Telecommunications Policy ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Telecommunications Policy

URL: www.elsevier.com/locate/telpol

Internet governance *by* social media platforms

L. DeNardis *, A.M. Hackl

American University, School of Communication, Washington, DC, United States

ARTICLE INFO

Keywords:
Internet governance
Infrastructure studies
Social media platforms
Civil liberties online
Freedom of expression
Permissionless innovation

ABSTRACT

An emerging area of inquiry in Internet governance scholarship is the role of private information intermediaries in enacting governance via technical design choices and user policies. Following this trajectory, this paper addresses governance *by* social media rather than governance *of* social media. Informed by conceptual frameworks from Internet governance and Science and Technology Studies, it examines the extent to which these platforms either promote or constrain rights in three thematic areas: (1) anonymous speech and individual privacy; (2) the ability to express ideas or, stated as a negative liberty, freedom from censorship; and (3) technical affordances of interoperability and permissionless innovation. Because of their unique role as the intermediaries providing citizens with access to the digital public sphere, social media platforms are central points of control on the Internet. Viewing these private platforms through an Internet governance lens, rather than a content lens, suggests that social media technical architectures and policies actually pose several challenges to communication rights as well as to the open Internet. There is an opportunity for Internet governance studies, which have primarily focused on governmental policies and new global institutions, to give greater consideration to the direct policymaking role of private intermediaries and the accompanying phenomenon of the privatization of human rights.

1. An Internet governance lens into social media platforms

Much scholarship related to the politics of social media has focused on content and usage issues, such as the salutary relationship between social media and political transformation (Howard et al., 2011), the use of these platforms for self-representation (boyd & Ellison, 2007; Correa, Willard Hinsley, & Gil de Zuniga, 2010; Gray, 2009, Marwick & boyd, 2010; Tufekci, 2008), and ways in which social media usage expands freedom of expression and facilitates new forms of citizen journalism, alternative media, and dissent (Lynch, Freelon, & Aday, 2014). These inquiries are primarily focused on content rather than the less visible area of the technical infrastructure supporting social media content.

Though not visible in the same way content is visible, how technical infrastructure is designed and administered is not only a technically complex function but one with significant public interest implications. The broad term "Internet governance" is often used to describe the design and administration of the technical infrastructure necessary to keep the Internet operational and the enactment of substantive policies around these technologies (DeNardis, 2014). A dominant theme in both the scholarship and practice of Internet governance examines the policymaking role of new global

* Corresponding author.
E-mail address: denardis@american.edu (L. DeNardis).

http://dx.doi.org/10.1016/j.telpol.2015.04.003
0308-5961/

Please cite this article as: DeNardis, L., & Hackl, A. M. Internet governance *by* social media platforms. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.04.003

institutions, such as the Internet Corporation for Assigned Names and Numbers (ICANN) overseeing domain names and the Internet address space, the Regional Internet Registries distributing Internet Protocol (IP) addresses, or the Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C) establishing the technical standards that enable interoperability among computing devices (Froomkin, 2003; Klein, 2002; Mueller, 2002). Another prominent theme is the role of nation states and intergovernmental organizations in regulating or coordinating the Internet in areas as diverse as antitrust, net neutrality, computer fraud and abuse, privacy, or hate speech (DeNardis, 2009; Goldsmith & Wu, 2006; Mueller, 2010).

A less established but growing area of inquiry examines private information intermediaries, such as social media platforms, in enacting global governance via platform design choices and user policies. Discussing real identification requirements on Facebook and Google+, Rebecca MacKinnon (2012) contends that these platforms take a "Hobbesian approach to governance" (p. 164), with users consenting to give up fundamental rights in exchange for services. Tarleton Gillespie (2010) suggests that private intermediaries strategically frame themselves as "platforms" to pursue economic interests and impact the legal framework in which they operate.

The definition of social media platforms is both capacious and mercurial. Some definitions characterize social media platforms as applications that allow for "user-generated content" (Kaplan & Haenlein, 2010). Other definitions focus on the ability to interactively exchange information with dispersed groups of recipients (Hogan & Quan-Haase, 2010). Drawing from existing definitions, this paper defines social media platforms as providing three specific technological affordances: 1. the intermediation of user-generated content; 2. the possibility of interactivity among users and direct engagement with content; and 3. the ability for an individual to articulate network connections with other users. These common characteristics materialize in various types of information intermediaries: social networking sites like Facebook, microblogging platforms like Twitter, content aggregation sites like YouTube and Reddit, reputation engines like Yelp, mobile image messaging services like Snapchat, e-commerce sites like Etsy and virtual gaming platforms like Xbox Live.

Viewing social media platforms through an Internet governance lens suggests several distinct areas of inquiry. One is the question of how national statutory mechanisms or international legal instruments attempt to, or should, *regulate* social media, whether for intellectual property rights enforcement, antitrust, privacy or other public interest concerns. As a separate matter, governments also *use* social media to carry out paradigmatic responsibilities such as communicating with citizens or providing e-governance services. Another issue at the intersection of governance and social media involves user employment of these platforms as technologies of *dissent* to organize or protest against authoritative regimes. A quite distinct issue, and the narrow one this paper addresses, is how social media platform policies and technical design choices serve as a form of *privatized governance* directly enacting rights and regulating the flow of information online.

This inquiry focuses quite narrowly on this latter question of *privatized governance* via social media platforms, examining how social media platform policies, design choices, and business models predicated upon identity infrastructures and metadata aggregation, enact Internet governance or affect the universality and free flow of information on the Internet and, in doing so, promote or constrain civil liberties. In other words, it addresses governance *by* social media rather than governance *of* social media. To what extent are public interest concerns mediated by private intermediaries rather than by governmental structures and global Internet governance institutions? How do the technological and policy affordances of social media platforms promote or constrain free expression? What are the implications of governance by private intermediaries for individual rights?

