# CENSORSHIP AND SURVEILLANCE IN THE DIGITAL AGE: THE TECHNOLOGICAL CHALLENGES FOR ACADEMICS

*Leonie Maria Tanczer, Ryan McConville, & Peter Maynard*

## INTRODUCTION

Technologically supported censorship and surveillance practices have become prominent topics both in research and the media. Influenced and fuelled by revelations such as the ‘Snowden leaks’ (Bauman et al. 2014) or censorship methods used during the Arab Spring (Deibert and Crete-Nishihata 2012, 344), the general public has been lucidly made aware of how digital tools and information are prone to tracing, interception, and suppression. Processes of eavesdropping and the collection of information (i.e., surveillance) are thereby often interrelated with processes of removal, displacement, and restriction of material or speech (i.e., censorship). Both are entangled with dynamics of secrecy, allowing censorship and surveillance techniques being open to abuses (Setty 2015). They are frequently implemented on the grounds of security discourses and practices (Bigo 2008) or enforced in light of standards applied by suppressive powers (Deibert 2003, 513).

In scholarly professions specifically, digital censorship and surveillance may constitute a threat to academic freedom. This is not least because of the increasing reliance on the Internet and information and communication technologies (ICT) to communicate, collect data, or distribute findings. Digital tools and data allow for the easier confiscation or destruction of research (Cyranoski 2008, 871; Gellman 2015), the manipulation of information, or the control and prevention of access to it (Fishman 2010). In particular, technologically supported censorship and surveillance impinge upon the higher education sector’s ability to conduct unobstructed inquiry. It puts users under general suspicion, creates a securitised climate, and leads to chilling effects. The field of security studies which frequently scrutinises these practices is certainly not immune to these measures.

This contribution aims to systematically explore the methods which can be used for 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 must engage with debates on technological information control. The second section outlines *how* censorship is technically implementable and *how* these techniques can affect the academic profession. The final section examines *what to do* against technologically supported censorship and surveillance and explores cryptographic circumvention methods. On these grounds, the paper strives to stimulate a discussion about the inclusion of cryptographic tools within academic teaching and scholarship. It endeavours to foster a debate about the legal and technical protection of researchers and hopes to introduce a culture of critical reflection about digital security.

## THE WHY

One of the most profound reasons *why* academics are exhorted to participate in debates on technological information control can be found in arguments surrounding human rights. The right to privacy and unfettered correspondence as well as the right to freedom of opinion and expression constitute fundamental pillars upon which reasons against censorship and surveillance rest. They have been outlined in international documents and treaties, with the United Nations Human Rights Council recently adopting a resolution that declared the unequivocal application of human rights onto the online sphere (A/HRC/32/L.20). Article 19 of the International Covenant on Civil and Political Rights (1976) in particular highlights the ability to seek, receive, and impart information through any media, regardless of frontiers. This Article is essential for the scholarly profession and touches upon the fundamental idea of unrestricted academic inquiry.

A further argument favouring the unimpaired ability to access information therefore originates from core principles of academic freedom. Academic freedom allows for independent teaching, research, and scholarly expression, crucial in advancing expertise, critical thinking, and general human knowledge (Altbach 2001, 205). Its importance has been discussed in myriads of publications and various special issues (*Thought & Action,* 2005; *International Studies Review*, 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 from the securitised post-9/11 climate with its over-emphasis on secrecy and "preemptive security practices" (Falk 2007; De Goede 2014, 101).

Scholars dealing with sensitive issues and information/data in the 'digital age' are affected in several ways. Most obviously, they need to be aware that information 'freely' accessible online is often filtered and, thus, censored. This raises the question where to find and how to gain access to digitised information that is kept secret from the public. In turn, researchers must think carefully about how to protect digitised data from third party access. They need to be aware that doing research involving ICT on politically sensitive topics can lead to being caught in a net of surveillance and information control.

