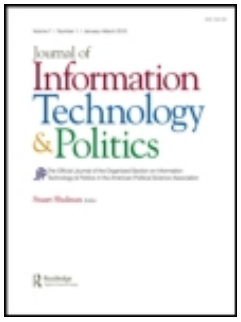

Journal of Information Technology & Politics

ISSN: 1933-1681 (Print) 1933-169X (Online) Journal homepage: http://www.tandfonline.com/loi/witp20

Networked Governance and the Regulation of Expression on the Internet: The Blurring of the Role of Public and Private Actors as Content Regulators

Benjamin Farrand & Helena Carrapico

To cite this article: Benjamin Farrand & Helena Carrapico (2013) Networked Governance and the Regulation of Expression on the Internet: The Blurring of the Role of Public and Private Actors as Content Regulators, Journal of Information Technology & Politics, 10:4, 357-368, DOI: 10.1080/19331681.2013.843920

To link to this article: https://doi.org/10.1080/19331681.2013.843920

Accepted author version posted online: 18 Sep 2013.
Published online: 18 Sep 2013.

Submit your article to this journal

Article views: 476

Citing articles: 3 View citing articles

Full Terms & Conditions of access and use can be found at
http://www.tandfonline.com/action/journalInformation?journalCode=witp20

Journal of Information Technology & Politics, 10:357–368, 2013
Copyright © Taylor & Francis Group, LLC
ISSN: 1933-1681 print/1933-169X online
DOI: 10.1080/19331681.2013.843920

Routledge
Taylor & Francis Group

GUEST EDITORIAL

Networked Governance and the Regulation of Expression on the Internet: The Blurring of the Role of Public and Private Actors as Content Regulators

Benjamin Farrand
Helena Carrapico

ABSTRACT. This editorial provides an overview of the themes of network governance and content regulation that are expanded upon in the subsequent articles, identifying key issues and concerns that are prevalent in the literature in this field. In particular, this text considers governance not as an Internet-specific phenomenon, but as a global phenomenon, identifying and discussing literature pertaining to governance both online and offline, and providing examples of theories that seek to explain these forms of governance. Focusing on the interaction between public and private actors in content regulation, this editorial highlights that content regulation is a complex and contested issue that cannot be separated from its social and cultural contexts, and provides an overview of the articles contained.

KEYWORDS. Governance, networks, content regulation, public-private partnership

Benjamin Farrand is Lecturer in Intellectual Property Law and Policy at the University of Strathclyde in Glasgow, Scotland. He holds a Ph.D. in law from the European University Institute in Florence, Italy, on the cross-border regulation of digital copyright. His current research focuses on lobbying processes in the field of intellectual property law, in addition to the law, philosophy, and governance of human enhancement technologies.

Helena Carrapico is a Newton International Fellow at the University of Dundee in Dundee, Scotland. Prior to her current position, she was a researcher at the Center for Social Studies of the University of Coimbra, Portugal. She holds a doctoral degree in social and political sciences from the European University Institute (Florence), where she developed her thesis on EU policies on organized crime. Her current research focuses on the United Kingdom opt-in and opt-out strategies in the area of justice and home affairs, and on the reasoning behind the United Kingdom's model of selective participation in the area of freedom, security, and justice. Other areas of research include the external dimension of Justice and Home Affairs and European Union organized crime policies. Her broader interests comprise critical security studies.

Address correspondence to: Benjamin Farrand, School of Law, University of Strathclyde, Graham Hills Building, 50 George Street, Glasgow G1 1QE, Scotland, UK (E-mail: benjamin.farrand@strath.ac.uk) or Helena Carrapico, School of Humanities, Politics and International Relations, University of Dundee, Dundee DD1 4HN, Scotland, UK (E-mail: h.carrapico@dundee.ac.uk).

This special issue of the *Journal of Information Technology & Politics* began as the result of a discussion panel at the 2012 International Studies Association International Convention in San Diego, California, an event significantly influenced by events in Tunisia and Egypt now known as the "Arab Spring." One theme that developed as a result of these discussions was that liberal democracies such as those in Europe and the United States are not averse to repressing forms of expression viewed as undesirable; where there were differences appeared to be in the form and structure of the regulatory models that were used. Discussions centered on the role of agreements between public and private actors, and the importance of the Internet as both a means of facilitating expression and a means of repressing it. One point commonly made was that scholarship and discussions concerning the social impacts of the Internet should avoid characterizations that could be considered purely "cyber-utopian" or "cyber-dystopian."

This editorial begins by considering the concept of "network," not as it pertains to the infrastructure of the Internet, but as a form of governance model that highlights the importance of both public and private actors as regulators. Taking into account both general governance literature and Internet-specific literature, the first section of this text expands upon theorizations of this model, and also the justifications for its existence that concern the perception of expertise possessed by private actors and the comparative inability of public actors to regulate the Internet without private support. The second section of this article expands on the concept of content regulation, demonstrating that the Internet has the technical potential to both facilitate and suppress expression, leading to a divergence in literature between that which views the emancipatory potential of digital communications technology optimistically, and that which views it pessimistically. This editorial seeks to present a more nuanced view, demonstrating the "dual-use" function of the Internet, and that conceptualizations of what content should be regulated, and how, are dependent upon social, political, and cultural contexts, which are often transitory and malleable, allowing for both increased control and resistance. Finally, this text provides an overview of the key themes and issues identified in the remaining six articles comprising this special issue.