These questions build upon scholarship suggesting that expression is no longer merely about content but about the institutional and technological structures underlying this content. On a material level, these underlying structures could potentially be viewed as neutral. Scholarship influenced by the field of Science and Technology Studies (STS) emphasizes the inherently political nature of infrastructure (Bowker, Baker, Millerand, & Ribes, 2010; Nissenbaum, 2001) and successfully challenges the notion of neutrality in science and technology (Sismondo, 2008). In his influential work "Do Artifacts Have Politics," for instance, Langdon Winner (1980) suggests that technological architecture is reflective of political power structures. Scholars applying this lens to Internet governance explain that the underlying technologies that keep the Internet operational "not only embed political values in their design and operations but are increasingly being co-opted for political purposes irrelevant to their primary Internet governance function" (DeNardis, 2012, p. 2). For example, repressive regimes have turned to interconnection infrastructures to cut off communications during political unrest and law enforcement has turned to the Domain Name System (DNS) to block access to websites that illegally share copyrighted content or sell trademarked goods (DeNardis, 2012).

This theme of the underlying politics of infrastructure has similarly emerged in legal scholarship. Constitutional law scholar Lawrence Lessig (2006) has famously suggested that "code is law." Jack Balkin (2014) considers the connection between free expression and infrastructure as a defining feature of the digital age:

> the infrastructure of free expression increasingly is merging with the infrastructure of speech regulation and the infrastructure of public and private surveillance. The technologies and associated institutions and practices that people rely on to communicate with each other are the same technologies and associated institutions and practices that governments employ for speech regulation and surveillance (p. 4).

Balkin (2009) identifies the key values of free expression as the "protection of individual freedom to express ideas, form opinions, create art, and engage in research; the ability of individuals and groups to share their views with others, and build

Please cite this article as: DeNardis, L., & Hackl, A. M. Internet governance *by* social media platforms. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.04.003

on the ideas of others; and the promotion and dissemination of knowledge and opinion" (p. 427). These values will be increasingly protected by technological and administrative design, peer production by users and business decisions of information intermediaries rather than the law. This trend is exemplified by section 230(c)(I) of the Telecommunications Act of 1996 as one of the "most important guarantors of free expression on the Internet" (p. 433). Service provider immunity from liability is designed to protect speech because it obviates the need for intermediaries to strategically censor content to avoid legal consequences and it also removes a potential legal disincentive for entrepreneurs to introduce new intermediary platforms (Balkin, 2009).

Values closely linked to communicative expression are privacy and anonymous speech. Jonathan Zittrain (2008) describes an expansion from *privacy 1.0* to *privacy 2.0*, the former primarily concerned with data collection technologies of governmental and private institutions, and the later concerned with privacy issues arising out of "peer to peer" interactions. Social media platforms like YouTube have facilitated not only the sharing of one's own personal information but also information about one's peers, making involuntary "public selves" of all. According to Zittrain, this phenomenon can undermine the choice to speak anonymously, a traditional value associated with free speech in the United States and other democratic countries.

Internet governance scholarship often brings together approaches from STS and rights concerns in legal scholarship to examine the increasingly significant role of technical architecture in mediating values of free expression. According to DeNardis (2012), the negotiation of civil liberties at the layers of infrastructure beneath content raises three specific concerns. A first concern revolves around the "ongoing privatization of Internet governance" (p. 15), with private intermediaries taking an increasingly central role in regulating civil liberties. The second concern is the role of technological and administrative designs in constraining or promoting values of free expression. Finally, there is the question of how the increasing connection between infrastructure and civil liberties could potentially pose a threat to technical features of the Internet associated with interoperability and innovation.

As such, this Internet governance analysis of social media platforms divides into the following three areas related to free expression:

(a) technical affordances of anonymous speech and individual privacy;
(b) technical affordances related to the ability to express ideas in the digital public sphere and, stated as a negative liberty, freedom from censorship; and
(c) technical affordances of interoperability and permissionless innovation.

This paper analyzes publicly available corporate transparency data, user policies, and technical design choices of dominant social media companies from each major category of social media platforms: content aggregation (YouTube), social networking (Facebook), microblogging (Twitter), photo messaging services (Snapchat), and reputation systems (Yelp). While this taxonomy of social media platforms does not include every conceivable type of social media platform, it does address those that create spaces for individual expression as a core purpose of their services. The overarching objective of this paper is to point to the technical and policy affordances of social media platforms necessary to preserve infrastructures of free expression and to recommend that studies of Internet governance give greater consideration to the policymaking role of private intermediaries and the accompanying phenomenon of the privatization of human rights.

2. Social media platform policies on privacy and anonymity

The early history of Internet infrastructure was characterized by some expectation that content was transmitted with a degree of privacy. Part of this was attributable to technological constraints. Until the 21st century, the processing power of routers and switches was not sufficient to inspect the contents of a packet while routed to its destination. At the same time, there was also some ability to communicate anonymously, or at a minimum under traceable anonymity in which law enforcement could secondarily obtain identity information from a service provider. This prospect for relatively private and anonymous communication has been considered a hallmark of democratic expression and deliberation (Zittrain, 2008).

The evolution of how the Internet is monetized and governed has increasingly complicated these conditions related to individual privacy. A great deal of global Internet governance attention to privacy is focused on governmental policies and the rule of law. Some government-centric examples include geopolitical concern over the expansive digital surveillance practices of some countries, the rise of nation-specific data localization policies that cite privacy concerns as a justification for requiring providers to store data within national borders, and emerging and controversial policies such as the Right to be Forgotten ruling in the European Union. This section focuses not on these governmental policies but on the privatization of conditions of privacy via the policies and technological affordances of social media platforms.

