Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics

Leonie Maria Tanczer, Ryan McConville, and Peter Maynard

Queen's University Belfast

Keywords: censorship, surveillance, cryptography, encryption, academic freedom, Internet

The "Snowden leaks" and censorship methods used during the Arab Spring have brought warranted attention to technologically supported censorship and surveillance (Bauman et al. 2014; Deibert and Crete-Nishihata 2012, 344). The public is now aware how digital tools and information are prone to tracing, interception, and suppression. Processes of eavesdropping and information collection (i.e., surveillance) are often interrelated with processes of removal, displacement, and restriction of material or speech (i.e., censorship). Both are often enshrouded in secrecy, leaving censorship and surveillance techniques open to abuses (Setty 2015).

Digital censorship and surveillance may also constitute a threat to academic freedom. Technologically supported censorship and surveillance impinge upon scholars' ability to conduct unobstructed inquiry. The increasing reliance on the Internet and other information and communication technologies (ICT) to collect data or distribute findings has only exacerbated this threat. Digital tools and data allow for: (1) the easier confiscation or destruction of research (Cyranoski 2008, 871; Gellman 2015); (2) the manipulation of information; or (3) the control and prevention of access to information (Fishman 2010). Digital surveillance creates a securitized climate and leads to chilling effects. The field of security studies is certainly not immune to these effects.

We aim to systematically explore the methods of digital censorship and surveillance, as well as techniques to resist them. The article is split into three parts. The first section discusses why academia—and especially security studies scholars—should engage in debates on technological information control. The second section outlines how the digital tools used by academics can be subject to censorship, and how this affects the profession. The final section examines what to do against digital censorship and surveillance, and explores whether cryptographic circumvention methods should be included within academic teaching and scholarship. As part of this discussion, we hope to foster a debate about the legal and technical protections for researchers, and engender a critical reflection about digital security.

The Why

Academics are exhorted to participate in debates about technological information controls because such controls are seen as inextricably linked to human rights. The rights to privacy and unfettered correspondence as well as the rights to freedom of opinion and expression constitute fundamental pillars upon which opposition to censorship and surveillance rest. Recently, the United Nations Human Rights Council adopted a resolution declaring the unequivocal application of human rights in the online sphere (UNHRC 2016). Dating further back, Article 19 of the International Covenant on Civil and Political Rights (1976) includes the right to seek, receive, and impart information through any media, regardless of frontiers. This Article is essential for the scholarly profession, as it touches upon the fundamental idea of unrestricted academic inquiry.

The principle of academic freedom also embodies rights to unimpaired access of information and unrestricted scholarship. Academic freedom allows for independent teaching, research, and scholarly expression, crucial to advancing expertise, critical thinking, and general knowledge (Altbach 2001, 205). Its importance has been discussed at great length (Wilson 2005; Falk 2007; Heisler 2007; Mittelman 2007). Academic freedom gives researchers the security to voice concerns and publish research that does not necessarily reflect official policies or public opinion. However, this "professorial freedom of teaching, research, and expression" (Altbach 2013, 138) is progressively suffering in the securitized post-9/11 climate with its over-emphasis on secrecy and "preemptive security practices" (Falk 2007; de Goede 2014, 101).

Scholars exploring sensitive issues and information in the "digital age" are affected by censorship in several

Tanczer, Leonie Maria et al. (2016) Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics. *Journal of Global Security Studies*, doi:10.1093/jogss/ogw016

ways. Most obviously, they need to be aware that information freely accessible online is often filtered and, thus, censored. This raises questions about where to find and how to gain access to digitized information that is *not* freely available. In turn, researchers must think carefully about how to protect digitized data from third-party access. They must be aware that research utilizing ITCs and involving politically sensitive topics can lead to digital surveillance and information control.

Restrictions affecting the higher education sector have, in the course of the past decade, been primarily implemented through regulatory means. For instance, both the US Patriot Act of 2001 and the UK Counter-Terrorism and Security Act of 2015 have been shown to impede academic staff as well as students (Wilson 2005; Newman 2008; Hall 2015). In addition, less obvious manifestations of censorship are connected to: (1) the changing nature of academic funding (Hedgecoe 2015); (2) the restriction to official documents (Barry and Bannister 2014); and (3) constraints in scholarly communication systems (Moran and Mallory 1991; Nye and Barco 2012). Indeed, in 2015, the International Studies Association (ISA) was suspected of refusing to publish papers that drew on diplomatic cables released on the whistle-blower platform WikiLeaks (Michael 2015; see also O'Loughlin, 337–345). Although the ISA (2015) issued a statement rejecting these practices, the allegation reinforces the growing need for international relations scholars—and particularly security studies scholars—to consider and grapple with the problems of information control.

While scholars such as Heisler (2007, 351) acknowledge these "conventional" threats to academic freedom, many others still fail to link this phenomenon with the growing process of digitalization. They ignore that censorship and academic freedom are not only "shaped by the times" (Mittelman 2007, 364) but also by technological developments. The higher education sector is increasingly using, and also reliant upon, the Internet and associated ICTs. Technologically supported censorship and surveillance practices subsequently challenge the academic profession, and oblige researchers to reconsider the role they may have on their work, as well as on their research subjects.