THE REGULATION OF THE INTERNET: FROM LEVIATHAN TO THE NETWORK

One central theme that links the articles in this special issue, and indeed, scholarship on contemporary forms of regulation and governance more generally, is that of the networked nature of regulation. Traditionally, "political philosophy is too often inclined to reduce power solely to the central authority, Leviathan," Veyne has argued (2010, p. 94), with the result that complex relationships that guide legislative and policy processes are not made apparent. However, academic thought is diverging from such conceptualizations of regulation, not only in political science and communications, but also disciplines perceived as being somewhat more conservative, such as law. Scholarship that is influenced by a range of different theoretical and methodological approaches has nevertheless come to similar conclusions concerning policy-making, namely that the state is not the sole regulatory body of society, but one of many interlinked actors. From a Foucauldian perspective, this is framed in terms of the relationships between actors, whether state and non-state, or individuals within society. It is wrong, Foucault argues, to think of the power to regulate as being one possessed by the powerful and exerted hierarchically onto the "powerless." Instead he says, "power must . . . be analyzed as something that circulates. . . . Power functions. Power is exercised through networks" (Foucault, 2004, p. 29). Power is relational, and as a result, the power to influence how the Internet is regulated is also relational. Governments do not develop these policies purely through the exercise of sovereign power, but through the relations that both influence and are influenced by governments through the production of knowledge (Dean, 2010, Chapter 1; Downing, 2008, p. 18; see, for example, Kelly, 2012, p. 33–34; Kiersey, 2011, p. 17). At a less conceptually abstract

level, others have considered the networked nature of governance in terms of the relationships between state or public actors and private actors. This approach considers that political decision-making is not restricted to formal governmental institutions, but is the result of the creation, construction, and establishment of policy networks (Koimann, 2000; Marcussen & Torfing, 2003; Marsh & Rhodes, 1992). For Mueller (2010), these policy networks are typified by corporate actors forming strong and stable network relations, being "drawn into regularized interaction around a set of laws and regulations in a specific sector" (p. 38). Castells (2011) also uses the term "network" to explain contemporary forms of governance. Each interdependent actor constitutes a node in the governance network, be it a state institution, corporate actor or individual, the importance of which varies depending on the particular activity being undertaken, and the level of competence and information possessed by that particular node (Castells, 2011, pp. 18–19). The increasingly networked nature of governance has been conceptualized as being the result of "neoliberal" reforms in the late 1980s and a discourse of the inefficiency, ineffectiveness, and undesirability of state regulation (Harvey, 2007), the proliferation of independent regulatory agencies, "public–private partnerships," and the delegation of state competences (Black, 2001; Braithwaite, 2008; Levi-Faur, 2005; Wright, 2011), or the perception of the need for external knowledge or expertise not possessed by governmental institutions (Baumgartner, 2009; Culpepper, 2011). In other words, it is not only governance of the Internet that is defined by networked relations, but also governance as a general phenomenon.

This transformation of conceptualizations of regulation is evident in discussions concerning the Internet as a specific phenomenon. John Perry Barlow's (in)famous Declaration of the Independence of Cyberspace in 1996 showed a preoccupation with the state as an oppressive actor, and the Internet as being free from that oppression through both technological and legal limitation: "You have no sovereignty where we gather." In this "cyber-libertarian" conceptualization of the Internet, "cyberspace" was a place that should be free from governmental or state interference, with decision-making regarding the regulation of the Internet viewed as being best approached through the consensus of users, or ensuring compliance with technical standards (Friedland, 1996; see for example Johnson & Post, 1996). However, the view of the Internet as the "Wild West" or unregulated frontier of communications was quickly replaced by one that acknowledged the networked nature of governance on the Internet, and the interaction between state actors and corporate/private actors such as Internet Service Providers and ICANN (Deibert, 2009; Goldsmith & Wu, 2006; see, for example, Lessig, 2004; Mueller, 2010; Wu, 2010). The speedy drafting and implementation of legislation pertaining to the regulation of content on the Internet, such as the Digital Millennium Copyright Act (1998) in the U.S., and E-Commerce (2000/31/EC) and Information Society Directives (2001/29/EC) in the EU and cross-jurisdictional cases concerning content removal such as *Licra v. Yahoo!* (2000), demonstrated that the conceptualization of the Internet as unregulated and unregulable was somewhat mistaken. Instead, state and non-state actors have demonstrated both the willingness and ability to actively regulate Internet-based activities, through coordinated action. Furthermore, other writers have considered that the Internet has the potential to widen participation in political processes, allowing looser coalitions of citizens to become involved in the framing of regulatory issues through combinations of on- and offline activism (Bimber, Stohl, & Flanagin, 2009; MacKinnon, 2012; Ward & Gibson, 2009). Dutton and Peltu (2009) refer not to networked governance but to "multi-stakeholder" processes, in which governments, infrastructure providers, and corporations are joined by nongovernmental organizations, civil society groups, and individuals in discussions concerning governance on the Internet (pp. 390–393). While the model for the governance of the Internet may not be Leviathan, the single overarching sovereign power centrally regulating all conduct, neither is it a model free from regulation, or regulation solely by technical bodies or corporations. Instead, the regulation of the Internet is the result of complex relationships between both public

and private actors who act both in coordination and competition with each other in order to ensure preferred regulatory outcomes.

