the means through which the responsibilization of internet intermediaries frequently occurs. A description of some common ways in which relationships between state actors and telecom service providers are established, as examples of unfolding responsibilization. Such responsibilization aligns intermediaries with particular state-determined goals. It integrates privately operated networks into an unfolding security apparatus or “surveillant assemblage” (Haggerty & Ericson, 2000), and targets the most effective points for monitoring, control, and user identification. Unfolding responsibilization may be enforced through the coercive power of the law, but private actors can often be aligned with state goals in a largely voluntary manner. These goals and the state’s definition of “good order” can be intrinsic to the state and its preservation, but they can also include values enfolded from civil society. As a prime example of such enfolded responsibilization, recent efforts to responsibilize a variety of actors as part of the policing of copyright by the “content industries” (referring to mass media industry groups that are heavily invested in copyright) are discussed. These policing efforts remind us that the idea of state interests cannot easily be foreclosed, and that the state itself can become a porous and contested territory through which non-state actors seek to responsibilize one another.

Around the world, intermediaries are participating in a variety of state surveillance and control strategies (Deibert et al., 2012), some of which reflect longstanding state priorities that have been updated for the internet era. Historically, telephone system providers have been required to install capabilities to allow for police wiretaps, and such “lawful access” requirements are also being applied to ISPs (sometimes combined
with requirements to retain certain types of data). One prominent example is the 2007 extension of the U.S. Communications Assistance for Law Enforcement Act (CALEA) to cover ISPs. This makes U.S. ISPs responsible for maintaining the capability to facilitate police surveillance by having monitoring and data collection equipment installed, and dedicated staff to service government demands. Essentially, CALEA provides an “easy button” (Landau, 2010, p. 249) for government to push when a wiretap is required, and ISPs are responsible for ensuring the button works according to government needs. This responsibility can be further delegated or outsourced by the ISP to companies specializing in CALEA compliance (Federal Communications Commission, 2013).

State surveillance and internet filtering sometimes takes place at particular points of access, such as cybercafés, but the typical targets of surveillance are key network nodes operated by major ISPs (Roberts & Palfrey, 2010) and the high-capacity fibre optic cables of international carriers (Timberg & Nakashima, 2013). State-directed communications filtering and monitoring is sometimes required in order for an intermediary to operate within a territory, as established through either an explicit or informal agreement with the state. This allows for controls that can effectively be “scaled-up” with the internet, and takes advantage of the expertise of private network operators (see Mueller, 2010).

States can responsibilize internet intermediaries through different means, chief among which are regulations. These may be legislated through a formal political process or established through less formal agreements worked out between states and service providers as a condition of these corporations being granted a license (Timberg & Nakashima, 2013). Since telecom service providers are often transnational in scope, such state policies present them with a choice: either to participate as a responsibilized component of a state-directed surveillance and control strategy, or to lose access to a particular market. However, telecom service providers also willingly share access to their networks or subscriber information, in the absence of any clear requirement to do so. As a public debate raged in Canada in 2012 over proposed legislation that would allow police to obtain basic subscriber information from ISPs without a warrant, it was revealed that ISPs were already voluntarily complying with approximately 94 percent of such requests from federal police (Parsons, 2012).

Following 9/11 in the U.S., telecom employees were assigned to Federal Bureau of Investigation (FBI) offices where they proactively granted access to information, including proposing legal shortcuts, doing away with legal requirements altogether, and singling out leads for the FBI (Michaels, 2010). Appeals to patriotic duty and collective security appear to be particularly valuable ways of enrolling private actors in state surveillance (Michaels, 2010; Riley, 2013).