Most notably, digital information allows for not only easier content duplication and distribution, but also easier restriction. This can occur in an unwanted manner, and with the interference of commercial and governmental actors, criminals, or mere curious lurkers. It indicates *why* academia has to think more thoroughly about the potential implementation of circumvention methods. Researchers are facing novel ethical, security, and privacy challenges that affect both themselves and their participants. Security scholars are therefore advised to reflect upon potential risks *through* and *in* cyberspace (Deibert and Rohozinski 2010, 17). It is of the utmost importance to question "techno-fallacies" (Marx 2007), as beliefs in alleged technological neutrality make academics inattentive to the negative side effects of ICTs.

In particular, traditional research processes involving the collection, analysis, storage, presentation, and reuse of data need to be reassessed. While digital data and online communication are essential for the daily practice of research, they can also put participants in danger. Information—and especially digital information—needs to be responsibly collected, managed, and stored. Some fields aim to increase transparency and replication via developments such as the Data Access and Research Transparency (DA-RT 2016) initiative. A key aspect of DA-RT involves cited data published in a trusted data repository. It requires authors to make the empirical foundation of their research as accessible as possible. Given the sensitive and secretive nature of the topics security scholars investigate striking the right balance between openness and transparency on the one hand, and the rights to privacy and security on the other, can pose a significant challenge. For instance, the high-profile Boston College tape lawsuit vividly displayed how confidentiality agreements with participants were legally leveraged. In this instance, participants' confidentiality was suspended due to a legal bid to gain access to interviews with former paramilitary members (Sampson 2015). The lawsuit exhibits this openness versus privacy dilemma, but also underlines how the collection of information leaves traces that can result in unanticipated consequences for participants and researchers.

The balance between data transparency and the responsibility to protect sources is further complicated by the move toward digital technologies. While technological developments have made data protection technically possible, they have also created legal problems. This was illustrated in the case of former UK PhD student Bradley Garrett, whose research data was confiscated and used in court proceedings against his subjects (Garrett 2014). Garrett's work focused on the topic of "place hacking" and involved the observation of groups that visited off-limited spaces, putting his participants and ultimately his whole research project on the edge of the law. As a result of the adverse outcomes for both him and his participants, Garrett (2014) emphasized the need for the academic community to stand up against such actions by the authorities and more carefully consider data collection and protection procedures.

These examples raise important questions about the legal status of scholars, the safeguarding of academics and participants, and, more profoundly, technological data safety and integrity. At this moment in time, many universities and researchers still seem oblivious to these questions. While there are plenty of publications associated with the ethics and methods of the digital age (Ackland 2013; Mutlu 2015), the digital security and protection of researchers and their subjects are barely addressed. In this regard, security studies scholars have failed to properly understand the implications of digitalization on their own research practices. A discussion about digital information control and the implementation of resistance techniques is therefore overdue. Researchers need to understand both how online surveillance and digital censorship operate and how to circumvent and protect themselves from these practices. The next two sections will shed some light on these areas.

The How

Having outlined some of the reasons why security scholars must engage with digital information control, we now examine how censorship is technically implemented, and how it can obstruct the academic profession. Eriksson and Giacomello (2009, 206) already accentuated the importance of studying Internet controls. Technology allows for different manifestations of censorship and surveillance practices, ranging from severely intrusive and restrictive to more subtle and unapparent forms. In this regard, academics may never be aware of clear infringements on, or interferences with, their work. Nevertheless, even if such techniques are "invisible" and/or based solely on the collection of electronic information, they can pose problems for scholars.

One substantial and invasive censorship method is Internet content filtering and blocking. It is often facilitated through the application of firewalls at the national and/or Internet Service Provider (ISP) level (Liang and Lu 2010; Wagner 2014, 61). It is the equivalent to borrowing a book from a library only after the librarian reads and assesses the content for suitability. If the book is deemed unsuitable, it is destroyed rather than lent out. While techniques vary, content restrictions are common across states and frequently supported by commercial and non-commercial institutions. The most renowned instance is the "Great Firewall of China" (Deibert 2002). However, the control of online information is becoming increasingly widespread, meaning that these measures are not restricted merely to oppressive regimes; increasingly liberal states engage in such illiberal practices (Reporters without Borders 2014, 3).

The United Kingdom, for instance, filters web access by default through ISPs. Although users have the ability to opt out of content blocking, there have been numerous reports of "legitimate" websites being censored. The restrictions included content related to sexual education and domestic abuse (Smith 2013), as well as politicians' websites (Burrell 2013). More examples of governmental content blocking can be found in countries such as India and Russia (Kashmir Media Service 2014; Roth and Herszenhorn 2014), and projects such as the *OpenNet Initiative* have documented many other examples of state-sponsored content blocking (Deibert et al. 2008, 2010, 2011; ONI 2016). Taken together, they demonstrate how the growing implementation of online blocking can hinder a comprehensive assessment of information, which is particularly important for security scholars in times of, for instance, elections or uprisings (Deibert and Rohozinski 2010, 27).