The relationship between public and private actors in the digital environment appears to be one that mirrors general approaches to governance in the offline environment, in which "rule-making displaces public ownership and centralized administration" (Wright, 2011, p. 31). Within this framework, governments or legislative institutions pass laws or regulations that dictate how a particular sector should be regulated, leaving the actual act of regulation to the private sector. These private actors take on the role of "self-regulated regulators" (see also Brown, 2010; Parker, 2002; Price & Verhulst, 2005), performing regulatory activities perceived as lying within the competence of the state (as shall be expanded upon in the next section). Again, this is a phenomenon that is not limited to Internet governance, but is reflected by partnerships between governments and industry in, for example, environmental regulation (Héretier & Eckert, 2008) or the regulation of finance, telecommunications, and broadcasting (Coen & Thatcher, 2008, p. 58). The oft-cited explanation for private, nongovernmental actors choosing to act as "self-regulated regulators" is the implied threat of increased legislative regulation of their business sectors (Bartle & Vass, 2007, p. 895; Héretier & Eckert, 2008, p. 116). The "safe harbor" provisions of legislation, such as under Articles 14–16 of the E-Commerce Directive, work on such an understanding; should an Internet service provider quickly respond to notification of illegal content (whether in the form of copyright infringements, child abuse images, or other materials), then the service provider has no liability for the hosting of that material. In terms of regulation, this may be framed in terms of "self-regulating regulation." While governments (or in this case, the EU) provide a legislative framework for regulation, the act of regulation is performed by the service provider. In doing so, the service provider regulates its own conduct, namely the speedy response to notification of the existence of illegal content. The service provider then removes the content. Should a service provider fail to do so, action may be taken against that service provider in national courts. One example of the implied threat of regulation comes in the form of "encouragement" of voluntary arrangements between service providers and copyright holders by institutions such as the European Commission. In order to better facilitate speedy cooperation, the Commission has identified voluntary agreements as being the preferred approach; however, should service providers fail to come to such arrangements, the Commission stated that it was "ready to consider alternative approaches" (European Commission, 2009, sec. 4.2). It is for this reason that Héretier and Eckert (2008) have described self-regulated regulators in network governance as operating "within the shadow of hierarchy" (p. 113). Nevertheless, corporate actors are not passive in the development of such forms of regulation, as they often take an active role in shaping that regulation through the participation of legal experts and corporate leaders (see also Amable, 2003, pp. 10–12; Culpepper, 2011, pp. 7–10; Lütz, Eberle, & Lauter, 2011, p. 331). If regulation is the result of networks, so too is the framing of that regulation. This is not to suggest that corporate or private actors are always completely willing participants in these regulatory deliberations, or that these arrangements will be particularly successful. In the EU context, Internet service providers have resisted attempts to impose upon them an active duty to monitor the use of their services in the context of alleged intellectual property infringements. In the cases of *Scarlet Extended* (2011) and *SABAM v. Netlog* (2012), Internet service providers argued that such an imposed duty would be in breach of the E-Commerce Directive accepted by the Court of Justice of the European Union. As the E-Commerce Directive does not allow for a responsibility on the part of service providers to specifically and actively monitor the use of their services by users, the legal imposition of such a duty by a national court was considered to be in breach of EU law. However, the prevention of the imposition of a *legal* duty does not preclude the possibility of a *voluntary* duty that an intermediary agrees to under the implied threat of subsequent legislation. If, for example, the E-Commerce Directive would be reformed to include an active duty to

monitor, then such resistance by intermediaries would not be effective. Nor does it mean that policy actors will be unified over the most suitable form of regulation, or indeed the nature of the content to be regulated. For example, information security in the digital environment would appear to be a particularly contested area of policy-making, especially where it concerns the balance between the perceived need for secrecy and a desire for transparency and information dissemination (Rogerson & Milton, this issue

On the part of governments and legislative bodies, two key themes recur in discussions as to *why* the involvement of private actors in regulation is considered desirable. The first is that of expertise. Governments rely on the perceived expertise of corporate actors in their particular fields of activity, considering that those actors understand their businesses, their needs, and their abilities better than state actors (Bernhagen & Bräuninger, 2005; see for example Esterling, 2004). At the level of rapidly developing digital technologies such as the Internet, the perceived need for technical experts to be involved in regulation is magnified (Christou & Simpson, 2006; Yu, 2010). Due to the perceived high technical complexity of the functioning of the Internet, governmental and legislative bodies defer to the expertise of actors such as Internet service providers concerning the most suitable means of regulating content; in this respect, policy-making competence is shared, with the public actor stating "this is the problem" or "this is the proscribed conduct," and the private actor proposing a technical, often code-based solution (Lessig, 2006). Related to this point on expertise is that of capacity. Given the transnational character of Internet access, national attempts to regulate the Internet by traditional public authorities such as the police or administrative bodies are substantially limited if there is no support from the private providers of these services. Whereas Goldsmith and Wu (2006) have stated that the conceptualization of the Internet as borderless is ultimately an "illusion," and that nation states quickly legislated jurisdictional issues concerning offences committed over the Internet, this system of regulation still requires the involvement of intermediary Internet service providers in order to be effective. In the above mentioned *Licra v. Yahoo!* (2000) case, the jurisdiction of French courts over the access by French citizens to illegal sales of Nazi memorabilia (under French law) was quickly established. While the advertisements were made in the U.S., where such sales were legal, the French courts nevertheless required that this information was to be made inaccessible in France—a technical requirement that could only be performed by the Internet service provider, rather than state regulators. Effective regulation of this content then requires the involvement of and interaction between public and private actors. As Mueller states (2010), "Most of the real world governance of the Internet is decentralized and emergent: it comes from the interactions of tens of thousands of network operators and service providers" (p. 9). The Internet by design is a system of distributed control, dispersing "participation in and authority over networking" (Mueller, 2010, p. 4). This, combined with the high volume of Internet traffic to be processed, requires the involvement and intervention of well-placed intermediary organizations that have the technical capacity to regulate, as well as the expertise.