At the surface of content, social media platforms like Facebook provide users with the opportunity to regulate how information is shared with their networks and the larger public. Beneath this visible layer, these intermediaries collect and aggregate a wide range of both content and accompanying user data such as registration information, identifying information (voluntarily provided by users), and metadata. Upon registration, most social media platforms require the disclosure of private information such as name, email address, gender and birth date. The additional information collected by these intermediaries varies across platforms. To personalize user accounts on Twitter, for instance, users can provide a

Please cite this article as: DeNardis, L., & Hackl, A. M. Internet governance *by* social media platforms. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.04.003

short bio, a personal website and picture (Twitter, 2013a). On Facebook, users have the option to share even more personal information like romantic and family relationships as well as work and educational history. Services like Yelp that allow users to make transactions with services through the website may also collect information like home address and credit card information (Yelp, 2013a). Specifically, this section assesses three privacy-related concerns – real name identification policies, approaches to collecting metadata, and policies on disclosure of data to third parties – and examines the implications of these policies for individual rights.

2.1. The politics of real name identification policies

Different social media platforms have different policies about whether a user has the option of remaining anonymous, or at least creating an online persona that representationally masks their identity to the public (Table 1). For example, Facebook requires the use of a real name. Google's YouTube service allows users to publicly represent themselves with either a real name or a pseudonym. Twitter's (2013a) privacy policy requires a full name upon registration but does allow users to change their Twitter handle to a pseudonym. Individuals registering for the reputation engine Yelp (2013a) are required to provide full name and email address. However, only the first initial is shown publicly for users' last names. The use of the mobile communication app Snapchat (2013) provides users with the possibility of relative anonymity, with registration only requiring a user name and password.

These policies have often prompted public debate because of the implications of real name requirements for activists in parts of the world in which they could be imprisoned for speech. In other cases, lesbian, gay, bisexual and transgender (LGBT) people can become targets of online or offline harassment if unable to use pseudonyms to participate in online discussions revealing their sexual orientation or gender identity. For the artistic community, real name policies can infringe upon their right to creative expression. Concerns such as these prompted Google to terminate its real name identification policies in Google+(Kayyali & York, 2014).

A controversy over Facebook's real name policy demonstrates how de facto regulations about real name identification come into conflict not only with privacy but with values of free speech and identity expression. Facebook has a clear real name requirement for users of its service. In the Fall of 2014, the Facebook accounts of several drag queens were terminated because they used their given drag queen names rather than their real names. Facebook had relied on reports by users who had flagged the "fake" accounts (Holpuch, 2014). The activism of several drag queens prompted Facebook to announce a relaxation of the real name policy's enforcement by modifying reporting processes. Facebook also assured users that they were only required to provide the "authentic name they use in real life" rather than their legal name (Cox, 2014). While Facebook and other social media platforms express a commitment to free speech and identity expression, real name polices not only constrain expression of identity, but also jeopardize the online safety of minority populations.

2.2. Universal metadata collection

Apart from name, other types of information surrounding content – such as where, when, and with whom a user is exchanging information – can be just as revealing as the actual content exchanged. Social media platform policies are forthcoming in disclosing the wide range of metadata collected about users, such as IP address, unique hardware identifiers, software configurations, and a variety of locational indicators based on GPS, Wi-Fi, or cellular location. The routinization of this extensive metadata collection as well as contextual content analysis is a fundamental departure from the Internet's original end-to-end design of locating intelligence at endpoints, technical neutrality toward packet contents, and simply using IP addresses as virtual identifiers.

Aggregated data allows intermediaries to better understand user preferences and behavior. For instance, locational data captures specific time and location of posts, comments and related activities. Similarly, activity data captures information on website usage such as retweets on Twitter or search activity. These identification technologies also collect information on the hardware employed to use the platform (device information) and software information including browser type (software footprint).

Table 1
Social media platforms' real name policies.

	Real name registration	Additional information	Public representation
Facebook	Full name required upon registration	Email address, birthday, gender	Real name
YouTube[a]	Google account required for commenting on content and other features, partial name required upon registration	Email address, birthday, gender, phone number, location	Google+ name or name of YouTube channel
Twitter	Full name required upon registration	Email address	Real name or pseudonym
Yelp	Full name required upon registration	Email address, zip code	Real name (initial displayed for last name)
Snapchat	Full name not required upon registration	Email address, phone number, date of birth or age	Username

[a] YouTube's identification requirements based on Google policies.

Please cite this article as: DeNardis, L., & Hackl, A. M. Internet governance *by* social media platforms. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.04.003

Table 2
Metadata collected by social media platforms.

	Location	Phone Number	Device Information	Cookies	Software Footprint	IP Address	Activity data
Facebook	✓	✓	✓	✓	✓	✓	✓
YouTube[a]	✓	✓	✓	✓	✓	✓	✓
Twitter	✓		✓	✓	✓	✓	✓
Yelp	✓		✓	✓	✓	✓	✓
Snapchat	✓	✓	✓	✓	✓	✓	✓

[a] YouTube's metadata collection based on Google policies.

Table 2 shows some of the metadata social media companies collect. The table is not exhaustive in that many other kinds of metadata are collected by social media platforms. But what is most revealing is that there is no discernable difference in the metadata collection policies of these dominant social media platforms. Even a platform such as Snapchat, with a "delete is the default" philosophy to information exchange collects as much user metadata as other types of social media platforms. Metadata collection is the default across all types of social media platforms.

2.3. Third party data disclosure

Third party disclosure policies vary across intermediaries but social media platforms generally share a great deal of information with external entities. The two rationales for this disclosure are completely distinct. One is intrinsic to social media platform business models and involves information sharing with third parties to maximize online advertising revenue generation. Facebook users may opt into a variety of services like games and other third party applications not under the control of Facebook and are also subject to the data collection practices of these third parties (Facebook, 2014a). Facebook's "instant personalization" feature also has significant implications for user privacy. To personalize advertising, Facebook partners receive user data like user name, friend lists and other public information. In order to disable personalization of applications, users need to "opt out" of this service (Facebook, 2014a). Similarly, targeted advertising on Twitter (2013a) is based on an "opt out" mode. In addition to advertisers and business affiliates, social media platforms also share information with service providers like hosting services and analysis firms. While social media platforms share user information with a wide range of third parties, they also retrieve information from external sources. As a Google affiliate, YouTube reserves the right to aggregate and combine data across platforms (Google, 2013). Similarly, Snapchat (2013) may retrieve information from services used through the application.