Restrictions interfering with the higher education sector have, in the course of the last decade, been primarily implemented through regulatory means. For instance, both the United States (US) Patriot Act and the United Kingdom (UK) Counter-Terrorism and Security Act 2015 have been shown to impede on academic staff as well as students (Wilson 2005; Newman 2008, Hall 2015). In addition, less obvious manifestations of censorship are connected to the changing nature of academic funding (Hedgecoe 2015), the restriction to official documents (Barry and Bannister 2014), and 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 O'Loughlin in this forum). Although the ISA issued a statement (2015) rejecting these practices, the allegation adds to the importance for security studies to engage with problems surrounding information control.

Whilst international studies (IS) scholars such as Heisler (2007, 351) acknowledge such 'conventional' threats to academic freedom, a lot of publications still fail to interlink the phenomenon with the growing process of digitalisation. 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, but also reliant upon, the Internet and associated ICTs. Technologically supported censorship and surveillance practices subsequently challenge the academic profession. These techniques and their secrecy oblige researchers to reconsider the possible role they may have on their work as well as on their research subjects.

Most notably, digitalisation of data and information not only allows easier content duplication and distribution, but also easier restriction and access to it. This can occur in an unwanted manner, and with the interference potentially being caused by 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. The higher education sector and, in particular, 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 ideas of an alleged technological neutrality make academics inattentive to ICTs potential negative side-effects.

In particular, ‘traditional’ research processes involving the collection, analysis, storage, presentation, and reuse of data need to be re-assessed. While digital data and online communication are essential for the daily practice of research, they can also put participants and their kin in danger. Information – and especially digital information – needs to be responsibly collected, managed, and stored. Some fields are progressing towards increasing 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 being 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 and subjects investigated, at times, keeping the balance between openness and transparency on the one hand and the rights to privacy and security on the other, poses 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 an entire research team.

The need to produce evidence of data while retaining the responsibility to protect sources is further complicated through the move towards digital technologies. While technological developments have made the protection of data technically possible, they have also created legal problems which remain unaddressed. This has been seen in the case of former UK PhD student Bradley Garrett whose research data was confiscated and used in court against his subjects (Garrett 2014). Garrett’s work focused on the topic of ‘place hacking’ and involved the observation of groups that visited off-limits 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 himself and his participants, Garrett (2014) emphasised that the academic community had to stand up against such actions by the authorities and needed to consider data collection and protection procedures more carefully.

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 curricula still seem oblivious to these questions. While there are plenty of publications on ethics and methods in the digital age (Ackland 2013; Mutlu 2015) as well as ethics and methods trainings and assessments, the digital security and protection of IS researchers and subjects is barely addressed. In this regard security studies have failed to properly understand the implications of digitalisation for their own research practice. A fundamental discussion about digital information control and the implementation of potential resistance techniques is therefore overdue. What is needed, on the part of the researcher, is good understanding of, first, how online surveillance and digital censorship works and, second, how to circumvent and protect one's work 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 are required to engage with digital information control, this paper will now examine *how* censorship is technically implementable and *how* these techniques can obstruct the academic profession. Eriksson and Giacomello (2009, 206) have already accentuated the importance of Internet controls for IS scholars. They acknowledge that the study of digital information control fosters the scholarship on global governance and emphasise how such measures vary across time, space, and issue-areas. Similarly, manifestations of technologically supported censorship and surveillance practices differ. They range from severely intrusive and restrictive to more subtle and unapparent forms. In this regard, academics may never experience clear infringements of or interferences with their work. Nevertheless, even if such techniques are ‘invisible’ and/or based solely on the collection of electronic information, they can potentially become problematic 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 the process of borrowing a book from a library where a librarian initially reads and assesses the content for suitability before the publication is either passed on to the recipient or destroyed. While techniques vary, content restrictions are common practices across states and frequently supported by the private and commercial sectors, as well as non-profit 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 such as those in North Korea or Saudi Arabia. Such control is also practiced in liberal states which nonetheless engage in illiberal practices (Reporters Without Borders 2014, 3).