THE ANSWER TO THE MACHINE IS NOT ONLY IN THE MACHINE: CULTURAL AND SOCIAL IMPACTS ON THE REGULATION OF CONTENT ONLINE

Scholarship concerning the role of the Internet in society can be undertaken from a "cyber-utopian" perspective, in which the Internet is the facilitator of expression, an emancipatory tool, and a means of encouraging citizen participation in democratic processes, so long as the Internet is not unduly interfered with or restricted by states or corporations (see for example Benkler, 2006; Shirky, 2011), or from a "cyber-pessimist" or "cyber-dystopian" perspective, considering the role of the Internet in state and/or corporate repression, the "balkanization" of opinion, and the appeal to "lowest common dominator" entertainment and politics (Lanier, 2013; see for example Morozov, 2011; Zittrain, 2008). Indeed, the Internet has the

potential for both. While there is, without doubt, the urge to perceive new technologies in light of all the potential they may have for increasing the quality of life, or in light of all the potential they may have for decreasing the quality of life, such black and white assessments provide little more than best-case or worst-case scenarios. The Internet has the potential to be both a tool of facilitation, allowing for mobilization, activism, and the sharing of information, or a tool of repression, allowing for surveillance, the dissemination of propaganda, and the control or blocking of information. For example, the Internet has been used by civil society groups and activists to politically organize and rally behind a presidential candidate (Gil de Zúñiga, Veenstra, Vraga, & Shah, 2010). Irrespective of the views of the legitimacy of such action, the Internet has been used to release information perceived by leakers to be in the public interest, such as the infamous leaking of U.S. diplomatic cables by WikiLeaks and Chelsea Manning (see for example McGreal, 2010). Regardless of the subsequent successes or failures of the "Arab Spring" movement, the Internet has been argued to have played an important role in the mobilization and coordination of protesters in Egypt (MacKinnon, 2012), and has also assisted in the coordination of activists and resistance movements, such as the "Occupy" movement (see Jensen & Bang, this issue) and ACTA protestors (Farrand, 2014; Smith, this issue). It can also be used for the facilitation of more violent forms of participation, such as those of alleged protestors/rioters in London in 2011 (Bright, 2011; Halliday, 2011). Yet digital technologies have also been used to monitor and suppress, the most recent example being the leaking of information concerning widespread surveillance by the NSA as part of the PRISM project (see The Guardian, 2013, for comprehensive coverage of the information leaked). These technologies have been used by more repressive regimes such as China and Saudi Arabia to limit access to information through the use of centralized firewall systems (Deibert, Palfrey, Rohozinski, & Zittrain, 2008, 2010, 2012), but also through the use of specific filtering systems used to prevent access to content considered illegal, such as child abuse material or materials deemed to infringe copyright in "Western liberal" democracies (Deibert et al., 2010; Goldsmith & Wu, 2006; McIntyre, 2012). States typified by more authoritarian approaches to governance may have overt systems of control, in which the existence of filtering mechanisms is explicitly recognized and attempts to access proscribed materials result in a specific message that warns users that they have attempted to access illegal content. States typified by less authoritarian approaches to governance may have more subvert systems of control, in which the filtering of content deemed illegal results in an error or "page not found" message, rather than specific mention made of the attempt (intentional or otherwise) to access that content. Alternatively, rather than the use of filtering or other forms of blocking of content, Western liberal democracies or private actors may use other means of suppressing or removing content through the use of other means, such as copyright infringement notices (see Farrand, this issue; Smith, this issue). These alternate means may be used through the combination of human assessment and technology to block access or remove material, or alternatively may be an automated computer process. Internet technologies therefore allow for both facilitation and repression, for emancipation and for control.

This, however, is not to suggest that technology in itself is neutral. While the answer to the machine may be in the machine, to use a common expression, the answer is not provided by the machine alone. While, as Lessig states "code is law" (Lessig, 2006, p. 1), neither code nor law constitute neutral, or politically or socially disconnected phenomena. Code, whether as a form of governance or as a set of written instructions to achieve a particular technological result (such as blocking certain kinds of content), is influenced by social, political, and cultural mores. It is difficult, if not impossible, to disassociate forms of content regulation and what content is deemed to be illegal, unethical, or otherwise undesirable from the sociopolitical and cultural context in which that regulation operates (see for example Zeno-Zencovich, 2008). For example, in China, a country considered Communist or (more recently) Authoritarian Capitalist, material deemed to challenge or

condemn the ruling party is forbidden. Access to pornography, which is deemed contrary to public morality, is also severely restricted. In comparison, in countries such as the U.S. or UK, where challenging the decisions of governmental actors is ostensibly perceived as a vital part of a healthy participative democracy, such content will not normally (or overtly) be restricted. Pornography, or other socially contentious material, may be less restricted or regulated than in countries such as China, save where the content in question is deemed to be illegal and/or obscene (such as child abuse images) or where it is subject to a "moral panic" (Breindl & Kuellmer, this issue; Jenkins, 2001; Wagner, this issue). One example is that of the UK's "section 63" of the Criminal Justice and Immigration Act 2008, which concerns "extreme pornographic images" that are deemed illegal, such as acts likely to result in injury to sexual organs, regardless of whether that act was both performed with consent and not illegal in itself to perform. This controversial section (Johnson, 2010; Murray, 2009) was drafted as the result of a citizen campaign following a highly mediatized criminal case in which an individual with a history of viewing extreme pornography online was convicted of murdering a woman (Murray, 2009). In a more recent example, the UK's current Conservative-Liberal Democrat coalition government has announced successful negotiation with several Internet service providers for the establishment by January 2014 of an "opt-in" system that limits access to pornography and other forms of "extreme content" until a user specifically requests access to such content (Shubber, 2013). This is not to say that such laws or regulations are not subject to criticism or challenge, or that all members of a society wholly accept them. Instead, the purpose is to demonstrate that content regulation is ultimately determined by notions of acceptability, levels of social permissibility, and other cultural factors that are fluid and malleable.