A second category of user data disclosure involves external requests from governments to disclose user data. These requests come from government agencies within nations in which social media businesses operate. Government requests are motivated by rationales as diverse as law enforcement, national security, defamation, computer fraud and abuse, child protection, or, in some cases, blatant political oppression such as identifying dissident media sources. Social media companies' "transparency reports" disclose the number of requests they receive and the extent to which they comply with these requests. Companies must determine when and when not to disclose data in the context of widely divergent nation-specific statutory environments and the companies' own corporate ethics.

Facebook's (2014b) *Data Use Policy* states that user data may be disclosed to law enforcement "if we have a good faith belief that the law requires us to do so." Numbers of country-specific requests are published in Facebook's *Global Government Request Report* (Facebook, 2013). In the first half of 2013, most user data requests came from United States governmental entities, with data requests for 20,000–21,000 users. Facebook disclosed at least some of the requested user data in 79% of cases. In the second half of 2013, Google (2014a) received 42,648 requests for specific user data, disclosing information in 64% of these cases. In the same time period, Twitter (2014a) received 2121 user data requests from governments, complying with 50% of requests. That social media platforms reject a portion of governmental requests for user data demonstrates a component of the privatized governance role these intermediaries play. Their business practices both create this powerful surveillance system and accompanying privacy concerns, but also push back against governmental misuse of this same system.

2.4. Balancing privacy and profitable business models

This section has described how the privatization of privacy governance occurs at many layers in social media platforms: whether anonymity is permissible, what information is collected about users, and how this information is shared with third parties. Most of these decisions are driven by underlying business models. The social media platforms this paper examines are freely available to users. Social media companies do not generate significant revenue directly from subscribers but rather from advertising. For example, of Google's $66 billion in 2014 revenue, $59 billion, or 89%, was advertising revenue (Google, 2014b). Currency does not flow between the platform provider and consumer, but rather between the provider and an entire ecosystem of third party online advertising firms and entities wishing to purchase targeted ads in social media environments.

Please cite this article as: DeNardis, L., & Hackl, A. M. Internet governance *by* social media platforms. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.04.003

Interactive online advertising is predicated upon a business model in which information intermediaries are able to collect information about users and then deliver targeted advertisements accordingly. This approach differs significantly from the traditional broadcast television and radio environment that is based on advertising revenue models involving a one-way and homogenous flow to users. These broadcasting business models rely on advertising revenues but do not involve the same type of collection of user data customized ad delivery and therefore do not raise commensurate individual civil liberty issues. The appropriate balance between new revenue generation models and individual privacy in social media platforms is yet unclear, but its resolution will be a substantial Internet governance decision with implications both for individual civil liberties and industry stability.

3. The privatization of freedom of expression policies

Social media platforms similarly play a decisive role in promoting or constraining free speech online. Through a technical lens, they are content-neutral in that they provide intermediation of content (videos, images, posts) provided by others rather than creating content and programming. In practice, they make day-to-day decisions about what content is allowed on their platform and the conditions under which this content should be removed. Intermediaries respond to incidents of cyberbullying and online harassment. They intervene in public controversies by censoring speech and terminating user accounts. As governments have come to understand the gatekeeping position of private intermediaries in controlling content, they ask social media companies to intervene in disputes over intellectual property and controversial speech.

A structural factor in the United States connecting social media platforms to questions of free expression is Section 230 of the Communication Decency Act (CDA), which provides information intermediaries with immunity from liability for the content posted by users. For example, a social media company is not liable for defamatory or otherwise illegal content a subscriber might post online. Section 230 is central to protecting values of free expression because it eliminates a possible disincentive for the introduction of new content mediation services (Freivogel, 2011). On the other hand, some argue that intractable social problems around content, such as cyberbullying and harassment, necessitate new legal frameworks in which intermediaries assume greater responsibility (Jaffe, 2013).

Despite immunity under the CDA, social media companies themselves provide frameworks and rules for how speech is either promoted or constrained on their services. One of Facebook's *Principles* (Facebook, 2014c) is the "freedom to share and connect," emphasizing that "people should have the freedom to share whatever information they want, in any medium and any format […]." The principle of "free flow of information" further states that users "should have the freedom to access all of the information made available to them by others. People should also have practical tools that make it easy, quick, and efficient to share and access this information." Similarly, Twitter asserts that "we respect the ownership of the content that users share and each user is responsible for the content he or she provides. Because of these principles, we do not actively monitor and will not censor user content, except in limited circumstances […]" (Twitter, 2014b).

The complex day-to-day decisions social media companies make about when to take down information are not necessarily in compliance with their own content mediation philosophies. The circumstances under which social media platforms reserve the right to restrict users' speech often involve straightforward content removals related to intellectual property rights enforcement, protecting against the disclosure of users' private information, spam and phishing attempts, and the posting of child pornography. In other cases, content take-down decisions arise in much more nebulous conditions.

During the 2012 Olympic Games in London, Twitter suspended the personal account of a British journalist who had been criticizing NBC's coverage of the games. The reporter had tweeted the email address of an NBC executive, which Twitter cited as the reason for the suspension (Shapiro, 2012). Twitter's suspension of the journalist's account provoked a strong public reaction, in part because of concern that its actions were motivated by its cross-promotional Olympics partnership with NBC. Twitter ultimately restored the journalist's account, but the legal right of a private information intermediary to terminate an account, in this case an account of a journalist, demonstrates the power private companies have in determining the conditions of participation in the public sphere. A central conceptual feature of democracy, the public sphere, allows members of society to come together and discuss issues of public concern (Habermas, 1989). In the digital age, the public sphere has "shifted from the national to the global and is increasingly constructed around global communication networks" (Castells, 2008, p. 78). With private companies playing a significant role in providing the infrastructure and platforms underlying these information networks, the determination of conditions of participation in the public sphere is increasingly privatized (DeNardis, 2014).