A more apparent effect of content filtering on the daily practice of researchers is seen at the university and library level, representing a challenge to the professorial freedom of research and expression. A recent study by the British "Managing Access to the Internet in Public Libraries" project indicates that filtering software is ubiquitous in libraries (Muir et al. 2016). Two-thirds of the surveyed UK libraries had received complaints about the over-blocking of websites, including the inability to access virtual learning environments and difficulty with rapidly unblocking content as a result of the filtering software. These findings echo those of previous studies, which found that such technologies have the potential to inadvertently restrict access to legitimate educational sources (Peace 2003; Jaeger et al. 2006).

In addition to these blunt censorship methods, mass data collection and analysis by institutional, commercial, and governmental actors pose risks to the academic community. A particular sub-field of data analytics is user profiling. This involves computer algorithms that discover patterns from personal data and proceed to identify correlations in these patterns among (groups of) individuals (Hasan et al. 2013). These algorithms construct profiles that foster "practices of exceptionalism" by including or excluding people and groups based on anticipated behaviors (Bigo 2006, 47). The accuracy of these profiles is fundamentally influenced by the data the algorithm receives, leading to potential misrepresentations.

Profiling technologies are already commonly used within the higher education sector. They are typically employed to monitor students' behavior and performance (Warrell 2015; *Harvard Magazine* 2014). However, variations of these technologies may also put academics under close watch. Specifically, security scholars who frequently investigate sensitive and controversial topics such as "terrorism" or "torture" can be earmarked for scrutiny. Professor Richard Jackson, Editor-In-Chief of the journal *Critical Terrorism Studies*, posted on Twitter that the New Zealand police had recently questioned him regarding his connection to terrorism (Jackson 2016). He thereafter speculated on whether his research and, in particular, blog posts in which he proposed to be a "terrorist sympathizer" led to the police questioning (Jackson 2015). In this regard, online monitoring and corresponding data analytics add to the history of academics being prime targets for intelligence and security service surveillance (White 2008).

Indeed, the mere knowledge that every website visited, web search performed, and message sent may be collected, stored, and analyzed can restrict online behavior. In the digital age, "big data" becomes an "'abstract authority' of knowledge" (Aradau 2015, 28). Multiple publications highlight how online surveillance leads to "chilling effects," discouraging users from writing, uploading, and posting material (Dawson 2006; Townend 2014; see also Pelopidas, 326–336). Two recent studies on the effects of the Snowden revelations show how perceptions of surveillance contribute to an online spiral of silence (Stoycheff 2016) and a significant drop in the amount of web traffic to "privacy sensitive" Wikipedia articles (Penney 2016). The impact of online self-censorship has also been ascertained by the PEN American Center (2013). PEN identified that one in six writers and editors admitted avoiding writing on a topic they believed would subject them to online surveillance. This raises questions about the amount of research not being conducted due to anticipated adverse ramifications.

Technologically supported censorship is not only limited to the communication and dissemination of information. It may also take the form of equipment confiscation or affect the storage and transport of digital material. A number of states, including the United States, Canada, and the United Kingdom, permit customs authorities to search the laptops of those entering the country (Burrell 2015). Both reporters and academics have had their laptops or data seized at Heathrow Airport (Topping 2013; Garrett 2014). Without proper precautions, data can be (accidentally or purposefully) impounded or destroyed. This can affect researchers even when they believe that they are acting within the law of a given jurisdiction. For example, foreign researchers conducting meteorological examinations in China had their equipment seized (Cyranoski 2008, 871). Although their equipment was returned, the Chinese tampered with many of their instruments. Digital data in particular is prone to such interceptions. Techniques exist that allow for the deletion of data beyond recovery (Wei et al. 2011).

The censorship and surveillance practices outlined above are complicated by the active endeavor to break and sabotage cryptographic techniques. The subversion ranges from efforts to influence technical standard bodies to those that exploit software and hardware vulnerabilities (Perlroth, Larson, and Shane 2013). In particular, intelligence agencies have an interest in breaking the very encryption that is essential for scholars to ensure secure communication or data storage (Ball, Borger, and Greenwald 2013). They support research into the ability to deanonymize Internet activity, sometimes with help of academic institutions or commercial actors (Cox 2016; Kushner 2016). In contrast, a report by the United Nations Special Rapporteur on freedom of expression provided strong support for the defense of anonymity and encryption (UNHRC 2016). Similarly, McKune (2015) calls the attempt to disrupt these tools a violation of the "right to science." Yet, in the current securitized climate, cryptographic tools are constantly threatened. This not only creates a risk due to the inability to protect material from intrusion. In the worst case, it can have the effect of discouraging research involving confidential, high-risk (re-)sources, limiting the comprehensive understanding of society overall.

The What (to Do)

The final part of this paper delineates methods for circumventing some technological information controls. Although we acknowledge that these issues require substantial political and social changes, we strongly believe that scholars can make gains by fighting these censorship and surveillance practices with technology. Indeed, one of the few articles addressing security issues in the scholarly profession has been published in the *Research Ethics Review*. Aldridge, Medina, and Ralphs (2010) provide fourteen guidelines for securing digitally held data. The authors refer to the importance of strong passwords, the need for secure storage and deletion of data, and the applicability of encryption software for researchers' computers and online communication. Extending this previous work, we hope to galvanize the security studies profession around the need for a broader examination of cryptographic tools to circumvent technologically supported censorship and surveillance practices.

