



**HAL**  
open science

## Online Surveillance, Censorship, and Encryption in Academia

Leonie Maria Tanczer, Ronald Deibert, Didier Bigo, Marianne Franklin, Lucas Melgaço, David Lyon, Becky Kazansky, Stefania Milan

► **To cite this version:**

Leonie Maria Tanczer, Ronald Deibert, Didier Bigo, Marianne Franklin, Lucas Melgaço, et al.. Online Surveillance, Censorship, and Encryption in Academia. *International Studies Perspectives*, 2019, 21, 35 p. 10.1093/isp/ekz016 . hal-03393680

**HAL Id: hal-03393680**

**<https://sciencespo.hal.science/hal-03393680>**

Submitted on 16 Feb 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

# Online Surveillance, Censorship, and Encryption in Academia

LEONIE MARIA TANCZER   
*University College London*


RONALD J. DEIBERT  
*University of Toronto*

DIDIER BIGO  
*King's College London, Sciences Po Paris*

M.I. FRANKLIN  
*Goldsmiths University of London*

LUCAS MELGAÇO  
*Vrije Universiteit Brussel*

DAVID LYON  
*Queen's University*

AND  
BECKY KAZANSKY  AND STEFANIA MILAN  
*University of Amsterdam*

**Abstract:** The Internet and digital technologies have become indispensable in academia. A world without email, search engines, and online databases is practically unthinkable. Yet, in this time of digital dependence, the academy barely demonstrates an appetite to reflect upon the new challenges that digital technologies have brought to the scholarly profession. This forum's inspiration was a roundtable discussion at the 2017 International Studies Association Annual Convention, where many of the forum authors agreed on the need for critical debate about the effects of online surveillance and censorship techniques on scholarship. This forum contains five critiques regarding our digitized infrastructures, datafied institutions, mercenary corporations, exploitative academic platforms, and insecure online practices. Together, this unique collection of articles contributes to the research on academic freedom and helps to frame the analysis of the neoliberal higher education sector, the surveillance practices that students and staff encounter, and the growing necessity to improve our "digital hygiene."

**Resumen:** Internet y las tecnologías digitales se han tornado indispensables en el ámbito académico. Resulta prácticamente imposible pensar en un mundo sin correo electrónico, motores de búsqueda y bases de datos en línea. Así y todo, en esta era de dependencia digital, los académicos apenas demuestran un deseo de reflexionar sobre los nuevos retos que las tecnologías digitales han traído consigo a las profesiones especializadas. La inspiración de este foro fue una discusión planteada en una mesa redonda en el marco de la Convención Anual de 2017 de la Asociación de Estudios Internacionales, donde muchos de los autores del foro coincidieron en la necesidad de un debate crítico acerca de los efectos de las técnicas de vigilancia y censura en línea que enfrentan los

académicos. Este foro contiene cinco reseñas relacionadas con nuestras infraestructuras digitalizadas, instituciones datificadas, corporaciones mercenarias, plataformas académicas explotadoras y prácticas en línea inseguras. En su conjunto, esta colección única de artículos contribuye a la investigación sobre la libertad académica y ayuda a enmarcar el análisis del sector neoliberal de la enseñanza superior, las prácticas de vigilancia con las que se encuentran los estudiantes y el personal, y la necesidad cada vez mayor de mejorar nuestra «higiene digital».