One particularly useful account of this sort of voluntary cooperation in the U.S. can be found in a leaked report by the NSA’s Inspector General (NSA, 2009), which describes cooperation between the NSA and telecom companies following 9/11. Two of these companies approached the NSA voluntarily with offers to help after the attacks, with one even drawing attention to “odd patterns” of communication in its records. Subsequently, the NSA began visiting a number of telecom company offices to enlist participation in what would become known as the President’s Surveillance
Program. Companies responded with varying degrees of cooperation. One company chose not to participate because of liability concerns, while another was declined participation when it wanted to seek outside legal counsel. Liability concerns continued over subsequent years, and the government attempted to provide adequate legal assurances for continued cooperation. At one point, the Director of National Intelligence sent three of the companies a letter underscoring the critical importance of their continued assistance in “protecting the country and the American people from terrorist attacks” (NSA, 2009, p. 32), showing the importance of moral suasion and patriotic duty in securing voluntary cooperation.

Cooperation between telecom providers and state surveillance efforts may violate domestic laws or leave providers liable to lawsuits, but the state can often grant legal immunity to assuage providers’ fears (Landau, 2010; Riley, 2013). Given the transnational nature of many telecom providers and the variety of laws they are therefore subject to, it is also possible for a company to comply with the law in one jurisdiction while making itself liable in another. For example, Yahoo’s lawful cooperation with Chinese authorities resulted in dissidents being jailed, who then sued the company in U.S. court (Mills, 2007). From these examples, it is clear that while laws provide a useful means for states to compel compliance from telecom companies, many such arrangements are extra-legal, and may even be illegal (see Fitsanakis, 2003).

To summarize, there are multiple reasons that telecom service providers might participate in state-directed surveillance or control strategies. Frequently, telecom service providers have little autonomy in terms of deciding whether to participate or not, short of refusing to deal with a particular state or pulling out of a market. However, even in situations where providers do maintain considerable autonomy, they have often facilitated state surveillance programs with significant degrees of access to their networks. The secrecy of such relationships, and the willingness of sovereign states to protect their private surveillance partners, means that many telecom providers seem perfectly willing to help states access the identities and communications of their users. Although some refuse or actively resist the state insofar as the law permits, the telecom industry is characterized by “strategic interdependence” (Jacobsen, 2009) between states and telecom providers. The interests of states and telecom providers may sometimes be at odds, but the two must deal with each other. As long as undue costs and risks related to state surveillance strategies are not incurred by telecom service providers, these private actors frequently assist state efforts to exploit the monitoring capabilities of the surveillant assemblage or to implement content controls. While the cascade of reporting and criticism that has followed Snowden’s disclosures has no doubt changed how these risks are perceived, it is still too early to tell how cooperation between state agencies and service providers will be affected by this particular breach of secrecy.

Historically, greater resistance to responsibilization has occurred when private intermediaries have been responsibilized to monitor and police copyright violations, since such actions not only impose costs, but can also challenge the telecom industry’s business model. In the examples of unfolding responsibilization discussed above, telecom service providers sometimes incur risks as a result of cooperating with state surveillance strategies, but these risks have historically been managed through secrecy
or not been perceived as significant enough to impede such relationships. In contrast, recent pushes toward responsibilization for copyright enforcement aim to impose both significant duties and liabilities (see de Beer & Clemmer, 2009; Edwards, 2011; Horten, 2012). While unfolding telecom responsibilization is often a strategy through which states seek to coordinate and extend the surveillant assemblage, surveillance is not the primary goal of enfolding copyright. Instead, surveillance can be a de facto consequence of the responsibilization of ISPs and OSPs, which suddenly become liable for the copyright-infringing actions of their users. Intermediaries may be explicitly required to monitor their users, but more commonly they are enlisted to help the content industries identify users that have already been deemed infringing. These users can then face lawsuits or have the services available to them restricted. Responsibilized intermediaries can also be required to act as gatekeepers and restrict the public’s access to infringing content.