The use of digital technologies, and the role of private actors in this form of content regulation, is not without its controversies. Brown (2010) refers to these processes as lacking procedural fairness and not having due regard for fundamental rights, with few schemes including "any substantive protection for individuals' rights to freedom of expression, association, or privacy" (p. 99). Frequently, the regulation of content on the Internet is the result of secretive negotiation processes rather than overt law making, which results in questions being raised over the lack of transparency and the legitimacy of online content regulation (Koumartzis & Veglis, 2011; Marsden, 2011, p. 12). This is particularly the case when dealing with information deemed to be highly confidential, such as that pertaining to national security (Rogerson & Milton, this issue). However, concerns over legitimacy and accountability can also be raised when "public" acts of regulation are performed by private entities without governmental oversight (or where such governmental oversight is limited and accountability mechanisms lacking), such as monitoring performed by bodies such as the Internet Watch Foundation in the UK (Wagner, this issue) or Freiwillige Selbstkontrolle Multimedia-Dienstanbieter in Germany (Breindl & Kuellmer, this issue). It is also possible for Internet-based systems of "regulated self-regulation" to be open to abuse, such as the use of copyright "notice and takedown" procedures as a way of suppressing embarrassing or damaging information, or silencing dissent. This is not to suggest that the potential for use of certain laws such as copyright laws for as a means of suppressing content is limited to notice and takedown on the Internet (see for example Patterson, 1987), but only that the use of the regulated self-regulation model and decision-making by private actors makes such actions easier on the Internet, and more difficult to challenge in the courts (Farrand, this issue). Nevertheless, the Internet can serve as a means of resisting these forms of content regulation, and indeed regulation both online and offline, through providing the means to more widely disseminate informational content and coordinate action between activists (Castells, 2011; see also Jensen, this issue; Smith, this issue). The same technologies that are used to remove or block access to Web sites can also be used as a means of protesting or raising awareness of issues, such as Wikipedia and other sites going "black" (thereby becoming inaccessible) to protest against the Stop Online

Piracy Act in the U.S. (see for example Smith, this issue). Furthermore, services such as the TOR onion browser can be used to allow near-anonymous use of the Internet and access to restricted content (Roberts, Zuckerman, York, Faris, & Palfrey, 2011)—although such services are neither immune from infiltration nor from their use for illegal content distribution, as was confirmed by the recent insertion of a security exploit by the FBI into Web sites hosted by Freedom Hosting, which identified users of the TOR browser as part of an investigation into the hosting and distribution of child abuse images (Poulsen, 2013). As has been discussed in this editorial, the Internet provides the means to both facilitate and suppress; to both allow and prevent activities deemed desirable in certain contexts, such as the provision of information detrimental to autocratic regimes; and to allow and prevent activities deemed undesirable, such as to distribute materials that are considered illegal or obscene. The purpose of this special issue of the *Journal of Information Technology & Politics* is to delve further into these issues, considering in greater detail the ways in which expression is governed in the digital environment, taking into account the ways the Internet can be used to facilitate and repress, and the regulatory structures that allow the Internet to be used in these ways. The next section of this editorial will provide an overview of these articles.

OVERVIEW OF THE ARTICLES IN THIS SPECIAL ISSUE

As evidenced by the previous sections of this editorial, the key theme of this special issue is that of networked governance and the role of public–private partnerships, coalitions, and agreements in the regulation of expression on the Internet. The six articles comprising this special issue consider content regulation as it pertains to materials generally accepted as illegal and harmful, such as sexual abuse images, to more contentious forms of content regulation, such as that of online copyright enforcement and the withholding of information deemed to be in the national security interest. In particular, this special issue considers the role of the Internet as both facilitator and suppressor of expression, as well as the facilitator and repressor of means of resisting that control. For this reason, articles focus both on the ways that the Internet is used as a means of regulating through multi-stakeholder processes, but also the way in which multi-stakeholder processes challenge contemporary modes of regulation.

The article by Yana Breindl and Bjoern Kuellmer on "Internet Content Regulation in France and Germany: Regulatory Paths, Actor Constellations, and Policies" focuses on how and why Internet content is regulated in liberal democracies, in particular considering how institutions are influencing such regulation. Based on actor-centered institutionalism and informed by technology-aware policy research, the article proposes two case studies that analyze online content regulation in France and Germany through technical filtering mechanisms. In order to answer how free speech is being regulated for each case study, the influence of institutional variables and actor constellation is analyzed, with a particular focus on private actors and self-regulation. As the article clearly demonstrates, France and Germany have chosen different regulatory paths. France has opted for a much more legislative control, whereas Germany has chosen self-regulation with limited public oversight. The divergence in paths between France and Germany is related to the different institutional settings and actor constellations that influence the governance of this field, resulting in different political debates. This text also highlights that filtering and blocking have become usual procedures, which are implemented by democratic and authoritarian governments alike. These processes are often outsourced to third parties, leading to problems of transparency and legitimacy. Finally, this article concludes by reiterating specified concerns with technical content regulation, in particular with regard to the protection of freedom of expression, privacy, rule of law, and due process.