**Extrait:** Internet et les technologies digitales sont devenus indispensables dans le milieu universitaire. Un monde sans e-mails, moteurs de recherche et bases de données en ligne est pratiquement impensable. Cependant, dans cette ère de dépendance digitale, le milieu universitaire ne semble pas préoccupé par les nombreux défis que posent les technologies digitales dans les professions universitaires. Cette tribune a été inspirée par le débat d'une table ronde lors de la Convention annuelle de l'Association d'études internationales de 2017, où un grand nombre d'auteurs dans l'assemblée ont convenu de la nécessité de lancer un débat critique sur les effets de la surveillance et des méthodes de censure en ligne sur le savoir universitaire. Cette tribune formule cinq critiques à l'encontre de nos infrastructures numérisées, des institutions pilotées par les données, des entreprises mercenaires, des plateformes universitaires abusives et des pratiques en ligne non sécurisées. L'ensemble des articles de cette collection unique contribue à la recherche sur la liberté universitaire et aide à encadrer l'analyse du secteur néolibéral de l'enseignement supérieur, les pratiques de surveillance rencontrées par les étudiants et le personnel et la nécessité grandissante d'améliorer notre «hygiène digitale».

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

### Articles in This Forum

Introduction

Leonie Maria Tanczer

Rescuing the Internet for Academic Freedom

Ronald J. Deibert

Digital Communication, Surveillance and Academic Freedom in The Transnational Universes of Competing Homo Academicus(es) Institutions

Didier Bigo

University Life Corporatizing the Digital: Academic Agency Interrupted?

M.I. Franklin

Surveillance and The Quantified Scholar: A Critique of Digital Academic Platforms

Lucas Melgaço and David Lyon

Infrastructure and Protocols for Privacy-Aware Research

Becky Kazansky and Stefania Milan

# Introduction

LEONIE MARIA TANCZER

*University College London*

This forum on online surveillance, censorship, and encryption is more than overdue. The Internet and the use of digital technologies have become indispensable in academia. A world without email, search engines, and online databases is practically unthinkable, and scholars and students are equally reliant on the ability to collect, store, and distribute data as well as post, tweet, and upload their work. Yet, in this time of digital dependence, the academy barely demonstrates an interest in reflecting upon the new challenges that information and communication technologies have brought to the scholarly profession. While some of us may study the misuse of technological capabilities by state and nonstate actors, critique border technologies, or examine global surveillance structures, we have been rather silent about the potential detriments that the Internet and data's inadvertent use have brought to our field, our students, and our participants.

This discussion goes also hand in hand with the threat to academic freedom that the higher education sector, and international relations in particular, are experiencing. Academic freedom implies that both faculty members and students can engage in intellectual debates without fear of censorship or retaliation. It means that the political, religious, or philosophical beliefs of politicians, administrators, and members of the public cannot be imposed on students or staff (Mills 2002; Falk 2007). However, an eerie and uncomfortable feeling arises when observing the creeping interference and rising managerial oversight at universities across the globe. While threats to academics are certainly not new (Mittelman 2007) and well-known social scientists have been subject to surveillance already in the past (White 2008), the scale and extent of risks that scholars presently face has significantly risen.

Indeed, the examples of such dangers are stockpiling. In the United Kingdom, the “prevent” duty as part of the Counter Terrorism and Security Act 2015 led to chilling effects on campuses (Bentley 2018; Cram and Fenwick 2018; Spiller, Awan, and Whiting 2018) and fostered a climate of fear especially among Muslim students and staff (Gilmore 2017). In autumn 2018, an essay by the political theorist Norman Geras was deemed “security-sensitive” because his argument that people may legitimately revolt against tyranny and grave social injustice was seen as potentially drawing students into terrorism (Courea 2018). Similarly, in Australia, the expanding counterterrorism reach led to a Sri Lankan student being falsely arrested on terror charges (Fattah 2018). The new “national interest test” gives ministers the right to block funding applications standing in alleged opposition to Australia's security, strategic interests, and foreign policy (Koziol 2018).

In addition to these measures built upon suspicions held against minorities, US academics report increased online harassment by right-wing white supremacist groups (Ciccariello-Maher 2017). Scholars further fear the adverse consequences—especially for women—arising from the recording of lectures and conferences (Galpin 2018). These developments are happening along with the drive for “smart” campuses and classrooms that permit the monitoring of both students and staff (Muhamad et al. 2017; Edwards, Martin, and Henderson 2018; Hope 2018) and are promoted on the premise of “student protection” or the “personalization” of learning experiences (Herold 2018).