While a range of national copyright strategies have been proposed and implemented, similarities among many of these approaches mean that it is possible to make some generalizations about such efforts. Of primary relevance to this article is the trend to responsibilize various intermediaries to participate in the policing of copyright-infringing users and content. Copyright regulations developed following the World Intellectual Property Organization (WIPO) internet treaties of the mid-1990s, including the U.S. Digital Millennium Copyright Act (DMCA) and the European Copyright Directive, which significantly limited intermediary responsibilities to police copyright infringement by users (WIPO, 2002). Monitoring the internet for copyright infringement and issuing notices of infringement to service providers was left to the content industries. Under the DMCA, for example, intermediaries are exempt from certain kinds of liability as long as they adhere to so-called “safe harbour” provisions. Similar liability exemptions in other jurisdictions include those applied to “mere conduits” under EU law, and “common carriers” in Canada. These exemptions protect companies as long as they do not step beyond a circumscribed intermediary function (e.g., by becoming content providers).

But following its enactment, the DMCA became increasingly used to pressure intermediaries such as ISPs to identify users exchanging copyright-protected media (Rimmer, 2007). Subsequent proposals for national copyright legislation and international treaties have aimed to extend intermediary obligations to identify users, revoke services to users identified as violators, remove links or content deemed to be infringing, and impose greater liabilities on intermediaries that do not meet these responsibilities. More extreme forms of the “graduated response” copyright enforcement model responsibilize ISPs to actively monitor the activities of their users and detect copyright infringement (Edwards, 2011). As the next section discusses, such proposals have faced considerable resistance since 2012. Responsibilizing intermediaries is still seen as a key means of copyright enforcement, but doing so through a formal legal route is currently no longer as attractive.

In comparison to the unfolding of responsibilization to assist in state surveillance strategies, these efforts to make intermediaries responsible for copyright enforcement share a number of similarities and maintain some key differences. Similarly, the con-
Content industries are keen to exploit the strategic position of internet intermediaries to identify particular users and content. As with lawful access legislation, these efforts seek to legally compel “third parties” (primarily ISPs) toward certain kinds of monitoring and record keeping. This surveillance is dedicated to a very specific goal, so that copyright enforcement more closely resembles targeted content filtering than the broad surveillance programs coordinated by state intelligence agencies. Copyright enforcement uses surveillance as a means toward a particular end—to limit infringing activities. Since copyright infringement online is often public or can be surveilled without any privileged access to the network (as with BitTorrent), internet intermediaries become primarily useful as gatekeepers to infringing content and as keepers of identifying information. By accessing this identifying information, content owners or their agents can make contact with individual infringers and “educate” them about their behaviour, or follow up with more significant consequences.

While both unfolding and enfolded responsibilization are implemented through the state, enfolded responsibilization originates with private actors in civil society, who work through the state in order to compel other private actors toward particular goals. The priorities of the actors working through the state (in this case, the content industries), become defined as state interests in the process. However, because state policymakers must be successfully captured for this to occur, the process is particularly susceptible to pressure from other interests that may feel threatened. While unfolding state-directed responsibilization strategies can also be contested by intermediaries and civil society (assuming they are not kept secret), any limited set of private actors that seek to impose their values on telecom and associated industries can expect to meet heavy resistance. Some have argued that ISPs and the content industries actually have a number of mutual interests in favour of expanded copyright responsibilization, since some ISPs already monitor users and impose restrictions on those engaged in large-scale file-sharing in order to conserve bandwidth (de Beer & Clemmer, 2007). But there are numerous examples of conflict between the content industries and intermediaries on the issue of responsibilization, reflecting their divergent business interests (Edwards, 2011; Horten, 2012).

Many intermediaries resist an increase in operating costs, taking on new policing responsibilities, or requirements to cut significant numbers of paying customers from their services. In the U.K., “voluntary” cooperation between U.K. ISPs and content owners was pursued under threat of government legislation (Horten, 2012). Likewise, the U.S. Copyright Alert System was promoted as a “voluntary” partnership between ISPs and content owners, but an important role was played by state actors such as “copyright tsar,” or Intellectual Property Enforcement Coordinator, Victoria Espinel (Brandle, 2013). This private partnership can be seen as a way to forestall more onerous forms of ISP regulation by the state. As Frances Moore, the CEO of the International Federation of the Phonographic Industries (IFPI), which represents the international recording industry, has stated, “people need to know if they don’t (reach an agreement) there will be some type of intervention” (Brandle, 2013). Private responsibilization has its limits, and when these are reached state mechanisms must be leveraged to overcome resistance.
Contesting responsibilization