This phenomenon of the privatization of conditions of civil liberties also enters more narrowly tailored social media platforms such as reputation and ratings systems. For example, Yelp (2013b) deleted ratings and comments about the Oregon bakery "Sweet Cakes by Melissa" after the establishment refused to sell a wedding cake to a lesbian couple (Nochlin, 2013). In response, LGBT allies took to Yelp to express their dismay, noting that "the cakes taste exactly like hate and hypocrisy" (Jen R.) and that they "[…] feel sorry for your children who will have to live knowing that their parents were on the wrong side of history" (Brian L.). Reviewer Jeff W. called on the bakery to "Practice your beliefs. Respect the law. I don't believe that there're [*sic*] a Biblical prohibition against selling someone a cake. There are prohibitions against hypocrisy." Prior to the controversy, the bakery had nine reviews, with an average review of 4.1. The number of reviews immediately jumped to 171, most of them negative responses to the wedding cake incident. On social media platforms, this type of deliberation is often part of public debate, but Yelp removed the majority of comments because some violated terms of services and others were not considered "recommended reviews." A review is not recommended if it might "have been

Please cite this article as: DeNardis, L., & Hackl, A. M. Internet governance *by* social media platforms. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.04.003

posted by a less established user, or it may seem like an unhelpful rant or rave. Some of these reviews are fakes […] and some suggest a bias (like the ones written by a friend of the business owner), but many are real reviews from real customers who we just don't know much about and therefore can't recommend" (Yelp, 2013c).

Social media platforms similarly mediate public controversies related to cyberbullying and other forms of online harassment. In response to the rise of cyberbullying-related teenage suicides, some have called for stronger intervention by social media companies. Considering their immunity from liability under the CDA, the policy frameworks of these companies address cyberbullying based on cultural norms and corporate values rather than statutory requirements. For instance, Yelp's (2012) *Terms of Services* prohibit using the platform to "threaten, stalk, harm, or harass others, or promote bigotry or discrimination." Similar, Facebook's (2014d) *Community Standards* prohibit cyberbullying and hate speech. YouTube (2010) also uses its *Terms of Services* to emphasize immunity from liability, suggesting "that you may be exposed to content that is inaccurate, offensive, indecent, or objectionable, and you agree to waive, and hereby do waive, any legal or equitable rights or remedies you have or may have against YouTube with respect thereto […]."

Inconsistent national laws and cultural norms around the world further complicate the content intermediation role of social media companies. Some European countries and Brazil take a clear regulatory stance against hate speech while the U. S. provides fewer legal restrictions because of strong First Amendment protections. This lack of regulatory harmonization has not only engendered a debate on the appropriate role of private intermediaries in responding to offensive material but also demonstrates the complicated values tensions that arise in cyberspace.

These same companies receive a barrage of daily requests from governments to remove or block content (or accounts) from their sites. Governments are not able to directly block or restrict content so they delegate censorship of information to private intermediaries. In the second half of 2013 alone, Twitter received 377 government requests to remove content, either via a court order or from government agencies or law enforcement (Twitter, 2014c). The company's Transparency data, similar to the content removal reports of other intermediaries, suggests that the company does not necessarily acquiesce to every request, but refuses to comply with a significant percentage (see Tables 3 and 4). This refusal to comply with some government requests helps to demonstrate the direct governance function of these companies.

Google's Transparency Report (Google, 2014a) presents a snapshot of the types of requests it receives on YouTube and across its various platforms. For example, in the second half of 2011, it received requests from the government of Thailand to remove 149 videos allegedly insulting the monarchy. To comply with the laws of Thailand (criminalizing insulting speech

Table 3
Social media platforms disclosing user data to third party platforms.

	Advertising/businesses, institutions	Service providers	Law enforcement
Facebook	Advertisers, developers of apps, games and websites, partners and affiliates	Providers of infrastructure, researchers	Disclosed under certain circumstances
Youtube[a]	Companies and organizations other than Google, advertisers	Users' domain administrator, affiliates	Disclosed under certain circumstances
Twitter	Library of Congress, advertisers	Hosts of wikis and blogs, Google Analytics	Disclosed under certain circumstances
Yelp	Businesses, advertisers, Facebook, Twitter	Quality testing, financial processing	Disclosed under certain circumstances
Snapchat	No details provided	Vendors, consultants, Flurry	Disclosed under certain circumstances

[a] YouTube's information disclosure to third parties based on Google policies.

Table 4
Twitter transparency data on government content removal requests (abridged) (Twitter, 2014c).

Country	Removal requests - Court orders	Removal requests – Agencies	Percentage where some content withheld	Accounts specified	Accounts withheld	Tweets withheld
Brazil	11	1	33	50	2	26
Canada	–	–	–	–	–	–
France	3	306	35	146	0	133
Germany	1	1	0	< 10	0	0
India	2	6	13	54	0	13
Japan	1	1	50	< 10	0	10
Kuwait	0	2	0	< 10	0	0
Mexico	0	1	0	< 10	0	0
Russia	0	14	64	14	1	9
UK	1	8	0	< 10	0	0
US	2	6	0	11	0	0
Total	24	353	11	317	3	191

Please cite this article as: DeNardis, L., & Hackl, A. M. Internet governance *by* social media platforms. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.04.003

about the monarchy), Google removed 70% of these videos. Conversely, and in that same year, Google refused to comply with a request from the Canadian passport office to remove a YouTube video of a Canadian flushing his passport down the toilet (Lee, 2012).

These examples suggest that social media intermediaries are not passive respondents to these requests. Their policy frameworks and day-to-day decisions perform a gatekeeping function about what information can exist in the online public sphere, even as they navigate widely divergent content policies and legal frameworks of different countries. Given that so much of social life and political discourse takes place in various social media platforms, this is a powerful lever of control over free expression.