Looking to other parts of the world, cases such as the death of the Italian PhD student Giulio Regeni in Egypt (Peter and Strazzari 2017), the imprisonment of the UK PhD student Matthew Hedges in the United Arab Emirates (BBC News 2018b), and the dismissal of more than 6,000 Turkish academics cause great concern (Anonymous 2017; Namer and Razum 2018). In fact, I could go on: there are

the ominous implications of the Protection of State Information Bill on researchers in South Africa (Duncan 2018); the censure of academics by the General Intelligence and Security Service in the Netherlands (Van Der Sloot 2017); the expansion of the Chinese censorship and surveillance apparatus into academic partnerships, professorships, and publishers (Brady 2017; Else 2017; Dukalskis 2018); the forced relocation of the Central European University (CEU) from Budapest to Vienna (Enyedi 2018); or the recent confiscation of higher education teaching materials by the military police in Brazil (Guardian 2018). Nonetheless, I would not be done and the examples continue.

### **This Relates to All of US**

The examples of threats to academic freedom stretch from the Global North to the Global South, and in recent years they have steadily become the norm. What many of these instances have in common is not only the perceived hazard that critical research, students, and scholars pose to the status quo, but the fundamental need by state authorities to control and to manage. For states, administrators, and industry actors the surveillance of the higher education sector has become so much easier with the rise of technological capabilities. One does not need to worry that criticism, subversion, and unionism are left unnoticed and potentially even go unpunished.

Digital communication systems, online learning and storage platforms, and, most recently, the pervasiveness of Internet-connected devices simplify the monitoring of our activities and viewpoints. Additionally, what we share, read, and reference in our research and what we say, critique, and do in our teaching are all subject to scrutiny. Just as academics have become in essence replaceable numbers—whether our staff identifier, our ORCID iD, or our h-index—our metrics are there to be compared and contrasted, to steadily justify the higher education sector’s surveillance and censorship means on the premise of quality assurance, efficiency, as well as impact generation (see the essays by Bigo and Melgaço and Lyon in this forum).

Unfortunately, we are far too often blissfully ignorant to online privacy and security considerations. Many scholars will disregard this forum on the assumption that “this will never affect me.” They will feel assured about their status, comfortable with the academy’s widespread “technophobia,” and believe their research is “unimportant” and “uncontroversial” enough to be of little concern to anyone. They will thereby overlook their colleagues in less secure employment situations, discounting the changing social, geopolitical, and technological transformations, or perhaps forget that their own students or coworkers are operating their laptops when going on fieldwork in conflict regions and use their phone to audiotape interviews with subject at risks.

While certain academics might not feel concerned or moved by the examples discussed above, digitally supported censorship and surveillance take many forms, including having one’s work and data accidentally or deliberately tampered with, stolen for their intellectual and commercial value, or unwillingly released, held ransom, or locked behind a paywall or nationally imposed restrictions (Peisert and Welch 2017, 94). In our posttruth era where simplistic slogans, anti-expert sentiments, and disinformation persist, dealing with these developments proves particularly challenging when studying politically sensitive or controversial topics.

Some of us may have considered the abuse, attacks, and online harassment directed at female, black, Asian, and minority researchers (Marwick, Blackwell, and Lo 2016). Some of us may think more than twice before publishing a particular article or hitting send on an email or tweet. Some of us may have already given in and begun to actively practice self-censorship and risk aversion for the sake of not being perceived as controversial. With all this in mind, we should no longer ask the “why me?” but rather the “what if?” question (Peisert and Welch 2017, 94).