Within the UK, for instance, web access is by default filtered by ISPs. Although users have the ability to opt out from content blocking, there have been numerous reports of ‘legitimate’ websites being censored. The restrictions included content referring to sexual education, domestic abuse (Smith 2013) as well as websites of politicians (Burrell 2013). More examples of governmental content blocking can be found in countries such as India or Russia (Kashmir Media Service 2014; Roth and Herszenhorn 2014). These and numerous other country-specific profiles have been documented by projects such as the *OpenNet Initiative* (Deibert et al. 2008; 2010; 2011; ONI 2016). 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 globally 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 (Muir et al. 2016) indicates that filtering software is ubiquitous in libraries. In the analysis, it was discovered that two-thirds of the surveyed UK libraries had received complaints about overblocking, including the inability to access virtual learning environments and the difficulty of rapidly unblocking content as a result of the filtering software. These findings echo those of previous studies, illustrating 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 and interference methods, mass data collection and data analytics by institutional, commercial and governmental actors should be of concern to the academic community. A particular sub-field of data analytics is user profiling. This involves computer algorithms which discover patterns from personal data and proceed to identify correlations between these patterns and (groups of) individuals (Hasan et al. 2013). By doing so, the algorithms can automatically construct profiles of people based on the data available. These technologies, which include and/or exclude particular groups due to their anticipated behaviour, foster "practices of exceptionalism" (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' behaviour and performance (Warrell 2015; Harvard Magazine 2014). However, variations of these technologies may also put academics under closer watch. Specifically, security scholars who frequently investigate sensitive and controversial topics such as ‘terrorism’ or ‘torture’ can be earmarked for closer scrutiny. In fact, only recently Professor Richard Jackson, Editor-In-Chief of the journal *Critical Terrorism Studies* posted on Twitter that he was questioned by the New Zealand police (Jackson 2016). He thereafter speculated whether his research and in particular one of his blog posts in which he proposed to be a ‘terrorist sympathiser’ led to this (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, for example, every website visited, web search performed, and message sent may be collected, stored, and analysed restricts online behaviour. 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). Two recent studies on the effects of the Snowden revelations show how perceptions of surveillance contributed to an online spiral of silence (Stoycheff 2016) and led to a significant drop in the amount of web traffic to ‘privacy sensitive’ Wikipedia articles (Penney 2016). Both immediate and long-term effects were thereby detected, offering compelling evidence for the chilling effect associated with online surveillance. The impact of online self-censorship has also been ascertained by the PEN American Center (2013). They identified that 1 in 6 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.

Yet, technologically supported censorship is not only limited to the communication and dissemination of information and knowledge. It may also take the form of confiscation of equipment and general problems around the storage and transport of digital material. A number of states permit the searching of laptops when entering the country, including the US, Canada, and the UK (Burrell 2015). There have been various cases of reporters and academics having their laptops/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, many of the used instruments had been tampered with. Digital data in particular is prone to such interceptions. Techniques exist and continue to be researched that allow for the deletion of data beyond recovery (Wei et al. 2011).

Most importantly, though, the censorship and surveillance practices outlined above are amplified through the active endeavour to break and sabotage cryptographic techniques. The subversion ranges from influencing technical standard bodies to exploiting software and hardware vulnerabilities (Perlroth et al. 2013). In particular, intelligence agencies have an interest in breaking encryption, essential for ensuring secure communication and/or data storage (Ball et al. 2013). In addition, there is ongoing research into the ability to de-anonymise web users, sometimes even with help of academic institutions (Cox 2016). In contrast, a report by the United Nation's Special Rapporteur on freedom of expression (A/HRC/29/32) provided strong support for the defence of anonymity and encryption. Similarly McKune (2015) calls the attempt to disrupt these tools a violation of the “right to science”. She argues that encryption is an implementation of mathematics and therefore a scientific development with the ability to facilitate free expression and privacy. Yet, in the current securitised 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, leading to the prohibition of knowledge production and limiting the comprehensive understanding of society overall.