4. Social media tension with interoperability and permissionless innovation

Since the Internet's inception, a fundamental design objective has been technical interoperability and universality. If software developers and device manufacturers adhered to openly published standards such as TCP/IP, they would be assured that their products would be able to exchange information, or interoperate, with devices also designed to the specifications of these open standards. This interoperability has enabled, at least at the technical level, a universal Internet, and replaced a legacy technological context in which computers made by different companies could not exchange information and two friends using different email systems could not communicate. Of course, in practice, the Internet is not universal because of language differences, variations in access speeds and devices, and systems of filtering and censorship implemented by governments with repressive information approaches. Users in different parts of the world do not have the same experience with social media platforms. Yet at a technical level, the Internet has had the building blocks of universality. It has also had what Zittrain (2008) calls *generativity*, the capacity for technologies to allow for new and unanticipated innovations that extract from and build upon existing platforms.

The protection of free speech is no longer merely about content, but also innovation and the ability to create technological tools that communicate ideas and knowledge. Benkler (2006) argues that digital media have inspired the emergence of "peer production" of technological tools, as well as "peer production" of knowledge, with individuals working collaboratively and non-hierarchically on creative projects. According to Balkin (2009), the ability to partake in the creation of culture as well as the ability to "build on the ideas of others" (p. 427) are two central values of free expression online, both related to the freedom to innovate. The policy frameworks of social media platforms mediate these values by constraining or enabling users to build their own applications and widgets or promoting or constraining users' ability to build on the content of the intermediaries as well as the content of other users.

Social media companies serve naturally as gatekeepers of the kinds of innovations that occur on their platforms. Examples help illustrate this role. Discussing the approval process of new apps through the Apple Store, Hestres (2013) finds that the company may constrain the free expression of users by making the process nontransparent and inconsistent. Twitter blocked applications created by UberMedia from its service due to violations of privacy and trademark rights, but such a ban could also be perceived to have economic motivations as UberMedia had created several applications competing with Twitter (Rao, 2011). On Facebook, users are required to "respect the way Facebook looks and functions. Don't offer experiences that change it" (Facebook, 2014e). Similarly, Twitter (2013b) users may not "replicate, frame, or mirror the Twitter website or its design." The Content Guidelines on Yelp (2014) instruct users not to "swipe content from other sites or users. You're a smart cookie, so write your own reviews and take your own photos and videos, please!" Of course, and indicative of the values always in tension in cyberspace, these gatekeeping roles also serve other social values such as copyright and trademark protection, the desire to maintain a high quality of services for users, and the business necessity of maintaining competitive advantage. Nevertheless, restrictions on the ability of users to innovate on these platforms help illustrate the governance and gatekeeping role of social media companies and how they shape conditions of generativity and creativity.

More directly at the level of the infrastructure of social media platforms, there is increasing concern about Internet fragmentation, both at the technical design level and because of politically motivated policies restricting end-to-end architectures. After disclosures about widespread NSA surveillance, and the role of American social media companies in this surveillance, international reactions have included wanting to "route around" Internet exchange points in the United States, creating walled off Internet services that do not interconnect to American servers and networks, and the development of region or nation specific cloud computing services. There were also initial reactions, in this case by the Brazilian government (Douglas, 2013) wanting American social media companies to store Brazilian customer data in Brazil. In parallel, more than a dozen countries have introduced data localization laws placing constraints on where data is stored, how it is shared, or the conditions under which companies are permitted to transact business within national boundaries (Chander & Le, 2014). Political reactions over the role of social media companies in United States surveillance, and accompanying restrictions on cross-border data flows, could have implications for the future of the Internet's architecture and whether there will be a universal or a fragmented Internet.

Fragmentation also arises when protocol interoperability diminishes. Several design features of social media platforms have eroded the traditional interoperability of the Internet, including lack of open technical standards underlying platforms, lack of Uniform Resource Locator (URL) universality; lack of universal searchability; reliance on Application Programming Interfaces (APIs) over protocols, and lack of data portability. These non-interoperable features are a significant departure from the interoperability inherent in other types of more traditional Internet applications, such as websites and email. The Web was designed to provide a uniform and universal way of accessing a website from any browser anywhere in the world.

Please cite this article as: DeNardis, L., & Hackl, A. M. Internet governance *by* social media platforms. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.04.003

Web inventor Tim Berners-Lee has long cautioned that social media platforms have become closed silos that fragment the Web and tear down a universal space for information (Berners-Lee, 2010). Based on sheer number of subscribers, the public has overwhelmingly chosen to use social media platforms that rely on more proprietary approaches than highly interoperable applications like email. Nevertheless, the closed design features of social media platforms may be diminishing universal Internet interoperability.

5. The social media challenge to Internet governance

Given their significant role as intermediaries providing citizens with access to the digital public sphere, social media platforms are central points of control on the Internet. By comparatively examining how social media platforms enact governance in the three thematic areas mentioned in this research paper – privacy, expression as well as interoperability and permissionless innovation – it becomes clear that there are several interfaces in which these companies exert direct power over online rights. They interface directly with content via their ability to delete or block content at will; with subscribers, via the technological affordances of system design and via terms of service; with governments, by serving as the intermediaries that carry out delegated law enforcement and delegated censorship; and with other institutions, via protocols, business models and technological interfaces. Each of these interfaces can be viewed as an information choke point determining how information flows. In short, the governance role of social media platforms is not only entrenched, it takes place in various ways outside of what most view as the policy role of terms of service and other user agreements.

There have always been privatized spaces for public deliberation in the offline world. While there are some similar concerns raised in online and offline spaces, there are also four substantive differences. Private spaces in the physical world are tied to geography while virtual spaces transcend national borders and therefore introduce ambiguity and conflicts of applicable jurisdiction and law. As corporate transparency reports suggest, the norms and laws in various jurisdictions are often in conflict and private intermediaries must determine which government requests to comply with and which to ignore. Another distinguishing feature is that social media platforms are largely free services that monetize customer data as their core online advertising revenue model. While there are examples of this in offline spaces, what is notable in the social media example is the large scale of voluntary acquiescence to this information collection and monetization and the fact that this collection takes place behind the scenes where it is not directly observable to users. A more visible quality is that social media platforms are choke points that individuals essentially must pass through to participate in significant parts of the online public sphere. Finally, the core function of social media platforms (the intermediation of content) is simultaneously related to several conditions of democracy: how people receive news; the articulation of relationships and associations; access to knowledge; and spaces for deliberation about issues of public concern.