Continuing with this theme of the private regulation of digital content, Ben Wagner's article on "Governing Internet Expression: How Public and Private Regulation Shape Expression Governance" explores how freedom of expression is governed online. The

emergence of the Internet has led to a redistribution of the governance capacity away from states towards private actors. Given that liberal democracies cannot directly intervene to regulate the actions of private actors in the area of media and communication technologies, this article explores what tools are left at the disposal of states to govern this specific area. Furthermore, the rapid expansion of the Internet and the limited capacity of public actors alone to regulate it have also led to the creation of a "space of expression," where different forms of speech do not always co-exist peacefully. The article looks at two case studies, one concerning a public actor and one concerning a private one: the U.S., which was the first state to consider strategies for online content regulation, and Facebook, a private actor that has achieved a de facto monopoly on social networking. The article analyzes how the freedom of expression is regulated, but also how the boundaries of free speech are established, considering the role of power as constitutive in defining such boundaries. More specifically, the article explores practices used in the creation of acceptable bounds for freedom of expression and their discursive framing, as well as the practices used for the implementation of such boundaries.

Whereas the previous two articles focus on the way in which content is regulated through agreements between private and public actors, and focusing on the relationships that foster this kind of regulation, Benjamin Farrand's article, "Regulatory Capitalism, Decentered Enforcement and its Legal Consequences for Digital Expression: The Use of Copyright Law to Restrict Freedom of Speech Online", considers the way in which copyright law can be misused as a means of suppressing embarrassing or politically sensitive information in the digital environment. In comparison to the previous articles, the predominant focus of this text is on the alleged abuse of such systems of regulation. Beginning with the consideration of contemporary governance as being an example of "regulatory capitalism," in which powers and activities that are traditionally considered the prerogative of the state are delegated to private, non-state actors in a form of "regulated self-regulation," this article argues that choice of governance structure impacts the way in which content is regulated. Whereas attempts to limit access to information considered sensitive through the use of copyright infringement allegations have been used in the offline environment, these attempts have been criticized by U.S. courts as a misuse of a law that was intended to ensure protection of information as a means of ensuring the dissemination of that content. However, as this article continues, the creation of a system of self-regulating "notice and takedown," where administrative decisions are made by private actors such as Internet intermediaries, makes the challenging of such decisions much more difficult, raising concerns over accountability and transparency. It also allows for the suppression of information by both state and non-state actors, indicating that the arguments in favor of limiting the application of the First Amendment (concerning freedom of speech) to the actions of public actors are less convincing within a system where private rather than state actors take an active role in the regulation of content.

Peter Jay Smith's article, "Speaking for Freedom, Normalizing the Net?", continues the analysis of how freedom of expression online can be limited through indirect ways through the usage of copyright legislation, and means by which it can be resisted. Departing from the idea that scholarly attention has increasingly been focusing on the control of online expression through censorship, in countries such as Iran and China, to the detriment of more concealed forms of control in liberal democracies, the author looks at U.S. attempts to curtail Internet freedoms through the adoption and enforcement of restrictive intellectual property legislation, such as the Anti-Counterfeiting Trade Agreement. Basing itself on the risk and security literature, the article focuses in particular on how the U.S. has, throughout the years, shifted the forum it uses to export copyright norms in an attempt to identify the most efficient venue. It also argues that such attempts have led to the emergence of widespread global resistance on the side of civil society, which is demanding the disappearance of online controls. The article concludes by pointing out that such resistance has diminished the capacity of the U.S. to impose its intellectual property norms through multilateral

negotiations, leading it to have recourse to bilateral agreements, which have, however, not been particularly efficient.

Continuing with themes of activism, resistance, and mobilization, Michael J. Jensen and Henrik P. Bang's article, "Occupy Wall Street: A New Form of Movement and Community?", discusses the means by which the Internet is providing the communication infrastructure necessary for the development and expansion of social movements, resulting in more innovative forms of collaboration and mobilization. Specifically, the online environment provides tools to shape meanings, knowledge, and identities. Within this context, the article compares old and new forms of social political movements. In order to study how the Occupy movement operates between the old and new forms of political participation, the authors develop an analytical framework that is based on four typologies. Focusing on the Twitter profiles of 50,000 participants, the article addresses how their conceptualization of the movement interacts with configurations of old and new forms of political participation involving both traditional associations concerned with voting and political parties, and the establishment of issue and cause-related politics. The article indicates that the variety of identities constructed and mobilized online during Occupy Wall Street (OWS) demonstrations do not coincide with the analyzed Twitter profiles, which are actually much more diverse than the image projected by the OWS movement. In particular, the authors find that the movement incorporated not only "leftist" or "liberal" actors, but also traditionally conservative and religious ones. This study shows, however, that common identities and interests are not automatically necessary for collective action to develop. Instead, the OWS movement appears to be one where participants develop and coordinate common action despite their social, cultural, moral, religious, and political differences, through mutual acceptance and recognition of difference.

In the final article, Kenneth Rogerson and Daniel Milton's "A Policymaking Process 'Tug of War': National Information Security Policies in Comparative Perspective" analyzes how states develop policies on information security. In comparison to other articles in this special issue, which highlight aspects of cooperation and cohesion between the interests of state and private actors in these forms of regulation, this text instead focuses on divisions in opinion between actors, and the inherent competition involved in establishing their preferred approaches as the commonly accepted one. Departing from the question of whether a greater flow of online information automatically leads to more democracy, the authors focus on how the flow of information is controlled and what arguments are used to justify such control. More specifically, the article explores ways in which we can understand competing policy makers' interests and the factors influencing the type of information security policy countries have. The authors propose that outcomes in information policy vary according to the type of information governments are attempting to control, that democracies often limit information when faced with external threats in order to protect their population, and that some countries attribute greater importance to privacy than others. As a result of such insights, the article concludes that the development of models to understand policymaking on information security must include elements as varied as the interests of the different actors involved in the field, the arguments they are presenting and the contexts in which they are proposing these arguments.