## THE WHAT (TO DO)

The final part of this paper delineates methods for circumventing some of the mentioned technological information controls. One of the few articles specifically addressing this issue in the scholarly profession has been published in the *Research Ethics Review.* Aldridge, Medina, and Ralphs (2010) provide fourteen guidelines for the security of 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, the current publication hopes to provide a starting point for the accentuation of the importance of cryptographic tools in the IS profession. It broadens the focus on data security to the examination and circumvention of technologically supported censorship and surveillance practices and aims to galvanise the security studies profession.

Akin to Zevenbergen's (2016) guidelines that inform research's ethical assessment and encourages stakeholders to minimise risks before the data collection takes place, the current paper hopes to stimulate reflexivity. It introduces a culture of security sensitivity and awareness of technological pitfalls. The article acknowledges that not all researchers are equally affected by the discussed censorship techniques and that not all of the here-outlined tools will always be needed. They may affect researchers working in diverse socio-political and socio-technical contexts in different ways. However, they should be applied under particular circumstances. They may be recommended when working on certain topics or with particular participants; they may be helpful when on fieldwork, in specific countries or conflict zones; indeed, they may be valuable when handling any form of sensitive data that may compromise the privacy, integrity and/or life of participants and researchers. Ultimately, the upcoming section encourages IS scholars to fundamentally scrutinise their use of the Internet and ICTs and take up methods that would be auxiliary in their research.

The hereafter 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. It is advised that academics are 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 emphasise, 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 are putting the burden on scholars to secure themselves. They are not challenging practices of censorship and surveillance as such. The instruments require some foundation of 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 technologists.

Two essential principles when bypassing censoring filters and monitoring systems are (a) the routing of connections over less restrictive network paths and (b) the modification of data prior to transit in order to prevent eavesdropping and the identification of activities.

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

However, this is not to say that full anonymity is guaranteed. Connections, despite being modified or directed through another path can have their true purpose inferred and – as highlighted earlier – an adversary with a large budget or substantial skills could break anonymity measures (Dahal et al. 2015). The methods can, thus, only improve the odds of not being tracked.

One way of anonymising online traffic is through tools such as *The Onion Router* (Tor). The Tor project provides a collection of software which can be used in various ways for anonymity. The easiest approach is to employ the Tor browser bundle, which is similar to any other web browser, but encrypts and routes traffic through intermediary machines before reaching its intended destination. Using different nodes which the traffic is routed through, Tor chooses paths rather than sending traffic directly to the intended destination. To put it more simply: The traffic basically 'jumps' through the network before entering the final exit node, reducing the chance of someone successfully monitoring or censoring the connection. Despite Tor's potential misuse for pernicious reasons and its ability to be identified and blocked, the browser increases the anonymity of users (Moore and Rid 2016). It is, hence, a common instrument used by law enforcement, journalists and activists (Lewman 2013). Similarly, in the worst cases, Tor provides options for academics in suppressive places to obtain uncensored information. However, it could also be implemented in the daily research practice of any regular scholar when investigating sensitive or restricted research topics.

Another way of overcoming censoring or monitoring network controls is by using a *Virtual Private Network* (VPN). A VPN is a technology typically used 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). Besides, VPNs are frequently utilised 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 to 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 to a machine that is, for example, outside of a conflict zone or if there is a requirement to bypass the ISP or even internal university or library 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 secure storage and transmission of data. The encryption of data is a way to elude censorship or surveillance, ensuring data integrity and preventing intellectual property from falling into the wrong hands. As universities are increasingly becoming a hub for the generation of new knowledge and innovation, the possible theft of intellectual property is a fundamental concern for academia. The prospect of, for instance, economic espionage may convince those sceptical of purely ethical arguments to apply encryption techniques within the remits of higher education. The encryption of data on computers, cloud services and also removable media – 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, academia can profit from the usage of encrypted communication methods. A recent ruling by the European Court of Human Rights (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 vulnerable research subjects through online means. Moreover, it mirrors revelations such as the monitoring of Harvard University's deans' email accounts (Carmichael 2013). In this particular incidence, academics' communication was secretly searched by the university administrators in quest of potential media leaks. These cases reveal that secure and unmonitored communication is not fully guaranteed. Nonetheless, GPG can be availed of to 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 et al. 2007). Furthermore, encrypted instant messaging services such as *Signal*, as well as multiplatform voice and video conferencing applications such as *Jitsi* are also beneficial when organising or conducting interviews with vulnerable research subjects.