As previously mentioned, various proposals to responsibilize intermediaries have been promoted since the mid-1990s. Sometimes, these have resulted in bitter political disputes, such as when the content and telecom industries find themselves on opposite sides of proposed copyright legislation. However, in recent years internet governance has been politicized as never before, with disputes becoming more visible and involving a greater breadth of actors—at times even turning national issues into international controversies. Over the course of 2012, resistance to a number of responsibilization proposals surprised policymakers. This resulted in the quiet withdrawal of lawful access legislation in Canada (Ibbitson, 2013), a dramatic failure of anti-piracy legislation in the U.S. (Downes, 2012), and the defeat of the Anti-Counterfeiting Trade Agreement (ACTA) in the EU (Meyer, 2012). While these conflicts have led to some reconsiderations of internet governance, intermediaries’ responsibilities have been successfully expanded elsewhere in the world—particularly in non-liberal countries.

When it comes to internet governance, formal political channels in many liberal countries currently seem fraught with risk and friction, and this has led to a search for alternate mechanisms. The U.S., avoiding the legislative route and ostensibly through private responsibilization, has implemented the Copyright Alert System. France’s HADOPI (Haute autorité pour la diffusion des oeuvres et la protection des droits d’auteur sur internet) regime, the most ambitious of the graduated response strategies, has now been scaled back, and the French government is emphasizing voluntary enforcement partnerships for intermediaries (Rees, 2013). The U.K. government has also made its preference for “voluntary” arrangements clear. It has recently championed the moral issue of regulating pornography, promising new legislation if intermediaries do not “play a responsible role [in society]” (Winning, 2013) and find ways of meeting its vision of order. Intermediaries continue to be the preferred instrument of internet governance, by virtue of their latent, actual, or imagined capacities. However, the political disputes they are at the centre of have suddenly magnified.

Finally, in considering the conflicts over responsibilization and the roles that intermediaries should accept, we should remember that we are not just discussing sites, or passive targets of control. Intermediaries function as actors in their own right—selectively complying, resisting, and disclosing demands made by others (in the form of “transparency reports”). They form partnerships, compete for new business, expand their services, and work to influence regulators or civil society. Roles and functions are not just imposed on intermediaries from without, but actively negotiated within and between organizations. For political and state actors, intermediaries can appear as blank instruments onto which various responsibilities can be inscribed. But from within, the position of intermediaries in today’s communication networks also leads to expansive ambitions and new roles. For example, some ISPs now also operate as broadcasters, and providers of security services and cloud infrastructure. Once a search engine, Google’s expansive list of services (including acting as an ISP in select regions) makes it difficult to specify just what kind of service provider it is. There is no historical precedent for organizations of such scope, because the capabilities of today’s communications networks are themselves without precedent. As these intermediaries assume
new roles they expand their interests, and we can expect them to come in conflict with one another, and with regulators, in new ways.

**Conclusion**

Responsibilization has become a crucial strategy for states extending their reach into new digital domains, as well as for non-state actors that seek to leverage state power to promote their interests. This has occurred because private intermediaries are strategically positioned as the internet’s organizational bottlenecks, so that considerable benefit can be gained by aligning them with particular goals. In this regard, ISPs have proven particularly valuable because of the intimate access they can facilitate to subscriber information. The largest ISPs and OSPs have also been targeted because of their control over the most effective chokepoints and the greatest volumes of data flow. The internet certainly poses challenges for sovereign power, but states have found ways to effectively target these privately operated points of control. As a consequence, intermediaries that once concerned themselves with how best to move packets of data are now being asked to consider the implications of their operations on national security and public morality.