It no longer makes sense for policy makers and scholars focusing on Internet governance and cyber policy to remain relegated to attending to either the global institutions that carry out specific administrative functions or to the policies of national governments or intergovernmental organizations. Attention to private intermediaries is necessary as administrative responsibilities with core civil liberties implications shift increasingly to these entities. Social media platforms and the private companies that run them are potent because they have become vital components of the digital public sphere. How they design their platforms, how they allow content to flow, and how they agree to exchange information with competing platforms have direct implications for both communication rights and innovation. One objective of free expression is to create a communicative context necessary for the advancement of democracy. As the responsibility for the preservation of free speech shifts from public to private contexts, this will have implications not only for what counts as free expression online but also for democracy itself.

References

Balkin, J. M. (2009). The future of free expression in a digital age. *Pepperdine Law Review*, *36*(2), 427–444.

Balkin, J. M. (2014). Old school/New school speech regulation. *Harvard Law Review, 127* (2296). Retrieved 31.03.14 from ⟨http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2377526⟩.

Benkler, Y. (2006). *The wealth of networks*. New Haven, CT: Yale University Press.

Berners-Lee, T. (2010). Long live the web: A call for continued open standards and neutrality. *Scientific American*. Retrieved 13.04.14 from ⟨http://www.scientificamerican.com/article/long-live-the-web/⟩.

Bowker, G. C., Baker, K., Millerand, F., & Ribes, D. (2010). Toward information infrastructure studies: Ways of knowing in a networked environment. In J. Hunsiger, L. Klastrup, & M. Allen (Eds.), *International handbook of Internet research* (pp. 97–117). doi:10.1007/978-1-4020-9789-8_5.

boyd, d. m., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*, 210–230, http://dx.doi.org/10.1111/j.1083-6101.2007.00393.x.

Castells, M. (2008). The new public sphere: Global civil society, communication networks, and global governance. *Annals of the American Academy of Political and Social Science*, *616*(1), 78–93.

Chander, A., & Le, U. P. (2014). *Breaking the web: Data localizaton vs. the global Internet*. UC Davis Legal Studies Research Paper series, 378.

Correa, T., Willard Hinsley, A., & Gil de Zuniga, H. (2010). Who interacts on the web?: The intersection of users' personality and social media use. *Computers in Human Behavior*, *26*(2), 247–253.

Cox, C. (2014). Status update [Facebook page]. Retrieved 13.03.15 from ⟨https://www.facebook.com/chris.cox/posts/10101301777354543⟩.

DeNardis, L. (2009). *Protocol politics: The globalization of Internet governance*. Cambridge, MA: MIT Press.

DeNardis, L. (2012). Hidden levers of Internet control: An infrastructure-based theory of Internet governance. *Journal of Information, Communication and Society*, *15*(3), 720–738, http://dx.doi.org/10.1080/ 1369118X.2012.659199.

DeNardis, L. (2014). *The global war for Internet governance*. New Haven, CT: Yale University Press.

Douglas, B. (2013). Brazil debates Internet law in wake of NSA scandal. *BBC News*. Retrieved 13.04.14 from ⟨http://www.bbc.com/news/technology-24899396⟩.

Please cite this article as: DeNardis, L., & Hackl, A. M. Internet governance *by* social media platforms. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.04.003