There are, of course, far more tools available that academics can implement 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 of the device. By default Tails leaves no trace on the actual computer/laptop. It is, thus, a convenient application for researchers when travelling, allowing not only for 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). Yet, based on all the discussed technologically supported censorship and surveillance methods, they would certainly also be valuable for the academic and in particular the security scholar profession.

## CONCLUSION

This contribution examined the ‘*why'*, ‘*how'* and the ‘*what to do*’ in relation to technologically supported censorship and surveillance practices. Its basic message is for academics to pay more attention to these aspects, due to the profound effects that the ‘digital revolution’ has on the right to privacy, the ability to seek, receive, and impart information as well as the core principles of academic freedom. To this end, the article explored the methods which are used to control the digital sphere as well as ways to circumvent them. While the paper acknowledges that research must be public and transparent, this requirement does not remove the right to privacy and protection both for academics as well as any participants involved. This is particularly important for security scholars, given the sensitive nature of the issues, approaches, and research subjects studied. Digital censorship can impact on the accuracy of research findings, highlighting why scholars need to think more carefully about the consequences of digitalisation for the field.

Although the paper accepts the inability to address the manifold realities of researchers, it informs and also tries to tackle the suspicion of some of the here-outlined circumvention techniques. A few of the measures may seem novel and radical. Yet, in the view of the ongoing (in)securitisation processes (Bigo 2008; Bigo and Tsoukala 2008), security scholars are exhorted to study and know about the (in)securities that not only the world, but also the discipline, is facing. With this in mind, the article hopes to stimulate discussion about the consequences of digitalisation for the field. The paper encourages the inclusion of cryptographic tools within the academic profession. These can equip researchers with a suitable toolkit for bypassing technologically supported censorship and surveillance practices and are helping to improve the anonymity and confidentiality of research processes. The article also prompts security scholars to be mindful of the use of digital technologies and seek both legal and technical assistance for overcoming restrictions and implementing protection methods.

Aside from outlining these proposed technical circumvention methods, the article also hopes to introduce a culture of critical reflection about digital practices. This reflection requires closer examination of the complicated links between secrecy, surveillance and censorship, and the balance between openness and transparency as well as the rights to security and privacy in the digital age. Besides, the questioning of censorship and surveillance techniques demands the instillation of security sensitivity and awareness. Security speaks to behaviour far more than it does to technology. One must acknowledge the behavioural limitation of technological security posed by human error or convenience (Scott-Railton 2016). Thus, challenging online censorship and surveillance is 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 behavioural limitations is far more profound and needs to go hand-in-hand with the here-proposed technological measures.

Lastly, the article wants 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 on the daily practice of academics, the training of students and staff, and the composition of ethics committees. The latter would profit from ethical, legal and technical advice. Institutional review boards need to develop an understanding of these issues so that they can sufficiently evaluate the security protocols academics propose.

It is also important to emphasise that none of the here-outlined techniques, nor any of the named products, can be 'recommended' as such. A crucial message to 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. We point to discussions taking place in fields such as digital sociology and surveillance studies (Martin et al. 2009; Lyon 2013; 2014) and direct academics to the work of non-profit digital rights groups such as the *Electronic Frontier Foundation* as well as the worldwide *Cryptoparty* movement.