Two essential principles when bypassing censoring filters and monitoring systems are: (1) the routing of connections over less restrictive network paths; and (2) the modification of data prior to transit to prevent eavesdropping and the identification of activities. However, this is not to say that full anonymity is guaranteed. Despite modified or rerouted connections, an adversary with the required budget or substantial skills could overcome these efforts (Dahal et al. 2015). The methods can, thus, only improve the odds of remaining anonymous.

One way of anonymizing online traffic is through tools such as the Onion Router (Tor). Although the Tor project provides a collection of software, the easiest approach is to employ the Tor browser bundle. It is similar to any other web browser, but it encrypts and routes data through intermediary machines (i.e., nodes) before reaching its intended destination. By routing data through these different nodes, Tor avoids sending traffic directly. To put it more simply, the encrypted traffic basically "jumps" through the network before leaving the final exit node. Tor consequently cloaks the original source and intended destination, reducing the chance of someone successfully monitoring or censoring the connection. Despite the potential for misuse and its ability to be identified and blocked, Tor increases the anonymity of users (Moore and Rid 2016). This makes Tor a common instrument used by law enforcement, journalists, and activists (Lewman 2013). Similarly, Tor provides options for academics in suppressive environments to obtain uncensored information, but it could also be useful for any scholar researching sensitive or restricted topics.

Another way of overcoming censoring or monitoring network controls is by using a Virtual Private Network (VPN). A VPN is typically employed to send traffic in a secure manner over an insecure network. It is advantageous when using a public or untrusted Internet connection, for example, at airports. It prevents others who are also part of the network from intercepting and modifying network traffic, avoiding so-called man-in-the-middle attacks (Desmedt 2011). Thus, it involves creating a secure tunnel between one's device (i.e., laptop; Point A) and the VPN (Point B), using the untrusted Internet connection. Through this connection one can then securely access the actual service one wants to reach (Point C). Additionally, VPNs are frequently utilized to connect employees to internal employer networks, or in academic settings to access journal papers/services from geographically separated networks beyond the university (Wolinsky et al. 2010). Hence, in the course of such a process, the traffic is routed in a manner as if the device was accessing the content directly from within a private network.

VPNs also help hide the data that is being transmitted. The process can be explained through the metaphor of having paper wrapped around a translucent tube (i.e., the Internet), that is, through the VPN, now hidden behind an opaque coating. Although the actual transfer process can—similar to the application of Tor—potentially be detected and blocked, it provides a helpful method when sending data securely via a machine that is, for example, outside a conflict zone, or if there is a requirement to bypass the ISP or internal university restrictions. Unlike Tor, VPNs do not provide any form of anonymization, but employ both of the earlier-mentioned principles: they route traffic over an unrestricted network through the VPN server, and encrypt traffic between the Internet-enabled device, for example a researcher's laptop, and the VPN.

There are other methods that facilitate the secure storage and transmission of data. The encryption of data is a way to elude censorship or surveillance, thus ensuring data integrity and preventing intellectual property from falling into the wrong hands. As universities are increasingly becoming hubs for the generation of new knowledge and innovation, the possible theft of intellectual property is a fundamental concern for scholars. The prospect of, for instance, economic espionage may convince those skeptical of purely ethical arguments to apply encryption techniques within the remits of higher education. The encryption of data on computers, cloud services, and removable media devices—such as USB drives—may be achieved through software such as Veracrypt or GnuPG (GPG). Both guarantee password-protected access to documents or folders.

In addition to secure data storage, academics can benefit from the usage of encrypted communication methods. A recent ruling by the European Court of Human Rights (ECtHR) (*Bărbulescu v. Romania*) highlighted that employers are allowed to read messages of employees sent through institutional accounts (Rawlinson 2016). For security studies scholars and academics in general, the decision is of significant importance when planning to communicate with research subjects through online means. The ECtHR case mirrors revelations about similar practices in the United States, such as the secret monitoring of Harvard University's deans' email accounts to search for potential media leaks (Carmichael 2013). These examples reveal that secure and unmonitored communication is not fully guaranteed. Nonetheless, GPG can encrypt email content, provided that sender and receiver have correctly configured GPG on their machines.

A further method to communicate without fear of interception and/or modification is through a protocol called Off-the-Record (OTR). OTR is commonly used over instant messaging protocols and can be applied when using social media sites such as Facebook (Bian, Seker, and Topaloglu 2007). Encrypted instant messaging services such as Signal, as well as multiplatform voice and videoconferencing applications such as Jitsi, are also beneficial when organizing or conducting interviews with research subjects.

There are, of course, far more tools available that academics can incorporate into their daily practice. They range from password managers that allow for large character and number combinations to be securely stored, to alternative operating systems such as Tails. Tails is a live operating system, which is booted via a DVD, USB stick, or SD card rather than the internal, more permanent, hard disk storage device. By default, Tails leaves no trace on the actual computer. It is, thus, a convenient application for researchers when traveling, allowing for not only secure retention of research records but also their consequent destruction. Tails and the other techniques outlined here are some of the many free software projects used by journalists working on sensitive issues (Greenberg 2014), that would certainly also be valuable for the academic and, in particular, the security studies scholar.