### Why This Forum and Why Now?

This forum was sparked by a roundtable discussion at the 2017 International Studies Association Annual Convention in Baltimore. In the course of it, many of the featured authors discussed the challenges for the academic profession arising from information and communication technologies. The growing reliance on digital tools to collect, store, and distribute data was at the heart of our conversation, as were the potential detriments of their inadvertent use. The panelists agreed that current technological developments require a critical debate on the way scholars potentially can be affected by online surveillance and censorship techniques. The roundtable discussion aimed to pinpoint some of these dangers and assess the technical and legal boundaries for scholarly work; not all of these topics are addressed here.

In line with our conversations in 2017, in this forum we hope to continue the conversation on the implementation of encryption tools in the daily academic profession. As recent events and the many cases featured here show, the incautious use of digital tools cannot only impede research participants, but also academics themselves. Raising awareness of the issue is particularly important for scholars who work in countries where online surveillance is omnipresent and where researchers engage with vulnerable groups.

The forum situates itself next to publications released in recent years, ranging from the special issue in *International Studies Perspectives* on “Academic Freedom in International Studies” (2007), the forum in the *Journal of Global Security Studies* on “Censorship in Security Studies” (2016), as well the issue on “Academic Freedoms in Turkey” in *Globalizations* (2017). This forum also embeds itself within the myriads of articles on the topics of which, unfortunately, only a small fraction are discussed here. Additionally, this forum fosters the expansion of digital skills and privacy and security best practices in academia (Tanczer 2017). Since the roundtable in 2017, three so-called “CryptoParties”—digital security trainings—for academics have occurred at the ISA annual convention (2017, 2018, 2019).

### The Current Forum

The forum centers around five concrete themes and aims to speak to all actors within the higher education sector, including established academics, early career scholars, PhD candidates, undergraduate students, as well as university administrators. Each article emphasizes a different issue: an extensive critique of our digitized infrastructures (Deibert), datafied institutions (Bigo), mercenary corporations (Franklin), exploitative academic platforms (Melgaço and Lyon), and insecure online practices (Kazansky and Milan). Due to this diverse focus, the essays fundamentally question the neoliberal academy, reveal the daily surveillance practices that students and staff encounter, and point to the necessity to improve our digital practices. In many ways, the forum is a commentary on the marketized regime that has hit the academic community with its datafication, digitalization, and managerialism and found a flourishing breeding ground in our halls, classrooms, and campuses.

The first essay by Deibert focuses on the fundamental question of how the Internet, which was created in and prospered through its use by universities, is no longer the same infrastructure nor based on the same principles it once was. Deibert articulates concerns on the growing scale of Internet surveillance and censorship, which is routinely practiced in both public and private spaces, including universities and libraries. He sees a need for more digital security awareness in the scholarly profession. The latter has become prone to phishing schemes (Changchit 2017) and targeted espionage (BBC News 2018a). Despite these risks and the expansion of third-party intermediaries, academics still seem to perceive digital security as something left to IT departments. Deibert therefore calls the higher education sector into action.

Shifting the focus away from the technical infrastructure, Bigo's essay critiques the move toward surveillant forms of governance and evaluation in research. The rise of administrative control over academics finds particular manifestation in the United Kingdom, where metrics such as the Research Excellence Framework, the Teaching Excellence Framework, and the Knowledge Exchange Framework assess, among others, scholars' publication output, income generation, student evaluations, and policy impact. This "audit culture" equally affects academics across Europe, the United States, New Zealand, and Australia (Ruth et al. 2018). For Bigo, this transformation decreases the freedom and autonomy upon which universities were built and solidifies a fetishism of numbers that reinforces a dominance of the average. In this climate, the surveillance of the "academic worker" is eased by technological means that have become tools to restrain, manage, and censor.

The third contribution by Franklin emphasizes the role that commercial actors such as *Google*, *Amazon*, and *Facebook* play in the datafication of the university and the monitoring of students and staff. Tech giants are increasingly subcontracted to offer services to academic institutions. They have made the higher education sector reliant on their products, including email clients, cloud storage facilities, and analysis programs. Despite businesses' intrusive data collection, the seamless convenience that these systems provide as well as the "technophobia" that scholars frequently uphold hamper the adoption of better security and privacy practices. Franklin consequently defends the implementation of encryption tools and technical skills into the scholarly profession. We should not see good digital security and encryption as a hindrance to our work, Franklin argues, but rather as an enabler that guarantees independent research.