This special issue of the *Journal of Information Technology & Politics* constitutes a contribution to the development of the literature concerning governance on the Internet. It provides a range of different theoretical and methodological approaches, indicating that irrespective of approach taken, key themes such as the interaction between state and private actors become readily apparent. In particular, these articles indicate that certain concerns exist due to these forms of cooperation, including over transparency, legitimacy and accountability. For this reason, it is submitted that further research needs to be conducted in this field, going beyond the traditional Internet studies literature to take into account literature and theoretical conceptualizations that seek to consider the role of governance by private actors in a more holistic way. While this special issue focuses on the Internet as a form of "case study," and

seeking to reveal issues that arise as a result of this type of governance, the editors propose that this online content regulation is representative of a more general approach to governance that applies to both online and offline environments.

REFERENCES

Amable, B. (2003). *The diversity of modern capitalism*. Oxford, England: Oxford University Press.

Bartle, I., & Vass, P. (2007). Self-regulation within the regulatory state: Towards a new regulatory paradigm? *Public Administration*, *85*(4), 885–905.

Baumgartner, F. R. (2009). *Lobbying and policy change: Who wins, who loses, and why*. Chicago: University of Chicago Press.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven, CT: Yale University Press.

Berkman Center for Internet and Society. (2011). *International bloggers and Internet control*. Cambridge, MA: Roberts, H., Zuckerman, E., York, J., Faris, R., & Palfrey, J. G.

Bernhagen, P., & Bräuninger, T. (2005). Structural power and public policy: A Signaling Model of Business Lobbying in Democratic Capitalism. *Political Studies*, *53*(1), 43–64.

Bimber, B., Stohl, C., & Flanagin, A. J. (2009). Technological change and the shifting nature of political organization. In A. Chadwick & P. N. Howard (Eds.), *Routledge handbook of Internet politics* (pp. 72–85). London: Routledge.

Black, J. (2001). Decentering regulation: Understanding the role of regulation and self regulation in a "post-regulatory" world. *Current Legal Problems*, *54*(1), 103–146.

Braithwaite, J. (2008). *Regulatory capitalism: How it works, ideas for making it work better*. Cheltenham, England: Edward Elgar.

Bright, P. (2011, August 10). How the London riots showed us two sides of social networking. *Ars Technica.* Retrieved from http://arstechnica.com/tech-policy/news/2011/08/the-two-sides-of-social-networking-on-display-in-the-london-riots

Brown, I. (2010). Internet self-regulation and fundamental rights. *Index on Censorship*, *1*, 98–106.

Castells, M. (2011). *Communication power*. Oxford, England: Oxford University Press.

Christou, G., & Simpson, S. (2006). The Internet and public-private governance in the European Union. *Journal of Public Policy*, *26*(1), 43–61.

Coen, D., & Thatcher, M. (2008). Network governance and multi-level delegation: European networks of regulatory agencies. *Journal of Public Policy*, *28*(1), 49–71.

Culpepper, D. (2011). *Quiet politics and business power: Corporate control in Europe and Japan*. Cambridge, England: Cambridge University Press.

Dean, M. (2010). *Governmentality: Power and rule in modern society* (2nd ed.). London: SAGE.

Deibert, R., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (2008). *Access denied: The practice and policy of global Internet filtering*. Cambridge, MA: MIT Press.

Deibert, R., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: MIT Press.

Deibert, R., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (2012). *Access contested: Security, identity, and resistance in Asian cyberspace information revolution and global politics*. Cambridge, MA: MIT Press.

Deibert, R. J. (2009). The geopolitics of Internet control: Censorship, sovereignty, and cyberspace. In A. Chadwick & P. N. Howard (Eds.), *Routledge handbook of Internet politics* (pp. 323–336). London: Routledge.

Downing, L. (2008). *The Cambridge introduction to Michel Foucault*. Cambridge, England: Cambridge University Press.

Dutton, W. H., & Peltu, M. (2009). The new politics of the Internet: Multi-stakeholder policy-making and the Internet technocracy. In A. Chadwick & P. N. Howard (Eds.), *Routledge handbook of Internet politics* (pp. 384–400). London: Routledge.

Esterling, K. M. (2004). *The political economy of expertise: Information and efficiency in American national politics*. Ann Arbor: University of Michigan Press.

European Commission. (2009). *Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee: Enhancing the enforcement of intellectual property rights in the internal market* (No. COM(2009) 467 final). Brussels: European Commission.

Farrand, B. (2014). *Networks of Power in Digital Copyright Law and Policy: Political Salience, Expertise, and the Legislative Process*. London: Routledge.

Foucault, M. (2004). *Society must be defended: Lectures at the Collège de France, 1975–76*. (D. Macey, Trans.). London: Penguin.

Friedland, L. A. (1996). Electronic democracy and the new citizenship. *Media, Culture and Society*, *18*, 185–212.

Gil de Zúñiga, H., Veenstra, A., Vraga, E., & Shah, D. (2010). Digital democracy: Reimagining pathways to political participation. *Journal of Information Technology & Politics*, *7*(1), 36–51.

Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford, England: Oxford University Press.

Halliday, J. (2011, August 8). London riots: How BlackBerry Messenger played a key role. *The Guardian.* Retrieved from http://www.theguardian.com/media/2011/aug/08/london-riots-facebook-twitter-blackberry

Harvey, D. (2007). Neoliberalism as creative destruction. *The ANNALS of the American Academy of Political and Social Science*, *610*(1), 21–44.

Héretier, A., & Eckert, S. (2008). New modes of governance in the shadow of hierarchy: Self-regulation by industry in Europe. *Journal of Public Policy*, *28*(1), 113–138.

Jenkins, P. (2001). *Beyond Tolerance: Child Pornogaphy on the Internet*. New York: New York University Press.

Johnson, D., & Post, D. G. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, *48*, 1367.

Johnson, P. (2010). Law, morality and disgust: The regulation of "extreme pornography' in England and Wales. *Social & Legal Studies*, *19*(2), 147–163.

Kelly, M. G. E. (2012). *The political philosophy of Michel Foucault*. London: Routledge.

Kiersey, N. J. (2011). Neoliberal political economy and the subjectivity of crisis: Why governmentality is not hollow. In N. J. Kiersey & D. Stokes (Eds.), *Foucault and international relations: New critical engagements* (pp. 1–24). New York: Routledge.

Koimann, J. (2000). Societal governance: Levels, modes, and orders of social-political interaction. In J. Pierre (Ed.), *Debating governance: Authority, steering, and democracy* (pp. 138–166). Oxford, England: Clarendon.

Koumartzis, N., & Veglis, A. (2011). Internet regulation: The need for more transparent Internet filtering systems and improved measurement of public opinion on Internet filtering. *First Monday*, *16*(10). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/3266/3071

Lanier, J. (2013). *Who owns the future?* London: Allen Lane.

Lessig, L. (2004). *Free culture: The nature and future of creativity*. New York: Penguin Press.

Lessig, L. (2006). *Code 2.0*. New York: Basic Books.

Levi-Faur, D. (2005). The rise of regulatory capitalism: The global diffusion of a new order. *The ANNALS of the American Academy of Political and Social Science*, *598*(1), 12–32.

Lütz, S., Eberle, D., & Lauter, D. (2011). Varieties of private self-regulation in European capitalism: Corporate governance codes in the UK and Germany. *Socio-Economic Review*, *9*(2), 315–338.

MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for Internet freedom*. New York: Basic Books.

Marcussen, M., & Torfing, J. (2003). Grasping governance networks. *Centre for Democratic Network Governance Working Paper Series*, *5*, 1–31.

Marsden, C. T. (2011). *Internet co-regulation: European law, regulatory governance and legitimacy in cyberspace*. Cambridge, England: Cambridge University Press.

Marsh, D., & Rhodes, R. A. (1992). *Policy networks in British government*. New York: Oxford University Press.

McGreal, C. (2010, April 5). WikiLeaks reveals video showing US air crew shooting down Iraqi civilians. *The Guardian.* Retrieved from http://www.theguardian.com/world/2010/apr/05/wikileaks-us-army-iraq-attack

McIntyre, T. (2012). Child abuse images and cleanfeeds: Assessing Internet blocking systems. In I. Brown (Ed.), *Research handbook on governance of the Internet* (pp. 277–308). Cheltenham, England: Edward Elgar Publishing.

Morozov, E. (2011). *The net delusion: The dark side of Internet freedom*. New York: PublicAffairs.

Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press.

Murray, A. D. (2009). The reclassification of extreme pornographic images. *The Modern Law Review*, *72*(1), 73–90.

Parker, C. (2002). *The open corporation: Effective self-regulation and democracy*. New York: Cambridge University Press.

Patterson, L. R. (1987). Free speech, copyright and fair use. *Vanderbilt Law Review*, *40*, 1.

Poulsen, K. (2013, August 5). Feds are suspects in new malware that attacks Tor anonymity. *Wired*. Retrieved from http://www.wired.com/threatlevel/2013/08/freedom-hosting/

Price, M. E., & Verhulst, S. G. (2005). *Self-regulation and the Internet*. The Hague: Kluwer Law International

Shirky, C. (2011). *Cognitive surplus: Creativity and generosity in a connected age*. London: Penguin.

Shubber, K. (2013, June 14). ISPs to include porn filters as standard in UK by 2014. *Wired UK*. Retrieved from http://www.wired.co.uk/news/archive/2013-06/14/parental-filtering-industry-standard

The Guardian. (2013, June 8). The NSA files. Retrieved from http://www.theguardian.com/world/the-nsa-files

Veyne, P. (2010). *Foucault: His thought, his character*. Cambridge, England: Polity.

Ward, S., & Gibson, R. (2009). European political organizations and the Internet: Mobilization, participation, and change. In A. Chadwick & P. N. Howard (Eds.), *Routledge handbook of Internet politics* (pp. 25–39). London: Routledge.

Wright, J. S. (2011). Regulatory capitalism and the UK Labour Government's reregulation of commissioning in the English National Health Service. *Law and Policy*, *33*(1), 27–59.

Wu, T. (2010). *The master switch: The rise and fall of information empires*. New York: Random House.

Yu, K. (2010). The graduated response. *Florida Law Review*, *62*, 1373–1430.

Zeno-Zencovich, V. (2008). *Freedom of expression: A critical and comparative analysis*. Abingdon, Oxon, England: Routledge-Cavendish.

Zittrain, J. (2008). *The future of the Internet: And how to stop it*. London: Allen Lane.