In conclusion, this publication hopes to have provided both answers but ultimately also raised questions for the higher education sector. The use of the Internet and the reliance on ICTs is both a gain but also a crux. The measures outlined above are not a *panacea*. They are probably more of a temporary relief than a remedy and do not address the root causes of technologically supported censorship and surveillance. It is therefore critical that academics across all disciplines raise the question of 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.

## REFERENCES

Academics Anonymous. May 13, 2016. “Universities Must Do More to Protect PhD Students Working in Dangerous Countries.” *The Guardian*.

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

Altbach, Philip G. 2001. “Academic Freedom: International Realities and Challenges.” *Higher Education* 41(1): 205-219.

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. September 6, 2013. “Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security.” *The Guardian*.

Barry, Emily and Frank Bannister. 2014. “Barriers to Open Data Release: A View From The Top.” *Information Polity* 19(1, 2): 129-152.

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): 121-144.

Bian, Jiang, Remzi Seker and Umit Topaloglu. 2007. “Off-The-Record Instant Messaging For Group Conversation.” Presented at the IEEE International Conference on Information Reuse and Integration (IRI). Las Vegas.

Bigo, Didier. 2008. “Globalized (In)Security: The Field and the Ban-Opticon.” In *Terror, Insecurity and Liberty: Illegal Practices of Liberal Regimes after 9/11*, edited by Didier Bigo and Anastassia Tsoukala, 10-48. London: Routledge.

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

Bigo, Didier and Anastassia Tsoukala. 2008. “Understanding (In)Security,” In *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes After 9/11*, edited by Didier Bigo and Anastassia Tsoukala, 1-9. London: Routledge.

Burrell, Ian. December 23, 2013. “O2 Changes Porn Filter after Charity Sites Blocked.” *The Independent*.

Burrell, Ian. October 28, 2015. “Police use Terror Powers to Seize BBC Newsnight Journalist's Laptop.” *The Independent*.

Carmichael, Mary. March 9, 2013. “Harvard University Administrators Secretly Searched Deans’ Email Accounts, Hunting for Media Leak.” *Boston Globe*.

Cheredar, Tom. March 10, 2014. “NSA Views Encryption As Evidence of Suspicion and Will Target Those Who Use It, Security Journalist Says.” *VentureBeat*.

Cox, Joseph. February 24, 2016. “Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds.” *Motherboard*.

Cyranoski, David. 2008.” Check Your GPS at the Border.” *Nature* 451: 871.

Dahal, Saurav, Junghee Lee, Jungmin Kang and Seokjoo Shin. 2015. “Analysis On End-To-End Node Selection Probability in Tor Network.” Presented at the International Conference on Information Networking (ICOIN). Angkor.

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

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):100-118.

Deibert, Ronald J. (2003) Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. *Millennium-Journal of International Studies.* 32(3):501-530.

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

Deibert, Ronald J., John Palfrey, Rafal Rohozinski and Jonathan Zittrain. 2011. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Cambridge: MIT Press.

Deibert, Ronald J., John Palfrey, Rafal Rohozinski and Jonathan Zittrain. (2010) *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge: MIT Press.

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

Deibert, Ronald J. and Masashi Crete-Nishihata. (2012). “Global Governance and the Spread of Cyberspace Ccontrols.” *Global Governance.* 18(3): 339-361.

Deibert, Ronald J. 2002. “Dark Guests and Great Firewalls: The Internet and Chinese Security Policy.” *Journal of Social Issues* 58(1): 143-159.

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

Eriksson, Johan and Giampiero Giacomello. 2009. “Who Controls What, and Under What Conditions?” *International Studies Review* 11(1): 206-210.

Falk, Richard. 2007. “Academic Freedom Under Seige.” *International Studies Perspectives* 8(4): 369-375.

Fishman, Rob. December 4, 2010. “State Department To Columbia University Students: DO NOT Discuss WikiLeaks On Facebook, Twitter.” *The Huffington Post*.