Melgaço and Lyon follow up on Franklin's critique and hone in on digital academic platforms such as *ResearchGate* and similar sites such as *Academia.edu*. The authors do not only consider them as services that academics voluntarily engage in, but as manifestations of self-branding dynamics to increase one's own as well as one's institutions visibility. Melgaço and Lyon use the concepts of surveillance capitalism and surveillance culture to analyze the success of these publishing platforms, on which teachers and students have become reliant. Together, the forum contributions by Bigo, Franklin, and Melgaço and Lyon focus on "function" or "surveillance creep" (Marx 1988). The essays showcase how part of the control imposed upon academia is deriving from the use of technologies for purposes that they were not originally designed for nor envisioned (Edwards et al. 2018, 8).

The final contribution by Kazansky and Milan effectively closes this forum. The authors share a set of privacy-conscious digital security practices that can help academics to engage in responsible research amid the surveillance and censorship processes other authors have highlighted. Their article follows on previous publications that provide digital security advice to academics (Marwick et al. 2016; Tanczer et al. 2016; Owens 2017; Reeder, Ion, and Consolvo 2017) and publications that emphasize how to conduct empirical research, especially fieldwork in authoritarian regimes (Peter and Strazzari 2017; van Baalen 2018). Kazansky and Milan discuss the responsibility of scholars for protecting vulnerable groups and their networks that must be shielded from present or future means of surveillance and repression. The essay offers an important contribution especially to those actively engaged in ethnographic research and ends the forum on a hands-on, practical note that future work in this space can update and amend as apps and programs will change.

### Read, Enjoy, Reflect

Together, this unique collection of essays contributes to the growing body of research on the topic of academic freedom, as well as the imperative work on digital censorship and surveillance. The forum represents different voices, perspectives, and experience, all of which echo an increasingly panopticon state of the academy.



Each contribution concludes with practical recommendations to guide scholars' future action. Collectively all authors invite each and every researcher, student, and interested party to question practices and assumptions about the use of technology in our academic profession. We encourage readers to reflect upon held assumptions and to engage in meaningful as well as privacy- and security-sensitive behaviors that do not endanger academics or other members of our departments, academic community, and society. The forum, therefore, hopes to frame a discussion of how our reliance on insecure infrastructures, commercial tech giants, and controlling university administrations threatens free and independent research.

## Rescuing the Internet for Academic Freedom

RONALD J. DEIBERT

*University of Toronto*

Twenty years ago, I published an article in the journal *International Organization* entitled "Virtual Resources: International Relations Research Resources on the Web" (Deibert 1998). The article was a guide for IR theorists to the (at the time) new medium of communications called "the World Wide Web." It is hard to believe how recently such an article was written that describes a communications system we now take entirely for granted as something novel and almost entirely beneficial. How times have changed.

The Internet was largely born of the university and designed as a means to facilitate networking, collaboration, information access, and sharing of scarce resources (Abbate 1999). Over time, however, the Internet has been vastly transformed. It exploded in popularity outside of the academic community to include businesses, civil society, government, and many others. Most of this dramatic growth occurred because of commercialization and systems that facilitated ease of use. While the basic protocols that underpin the Internet remain in place, the devices and applications we deploy, and the large companies that run them, have fundamentally reoriented the infrastructure in ways that would be unrecognizable to the Internet's early pioneers. Today our Internet experiences are principally mediated by always-connected mobile devices containing dozens of applications that push content and services while collecting information about us and our habits (Zittrain 2008).