Akin to Zevenbergen's (2016) guidelines that inform research's ethical assessment and encourage stakeholders to minimize risks before the data collection takes place, we hope to stimulate reflexivity. A culture of security sensitivity and greater awareness of technological pitfalls will provide the best way forward. We acknowledge that not all researchers are equally affected by the discussed censorship techniques, and that they may affect researchers working in diverse socio-political and socio-technical contexts in different ways. Thus, not all will need the tools we outline here. However, these tools are important to consider when working on certain topics or with particular participants. They may also be helpful during fieldwork in specific countries or conflict zones, and valuable when handling sensitive data that may compromise the privacy, integrity, and/or life of participants and researchers. Ultimately, we encourage security studies scholars to fundamentally scrutinize their use of the Internet and ICTs and take up methods that would be auxiliary in their research.

These discussed cryptographic tools should complement general computer security recommendations[1] and can be used, for example, to improve anonymity in the course of the research and data collection process. Academics should be cautious with their application. The information is published in good faith and for informational purposes. We stress the necessity of following regulatory requirements set out by institutions, ethics committees, or other bodies. Taking these extra measures can help protect scholars and their data, but also put them at additional risk.

We therefore emphasize, first, that the usage of these techniques can be restricted, resulting in breaches of contracts and/or legislation. Encryption and circumvention tools can be, if not outlawed, flagged as evidence of suspicious activity (Cheredar 2014). Second, we acknowledge that such technical recommendations put the burden on scholars to secure themselves. The instruments require some technological knowledge, and sometimes expenses that scholars may not have. Improperly safeguarding oneself can give a false sense of security and may put researchers and their subjects in danger. It is therefore recommended that scholars seek, if necessary, advice from IT professionals.

It is also important to emphasize that none of the techniques outlined here, nor any of the named products, are "recommended" as such. A crucial take-away is that researchers often cannot solely rely on any of the outlined steps alone. As technology changes rapidly, instruments, practices, and procedures have to adapt. Thus, we encourage researchers to keep up to date with the changing landscape of anti-surveillance and anti-censorship tools. Discussions taking place in the fields of digital sociology and surveillance studies (Martin, Van Brakel, and Bernhard 2009; Lyon 2013, 2014) are useful, as is the work of non-profit digital rights groups such as the Electronic Frontier Foundation as well as the worldwide Cryptoparty movement.

Conclusion

This contribution examined the *why, how*, and *what to do* in relation to technologically supported censorship and surveillance practices. We encourage academics to pay more attention to these aspects and to think more carefully about the consequences of digitalization. The "digital revolution" has had profound effects on the right to privacy; the ability to seek, receive, and impart information; and the core principles of academic freedom. We therefore encourage scholars to include cryptographic tools among the methods they consider for research and communication. These can equip researchers with a suit-

[1] Such as regular software updates, well-wrought backup schemes, usage of anti-virus software, strong passwords, secure Internet connection (HTTPS), and the active monitoring of security alerts.

able toolkit for bypassing technologically supported censorship and surveillance practices and help improve the anonymity and confidentiality of research processes. Since these methods also pose risks, we encourage scholars to be mindful when using these mechanisms and to seek both legal and technical assistance.

Aside from outlining these technical circumvention methods, we also hope to encourage a culture of critical reflection about digital practices. This reflection requires closer examination of the complicated links between secrecy, surveillance, and censorship, and the need to balance openness, transparency, security, and privacy. Any questioning of censorship and surveillance techniques also demands the instillation of security sensitivity and awareness. Security speaks to behavior far more than it does to technology. Challenging online censorship and surveillance is, thus, not simply a matter of setting up devices and downloading software. It requires critical evaluation of what it means to send sensitive messages, to click on attachments, or to store data online. Addressing these behavioral limitations is far more profound, and needs to go hand-in-hand with the here-proposed technological measures.

We hope to initiate a debate about the legal status and technical support of academics, aligning with recent calls for more safeguarding of universities' personnel (Academics Anonymous 2016). Researchers and their participants should receive the same levels of protection as journalists and their sources. All of the here-mentioned aspects can impact the daily practices of academics, the training of students and staff, and the composition of ethics committees. The latter would profit from ethical, legal, and technical advice. We therefore encourage institutional review boards to develop an understanding of these issues so that they can sufficiently evaluate the security protocols academics propose.

Finally, this article endeavored to raise questions for the higher education sector. It is critical that academics across all disciplines question how universities can defend academic freedom. Security scholars in particular are exhorted to drive these discussions to ensure the best possible protection for both ourselves as well as our research subjects, allowing for independent, critical research in the digital age to proceed.

Acknowledgments

The authors are indebted to Amalia Campos Delgado, Jana Eyssel, Josh Milburn, Anne Schroeter, Kyle Shuttleworth, Pauric Ward, and all participants of the Leverhulme (LINCS) PhD Reading Group. We are grateful for their wise and helpful suggestions on earlier drafts and would also like to thank the anonymous reviewers and the editors for their insightful comments.