Facebook (2013). *Global government request report.* Retrieved 27.03.14 from ⟨https://www.facebook.com/about/government_requests⟩.
Facebook. (2014a). *Other websites and applications.* Retrieved 27.03.14 from ⟨https://www.facebook.com/about/privacy/your-info-on-other⟩.
Facebook. (2014b). *Some other things you need to know.* Retrieved 27.03.14 from ⟨https://www.facebook.com/about/privacy/other⟩.
Facebook (2014c). *Facebook principles.* Retrieved 01.04.14 from ⟨https://www.facebook.com/principles.php⟩.
Facebook (2014d). *Facebook community standards.* Retrieved 01.04.14 from ⟨https://www.facebook.com/communitystandards⟩.
Facebook (2014e). *Platform policy.* Retrieved 28.09.14 from ⟨https://developers.facebook.com/policy⟩.
Freivogel, W. H. (2011). Does the Communications Decency Act foster indecency?. *Communication Law & Policy*, *16*(1), 14–48, http://dx.doi.org/10.1080/10811680.2011.536496.
Froomkin, A. M. (2003). ICANN 2.0: Meet the new boss. *Loyola of Los Angeles Law Review*, *36*, 1087–1102.
Gillespie, T. (2010). The politics of platforms. *New Media & Society*, *12*(3), 347–364, http://dx.doi.org/10.1177/1461444809342738.
Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford, UK: Oxford University Press.
Google. (2013). *Privacy policy.* Retrieved 27.03.14 from ⟨https://www.google.com/intl/en/policies/privacy/⟩.
Google. (2014a). *Google transparency report.* Retrieved 27.03.14 from ⟨https://www.google.com/transparencyreport/userdatarequests/countries/⟩.
Google. (2014b). *Google consolidated balance sheet 2014 4Q.* Retrieved 13.03.15 from ⟨http://investor.google.com/pdf/2014Q4_google_earnings_data.pdf⟩.
Gray, M. L. (2009). Negotiating identities/Queering desires: Coming out online and the remediation of the coming-out story. *Journal of Computer-Mediated Communication*, *14*(4), 1162–1189.
Habermas, J. (1989). *The structural transformation of the public sphere*. Cambridge, UK: Polity.
Hestres, L. E. (2013). App neutrality. Apple's app store and freedom of expression online. *International Journal of Communication*, *7*, 1265–1280.
Hogan, B., & Quan-Haase, A. (2010). Persistence and change in social media. *Bulletin of Science, Technology & Society*, *30*(5), 309–315.
Holpuch, A. (2014). Facebook still freezing accounts despite apology to drag queens over 'real names'. *The Guardian.* Retrieved 14.03.15 from ⟨http://www.theguardian.com/technology/2014/oct/17/facebook-still-freezing-accounts-despite-apology-drag-queens-real-names⟩.
Howard, P. N., Duffy, A., Freelon, D., Hussain, M., Mari, W., & Mazaid, M. (2011). *Opening closed regimes: What was the role of social media during the Arab Spring?* Project on Information Technology and Political Islam. Research Memo 2011.1. Seattle, WA: University of Washington.
Jaffe, E. M. (2013). Imposing a duty in an online world: Holding the web host liable for cyberbullying. *Hastings Communications and Entertainment Law Journal*, *35*(2), 277–302.
Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, *53*(1), 59–68.
Kayyali, N., & York, J. (2014). Facebook's real name' policy can cause real-world harm for the LGBTQ community. *Electronic Frontier Foundation.* Retrieved 28.08.14 from ⟨https://www.eff.org/deeplinks/2014/09/facebooks-real-name-policy-can-cause-real-world-harm-lgbtq-community⟩.
Klein, H. (2002). ICANN and Internet governance: Leveraging technical coordination to realize global public policy. *Information Society*, *18*(3), 193–207.
Lee, T. B. (2012). Google takedowns: Canadians can urinate on their passports but Thais can't insult their king. *Forbes.* Retrieved 13.04.14 from ⟨http://www.forbes.com/sites/timothylee/ 2012/06/18/google-takedowns-canadians-can-urinate-on-their-passports-but-thais-cant-insult-their-king/⟩.
Lessig, L. (2006). *Code and other laws of cyberspace, version 2.0*. New York, NY: Basic Books.
Lynch, M., Freelon, D., & Aday, S. (2014). *Blogs and bullets III: Syria's socially mediated civil war. Peaceworks*. Washington, DC: United States Institute of Peace.
MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for Internet freedom*. New York, NY: Basic Books.
Marwick, A. E., & boyd, d. (2010). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*, 96–113.
Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press.
Mueller, M. L. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, MA: MIT Press.
Nissenbaum, H. (2001). How computer systems embody values. *Computer*, *34*(3), 118–120.
Nochlin, E. (2013). Did a baker break the law when he denied service to same-sex couple?. *KATU.* Retrieved from ⟨http://www.katu.com/news/business/Did-a-baker-break-the-law-when-denying-service-to-same-sex-couple-189450071.html⟩.
Rao, L. (2011). Twitter suspends UberMedia clients for privacy and monetization violations, trademark infringement. *TechChrunch.* Retrieved 03.10.14 from ⟨http://techcrunch.com/ 2011/02/18/twitter-suspends-ubermedia-clients-ubertwitter-and-twidroyd-for-violating-policies/⟩.
Shapiro, R. (2012). Guy Adams' Twitter account back up, journalist's account was suspended after NBC Olympics Tweet. *The Huffington Post.* Retrieved 13.04.14 from ⟨http://www.huffingtonpost.com/2012/07/30/guy-adams-twitter-account-suspended-independent-nbc-olympics_n_1720008.html⟩.
Sismondo, S. (2008). Science and technology studies and an engaged program. In E. J. Hackett, O. Amsterdamska, M. Lynch, & J. Wajcman (Eds.), *The handbook of science and technology studies (3rd ed)*. Cambridge, MA: MIT Press.
Snapchat. (2013, December 20). *Privacy policy.* Retrieved 27.03.14 from ⟨http://www.snapchat.com/privacy/⟩.
Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science Technology & Society*, *28*(1), 20–36, http://dx.doi.org/10.1177/0270467607311484.
Twitter. (2013a, October 21). *Twitter privacy policy.* Retrieved 27.03.14 from ⟨https://twitter.com/privacy⟩.
Twitter. (2013b, July 2). *Developer rules on the road.* Retrieved 01.04.14 from ⟨https://dev.twitter.com/terms/api-terms⟩.
Twitter. (2014a). *Transparency report: Information requests.* Retrieved 27.03.14 from ⟨https://transparency.twitter.com/information-requests/2013/jul-dec⟩.
Twitter (2014b). *The Twitter rules.* Retrieved 01.04.14 from ⟨https://support.twitter.com/articles/18311-the-twitter-rules⟩.
Twitter (2014c). *Transparency report: Content removal requests.* Retrieved 13.04.14 from ⟨https://transparency.twitter.com/removal-requests/2013/jul-dec⟩.
Winner, L. (1980). Do artifacts have politics?. *Daedalus*, *109*(1), 121–136.
Yelp (2012). *Terms of services.* Retrieved 27.03.14 from ⟨http://www.yelp.com/static?country_=US&p=tos⟩.
Yelp. (2013a, September 10). *Privacy policy.* Retrieved 27.03.14 from ⟨http://www.yelp.com/tos/privacy_en_us_20130910⟩.
Yelp (2013b). Sweet cakes by Melissa [online reviews]. Retrieved 03.04.14 from ⟨http://www.yelp.com/biz/sweet-cakes-gresham⟩.
Yelp (2013c). *User reviews.* Retrieved 01.04.14 from ⟨http://www.yelp.com/faqrecommended_reviews⟩.
Yelp. (2014). *Content guidelines.* Retrieved 01.04.14 from ⟨http://www.yelp.com/guidelines⟩.
Youtube (2010). *Terms of service.* Retrieved 02.04.14 from ⟨https://www.youtube.com/static?template=terms⟩.
Zittrain, J. (2008). *The future of the Internet and how to stop it*. New Haven, CT: Yale University Press.

Please cite this article as: DeNardis, L., & Hackl, A. M. Internet governance *by* social media platforms. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.04.003