This article has foregrounded the rising significance of internet intermediaries, the broad range of capacities these actors are understood or imagined to possess, and the dynamics of governing through them. Intermediaries will continue to operate as the internet’s points of control, and if current trends continue, we will deepen our dependence on these institutions and enter into new relationships with them. They may come to mediate our interactions with a host of networked devices, authenticate and manage our identities, and guard us from threats. The responsibilities attached to these roles may serve to extend state power or benefit established industries, but responsibilization is an open-ended strategy that can also be used to further privacy, user interests, and principles of non-discrimination. Internet governance can work to enfold the values of civil society or it can ignore and oppose them. The failures of some recent responsibilization proposals clearly demonstrate the risks of the latter.

We need to keep in mind that the operations of enfolding and unfolding are not limited to responsibilization, but were conceived by Dean (2007) as broader processes in the dynamics of liberal governance. This helps us see that the recent history of internet governance has not just been that of states “catching up” with technology and applying reactionary regulations. Instead, many governments have largely enfolded the values and processes that enabled the internet’s development, and particularly those that have made it integral to economic activity. Once we recognize the state’s permeability, the dual operation of enfolding and unfolding points to the tensions and contradictions of the liberal state’s role in internet governance. The U.S. government can shepherd and defend a largely unregulated or privately governed vision of the internet, while simultaneously working to embed pervasive copyright enforcement systems and surveillance capabilities. The privacy concerns of users and businesses have become enfolded into politics, as have the concerns of businesses that depend on being able to exploit online personal information. The values shaping the internet are not opposed to formal politics, but have become enfolded into politics like never before. This is demonstrated by governments’ rapid backtracking from a number of tone-deaf internet governance proposals since 2012.
Yet, the unfolding of the state through liberal police remains a fundamental aspect of liberal order. While the internet of earlier years seemed to be exempt from this process, it was only a matter of time until the frontiers of social control caught up with the digital frontier, and the institutions behind our digital flows have proven particularly sensitive to the interplay of sovereignty and territory. We cannot expect any end of proposals to govern the latest threat or pathology by reaching into the internet and squeezing at the pressure points. The pressures to do so may originate in the state or civil domain, but the contours of internet governance will continue to be drawn through its intermediaries. As our relationships with these institutions deepen and change, the responsibilities accompanying their new roles will demand sustained attention.

Notes
1. While some authoritarian states have been attempting to seal off their domestic networks (Riesman, 2012), territorially based filtering is much more common (Deibert et al., 2012). Limited filtering is also common among liberal democracies, where many intermediaries voluntarily block child pornography.

2. This usage is distinct from the definition of intermediary in Bruno Latour’s (2005) social theory as that which “transports meaning or force without transformation” (p. 39). While some internet intermediaries may faithfully transport information without alteration, transformations or translations of data occur at a number of stages in the process even when a carrier is classified as a “mere conduit” or “common carrier.”

3. It is important to note that even virtual infrastructure has a physical basis in computer hardware that can be subject to territorial control.

4. According to The Guardian’s reporting of Snowden’s disclosures, one internal Government Communications Headquarters (GCHQ) memo written in 2011 outlined the U.K. intelligence agency’s focus in the following manner: “[Our] targets boil down to diplomatic/military/commercial targets/terrorists/organised criminals and e-crime/cyber actors” (MacAskill, Borger, Hopkins, Davies & Ball, 2013).

5. Several lawsuits have been launched against the NSA since elements of the program were revealed, and one 2006 lawsuit targeted AT&T because of the company’s participation. Passage of the FISA Amendments Act of 2008 legalized some of these warrantless surveillance practices and provided retroactive immunity for participating telecom companies (Landau, 2010).

6. The state may even actively court and solicit such influence, as Lawrence Lessig’s (2013) recent activism around political campaign financing has highlighted.

7. The state can be superseded by transnational policy mechanisms, as are found in the European Union.

8. However, copyright enforcement can also be “abused” to further illegitimate ends or to remove non-infringing content (Anderson, 2007).

References


Lessig, Lawrence. (2013). We the People, and the Republic we must reclaim. *TED*. URL: http://www.ted.com/talks/lawrence_lessig_we_the_people_and_the_republic_we_must_reclaim.html [October 15, 2015].