References

Academics Anonymous. 2016. "Universities Must Do More to Protect PhD Students Working in Dangerous Countries." *The Guardian*. Accessed May 13, https://www.theguardian.com/higher-education-network/2016/may/13/universities-must-do-more-to-protect-phd-students-working-in-dangerous-countries.

Ackland, Robert. 2013. *Web Social Science: Concepts, Data and Tools for Social Scientists in the Digital Age*. London: Sage.

Aldridge, Judith, Juanjo Medina, and Robert Ralphs. 2010. "The Problem of Proliferation: Guidelines for Improving the Security of Qualitative Data in a Digital Age." *Research Ethics Review* 6 (1): 3–9.

Altbach, Philip G. 2001. "Academic Freedom: International Realities and Challenges." *Higher Education* 41 (1): 205–19.

——. 2013. *The International Imperative in Higher Education*. Rotterdam: SensePublishers.

Aradau, Claudia. 2015. "The Signature of Security: Big Data, Anticipation, Surveillance." *Radical Philosophy* 191 (May–June): 21–28.

Ball, James, Julian Borger, and Glenn Greenwald. 2013. "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security." *The Guardian*. Accessed September 6, https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

Barry, Emily, and Frank Bannister. 2014. "Barriers to Open Data Release: A View from the Top." *Information Polity* 19 (1–2): 129–52.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and Rob B. J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8 (2): 121–44.

Bian, Jiang, Remzi Seker, and Umit Topaloglu. 2007. "Off-The-Record Instant Messaging for Group Conversation." Paper presented at the IEEE International Conference on Information Reuse and Integration (IRI), Las Vegas, NV.

Bigo, Didier. 2006. "Security, Exception, Ban and Surveillance." In *Theorizing Surveillance. The Panopticon and Beyond*, edited by David Lyon, 46–68. Milton: Willan.

Burrell, Ian. 2013. "O2 Changes Porn Filter after Charity Sites Blocked." *The Independent*. Accessed December 23, http://www.independent.co.uk/life-style/gadgets-and-tech/news/o2-changes-porn-filter-after-charity-sites-blocked-9023209.html.

——. 2015. "Police Use Terror Powers to Seize BBC Newsnight Journalist's Laptop." *The Independent*. Accessed October 28, http://www.independent.co.uk/news/uk/crime/police-use-terror-powers-to-seize-bbc-newsnight-journalists-laptop-a6712636.html.

Carmichael, Mary. 2013. "Harvard Secretly Searched Deans' E-mail: Chasing Leak in Cheating Scandal May Have Invaded Privacy." *Boston Globe*. Accesssed March 10, https://www.bostonglobe.com/metro/2013/03/10/harvard-university-administrators-secretly-searched-deans-email-accounts-hunting-for-media-leak/tHyFUYh2FNAaG2w9wzcrLL/story.html.

Cheredar, Tom. 2014. "NSA Views Encryption as Evidence of Suspicion and Will Target Those Who Use It, Security Journalist Says." *VentureBeat*. Accessed March 10, http://venturebeat.

com/2014/03/10/nsa-views-encryption-as-evidence-of-suspicion-and-will-target-those-who-use-it-security-journalist-says/.

Cox, Joseph. 2016. "Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed by Feds." *Motherboard*. Accessed February 24, http://motherboard.vice.com/read/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds.

Cyranoski, David. 2008. "Check Your GPS at the Border." *Nature* 451 (7181): 871.

Dahal, Saurav, Junghee Lee, Jungmin Kang, and Seokjoo Shin. 2015. "Analysis on End-To-End Node Selection Probability in Tor Network." Paper presented at the International Conference on Information Networking (ICOIN), Siem Reap, Cambodia.

DA-RT (Data Access and Research Transparency). 2016. Data Access and Research Transparency. Accessed June 24, 2016, http://www.dartstatement.org/.

Dawson, Shane. 2006. "The Impact of Institutional Surveillance Technologies on Student Behaviour." *Surveillance & Society* 4 (1–2): 69–84.

de Goede, Marieke. 2014. The Politics of Privacy in the Age of Preemptive Security." *International Political Sociology* 8 (1): 100–18.

Deibert, Ronald J. 2002. "Dark Guests and Great Firewalls: The Internet and Chinese Security Policy." *Journal of Social Issues* 58 (1): 143–59.

——. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press.

——. 2011. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Cambridge, MA: MIT Press.

Deibert, Ronald J., and Masashi Crete-Nishihata. 2012. "Global Governance and the Spread of Cyberspace Controls." *Global Governance* 18 (3): 339–61.

Deibert, Ronald J., John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2008. *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Deibert, Ronald J., and Rafal Rohozinski. 2010. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology* 4 (1): 15–32.

Desmedt, Yvo. 2011. "Man-In-The-Middle Attack." In *Encyclopedia of Cryptography and Security*, edited by Henk C. A. van Tilborg and Sushil Jajodia, 759. New York: Springer.

Eriksson, Johan, and Giampiero Giacomello. 2009. "Who Controls What, and Under What Conditions?" *International Studies Review* 11 (1): 206–10.

Falk, Richard. 2007. "Academic Freedom Under Siege." *International Studies Perspectives* 8 (4): 369–75.