Garrett, Bradley. June 5, 2014. “Place-Hacker Bradley Garrett: Research at the Edge of the Law.” *Times Higher Education*.

Gellman, Barton. October 7, 2015. “Scholarship, Security, and ‘Spillage’ on Campus.” *The Century Foundation*.

Greenberg, Andy. October 15, 2014. “Laura Poitras on the Crypto Tools That Made Her Snowden Film Possible.” *Wired*.

Hall, Martin. January 8, 2015. "Universities must Not Become Part of the Security Apparatus." *Times Higher Education*.

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

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.” Presented at the IEEE International Congress on Big Data (BigData Congress). Santa Clara.

Hedgecoe, Adam. 2015. “Reputational Risk, Academic Freedom and Research Ethics Review.” *Sociology* (OnlineFirst): 1-6.

Heisler, Martin O. 2007. “Academic Freedom and the Freedom of Academics: Toward A Transnational Civil Society Move.” *International Studies Perspectives* 8(4): 347-357.

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

J. Scott-Railton. 2016. "Security for the High-Risk User: Separate and Unequal." *IEEE Security & Privacy* 14(2): 79-87.

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

Jackson, Richard. 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. <https://twitter.com/RJacksonterror/status/704808341243957249> (2016, March 23).

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): 123-141.

Kashmir Media Service. March 18, 2014. "India Shuts Down Internet to Prevent Mirwaiz's Address." *Kashmir Media Service*.

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, 109-120. 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): 103-120.

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.

Lyon, David. 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): 213-232.

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): 175-199.

Mittelman, James H. 2007. “Who Governs Academic Freedom in International Studies?” *International Studies Perspectives* 8(4): 358-368.

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):338-356.

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. October 2, 2008. “Lecturers Fear Anti-Terror Laws.” *Times Higher Education*.

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

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

Peace, A. Graham. 2003. "Balancing Free Speech and Censorship: Academia's Response to the Internet." *Communications of the ACM* 46(11): 104-109.

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

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. September 5, 2013. "NSA Able to Foil Basic Safeguards of Privacy on Web." *The New York Times*.

Rawlinson, Kevin. January 14, 2016. "Private Messages at Work can be Read by European Employers." *BBC News*.

Reporters Without Borders. 2014. *Enemies of the Internet 2014*. Paris: Reporters Without Borders.

Roth, Andrew and David M. Herszenhorn. December 22, 2014. "Facebook Page Goes Dark, Angering Russia Dissidents." *The New York Times*.

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. December 18, 2013. "Porn Filters Block Sex Education Websites." *BBC News*.

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. August 19, 2013. “David Miranda's Detention at Heathrow ‘Extraordinary’, says Keith Vaz.” *The Guardian*.

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

Wagner, Ben. 2014. “The Politics of Internet Filtering: The United Kingdom and Germany in A Comparative Perspective.” *Politics* 34(1):58-71.

Warrell, Helen. July 24, 2015. “Students Under Surveillance.” *Financial Times*.

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

White, Scott G. 2008. “Academia, Surveillance, and the FBI: A Short History.” *Surveillance and Governance: Crime Control and Beyond* 10:151-174.

Wilson, John K. 2005. “Academic Freedom in America After 9/11.” *Thought & Action: The NEA Higher Education Journal* Fall:119-131.

Wolinsky, David, Kyungyong Lee, Oscar Boykin, and Renato Figueiredo. 2010. “On the Design of Autonomic, Decentralized VPNs.” Presented at the 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom). Chicago.

Zevenbergen, Ben. 2016. Networked Systems Ethics. <http://networkedsystemsethics.net/index.php?title=Main_Page> (2016, June 30).

## ACKNOWLEDGEMENTS

The authors are indebted to Amalia Campos Delgado, Jana Eyssel, Kyle Shuttleworth, Josh Milburn, Anne Schroeter, 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 editors for their insightful comments.