Fishman, Rob. 2010. "State Department to Columbia University Students: Do Not Discuss WikiLeaks on Facebook, Twitter." *The Huffington Post*. Accessed December 4, http://www.huffingtonpost.com/2010/12/04/state-department-to-colum_n_792059.html.

Garrett, Bradley. 2014. "Place-Hacker Bradley Garrett: Research at the Edge of the Law." *Times Higher Education*. Accessed June 5, https://www.timeshighereducation.com/features/place-hacker-bradley-garrett-research-at-the-edge-of-the-law/2013717.article.

Gellman, Barton. 2015. "Scholarship, Security, and 'Spillage' on Campus." *The Century Foundation*. Accessed October 7, https://tcf.org/content/commentary/scholarship-security-and-spillage-on-campus/.

Greenberg, Andy. 2014. "Laura Poitras on the Crypto Tools That Made Her Snowden Film Possible." *Wired*. Accessed October 15, https://www.wired.com/2014/10/laura-poitras-crypto-tools-made-snowden-film-possible/.

Hall, Martin. 2015. "Universities Must Not Become Part of the Security Apparatus." *Times Higher Education*. Accessed January 8, https://www.timeshighereducation.com/comment/opinion/universities-must-not-become-part-of-the-security-apparatus/2017752.article.

Harvard Magazine. 2014. "Faculty Tensions I: The Sanctity of the Classroom." Accessed March 23, 2016, http://harvardmagazine.com/2014/11/harvard-professors-object-to-student-monitoring.

Hasan, Osman, Benjamin Habegger, Lionel Brunie, Nadia Bennani, and Ernesto Damiani. 2013. "A Discussion of Privacy Challenges in User Profiling with Big Data Techniques: The EEXCESS Use Case." Paper presented at the IEEE International Congress on Big Data (BigData Congress), Santa Clara, CA.

Hedgecoe, Adam. 2016. Reputational Risk, Academic Freedom and Research Ethics Review. *Sociology* 50 (3), 486–501.

Heisler, Martin O. 2007. "Academic Freedom and the Freedom of Academics: Toward a Transnational Civil Society Move." *International Studies Perspectives* 8 (4): 347–57.

International Studies Association. 2015. "Statement on the Use of Classified Materials in ISA Publications." Accessed March 23, 2016, http://www.isanet.org/Publications/Classified-Materials.

Jackson, Richard. 2015. "Confessions of a Terrorist Sympathiser." Accessed March 23, 2016, https://richardjacksonterrorismblog.wordpress.com/2015/11/27/confessions-of-a-terrorist-sympathiser/.

——. 2016. "I've Just Been Interviewed by the Police Because Someone in NZ Made a Formal Complaint That I Was a Terrorist Sympathiser. It Had to Happen." Accessed March 23, 2016, https://twitter.com/RJacksonterror/status/704808341243957249.

Jaeger, Paul T., John Carlo Bertot, Charles R. McClure, and Lesley A. Langa. 2006. "The Policy Implications of Internet Connectivity in Public Libraries." *Government Information Quarterly* 23 (1): 123–41.

Kashmir Media Service. 2014. "India Shuts Down Internet to Prevent Mirwaiz's Address." *Kashmir Media Service*. Accessed March 18, http://www.kmsnews.org/news/2014/03/18/india-shuts-down-internet-to-prevent-mirwaizs-address.html.

Kushner, David. 2016. "Fear This Man. To Spies, David Vincenzetti Is a Salesman. To Tyrants, He Is a Savior. How the Italian Mogul Built a Hacking Empire." *Foreign Policy*. Accessed April 26, http://foreignpolicy.com/2016/04/26/fear-this-man-cyber-warfare-hacking-team-david-vincenzetti/.

Lewman, Andrew. 2013. "Tor: Uses and Limitations of Online Anonymity." In *Advances in Cyber Security: Technology, Operation, and Experiences*, edited by Frank D. Hsu and

Dorothy Marinucci, 109–20. New York: Fordham University Press.

Liang, Bin, and Hong Lu. 2010. "Internet Development, Censorship, and Cyber Crimes in China." *Journal of Contemporary Criminal Justice* 26 (1): 103–20.

Lyon, David. 2013. "Afterword: Digital Spaces, Sociology and Surveillance." In *Digital Sociology. Critical Perspectives*, edited by Kate Orton-Johnson and Nick Prior, 95–102. London: Palgrave Macmillan.

——. 2014. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1 (2): 1–13.

Martin, Aaron K., Rosamunde E. Van Brakel, and Daniel J. Bernhard. 2009. "Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework." *Surveillance & Society* 6 (3): 213–32.

Marx, Gary T. 2007. "Rocky Bottoms: Techno-Fallacies of an Age of Information." *International Political Sociology* 1 (1): 83–110.

McKune, Sarah. 2015. *Encryption, Anonymity, and the "Right to Science."* New York: Just Security, University School of Law.

Michael, Gabriel J. 2015. "Who's Afraid of WikiLeaks? Missed Opportunities in Political Science Research." *Review of Policy Research* 32 (2): 175–99.

Mittelman, James H. 2007. "Who Governs Academic Freedom in International Studies?" *International Studies Perspectives* 8 (4): 358–68.

Moore, Daniel, and Thomas Rid. 2016. "Cryptopolitik and the Darknet." *Survival* 58 (1): 7–38.

Moran, Gordon, and Michael Mallory. 1991. "Some Ethical Considerations Regarding Scholarly Communication." *Library Trends* 40 (2): 338–56.

Muir, Adrienne, Rachel Spacey, Louise Cooke, and Claire Creaser. 2016. "Regulating Internet Access in UK Public Libraries: Legal Compliance and Ethical Dilemmas." *Journal of Information, Communication and Ethics* 14 (1): 87–104.

Mutlu, Can E. 2015. "Of Algorithms, Data and Ethics: A Response to Andrew Bennett." *Millennium—Journal of International Studies* 43 (3): 998–1002.

Newman, Melanie. 2008. "Lecturers Fear Anti-Terror Laws." *Times Higher Education*. Accessed October 2, https://www.timeshighereducation.com/news/lecturers-fear-anti-terror-laws/403791.article.

Nye, Valerie, and Kathy Barco. 2012. *True Stories of Censorship Battles in America's Libraries*. Chicago: American Library Association.

ONI (OpenNet Initiative.) 2016. OpenNet Initiative. Accessed June 13, 2016, https://opennet.net/.

Peace, A. Graham. 2003. "Balancing Free Speech and Censorship: Academia's Response to the Internet." *Communications of the ACM* 46 (11): 104–9.

PEN American Center. 2013. *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*. New York.

Penney, Jon. 2016. "Chilling Effects: Online Surveillance and Wikipedia Use." *Berkeley Technology Law Journal* 31 (1): 1–58.

Perlroth, Nicole, Jeff Larson, and Scott Shane. 2013. "NSA Able to Foil Basic Safeguards of Privacy on Web." *New York Times*. Accessed September 5, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html.

Rawlinson, Kevin. 2016. "Private Messages at Work Can Be Read by European Employers." *BBC News*. Accessed January 14, http://www.bbc.com/news/technology-35301148.

Reporters without Borders. 2014. *Enemies of the Internet 2014*. Paris.

Roth, Andrew, and David M. Herszenhorn. 2014. "Facebook Page Goes Dark, Angering Russia Dissidents." *New York Times*. Accessed December 22, http://www.nytimes.com/2014/12/23/world/europe/facebook-angers-russian-opposition-by-blocking-protest-page.html.

Sampson, Fraser. 2015. "'Whatever You Say…': The Case of the Boston College Tapes and How Confidentiality Agreements Cannot Put Relevant Data Beyond the Reach of Criminal Investigation." *Policing* (OnlineFirst): 1–10.

Setty, Sudha. 2015. "Surveillance, Secrecy, and the Search for Meaningful Accountability." *Stanford Journal of International Law* 51 (1): 69–104.

Smith, Mike Deri. 2013. "Porn Filters Block Sex Education Websites." *BBC News*. Accessed December 18, http://www.bbc.com/news/uk-25430582.

Stoycheff, Elizabeth. 2016. "Under Surveillance Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring." *Journalism & Mass Communication Quarterly* 93 (2): 296–311.

Topping, Alexandra. 2013. "David Miranda's Detention at Heathrow 'Extraordinary,' Says Keith Vaz." *The Guardian*. Accessed August 19, https://www.theguardian.com/uk-news/2013/aug/19/detention-david-miranda-keith-vaz-glenn-greenwald.

Townend, Judith. 2014. "Online Chilling Effects in England and Wales." *Internet Policy Review* 3 (2): 1–12.

UNHRC (United Nations Human Rights Council). 2016. Resolution A/HRC/29/32. "The Promotion and Enjoyment of Human Rights on the Internet." Accessed June 27, 2016, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement.

UN ICCPR (United Nations International Covenant on Civil and Political Rights). 1976. Resolution 2200A (XXI), "Article 19." Accessed March 23, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

Wagner, Ben. 2014. "The Politics of Internet Filtering: The United Kingdom and Germany in a Comparative Perspective." *Politics* 34 (1): 58–71.

Warrell, Helen. 2015. "Students Under Surveillance." *Financial Times*. Accessed July 24, http://www.ft.com/cms/s/2/634624c6-312b-11e5-91ac-a5e17d9b4cff.html#slide0.

Wei, Michael, Laura M. Grupp, Frederick E. Spada, and Steven Swanson. 2011. "Reliably Erasing Data from Flash-Based Solid State Drives." Paper presented at the 9th USENIX Conference on File and Storage Technologies (FAST). San Jose, CA.

White, Scott G. 2008. "Academia, Surveillance, and the FBI: A Short History." *Surveillance and Governance: Crime Control and Beyond* 10: 151–74.

Wilson, John K. 2005. "Academic Freedom in America After 9/11." *Thought & Action: The NEA Higher Education Journal* 21 (Fall): 119–31.

Wolinsky, David, Kyungyong Lee, Patrick Boykin, and Renato Figueiredo. 2010. "On the Design of Autonomic, Decentralized VPNs." Paper presented at the 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom). Chicago, IL.

Zevenbergen, Ben. 2016. "Networked Systems Ethics." Accessed June 30, 2016, http://networkedsystemsethics.net/index.php?title=Main_Page.