The political and security context surrounding the Internet has also changed dramatically. In its early days, most governments took a hands-off approach to Internet policy to encourage economic innovation. Over time, as Internet security issues mounted, and as the Internet spread beyond the United States and to the developing world, governments have become far more interventionist (Deibert 2013). The Internet has become an object of intense struggle for geopolitical advantage and the exercise of political power. Many governments have already or are in the process of developing cyberwarfare capabilities. Internet censorship and surveillance have become normalized, and a huge market for cybersecurity products and services has provided authorities with means to undertake extensive information controls.

In short, what started as an infrastructure for academics has become something entirely different within which students and researchers are now completely enmeshed. That infrastructure may no longer serve academic scholarship in ways the original designers envisioned; indeed, it threatens to undermine it. In what follows, I review some of these more troubling trends and make recommendations for mitigating them.

### Growing Internet Censorship

The Internet was designed to facilitate seamless sharing of information. As it has grown, so too have concerns around access to controversial content and, thus,



restrictions. Internet censorship is practiced routinely now in schools, libraries, businesses, and on a national scale. A growing number of countries routinely filter, throttle, or otherwise interfere with access to the Internet, including liberal democratic countries (Deibert et al. 2008). Controlling information is also big business: cybersecurity companies make millions selling technologies that shape, restrict, and deny access to information on behalf of governments.

Internet censorship can take place at different points across the network. In many countries, keywords and websites are filtered as they pass through Internet gateways at national borders. However, these national-level firewalls can be prone to under- and overblocking and bypassed using circumvention technologies. As a consequence, it is now common for governments to mandate that Internet companies police their own networks, effectively “downloading” Internet censorship to the private sector. In China, for example, Internet companies are required to police their users, monitor chats and forums, and share information with the government’s security services on demand (Liang et al. 2018). This requirement not only means that information controls extend deeper into the application layer of the Internet, but also that Internet users experience a diversity of information controls.

Restricted content can vary widely as well, from pornography to religious material, to content critical of governments such as human rights reports or opposition websites. In many countries, including China, Saudi Arabia, Turkey, and Uzbekistan, access to portions, or even the entirety, of Wikipedia are filtered (Zittrain et al. 2017). Many liberal democratic countries also censor the Internet for hate speech, extremism, and copyright violations. Internet service companies such as *Google*, *Facebook*, and *Twitter* now routinely struggle with incessant demands from governments for removal of content or policing of networks, particularly content related to terrorism.

Internet censorship may happen in response to specific events, such as controversial anniversaries, elections, demonstrations, or discussion of sensitive topics. The most drastic form of information control is when the Internet is shut down entirely, defined as “just-in-time” blocking (Deibert et al. 2008, 7). Just-in-time blocking reflects a recognition that information has its most strategic value at critical moments. Access Now, an Internet advocacy group, has been tracking Internet shutdowns as part of its #KeepItOn campaign. It found more than 55 instances of Internet shutdowns in 2016 alone and 61 in the first three-quarters of 2017 (Dada and Micek 2017). Shutdowns can occur in specific regions or even neighborhoods. They can affect specific services or applications, such as when mobile services are disconnected. Governments have given many reasons for these disruptions, from quelling unrest to stopping students from cheating on high school exams. The latter is particularly noteworthy for its impact on academia. Access Now has documented more than 30 intentional disruptions to the Internet by authorities ostensibly to prevent cheating on exams (Olukotun 2017).

Interferences with Internet access can have varying degrees of transparency. In some cases, when users attempt to access banned content, they are presented with a block page. In other cases, no information is provided at all, or block pages are presented as network errors in order to disguise censorship. For instance, a report in the wake of the death of human rights activist Liu Xiabo found that WeChat silently removed images of Liu that were sent on one-to-one and group chat messages (Crete-Nishihata et al. 2017). Neither sender nor recipients were notified that images were removed, leaving both in the dark as to what had occurred.

University networks are the entry points for both students and staff to connect to the wider Internet, but they are, in turn, embedded within a country’s infrastructure and subject to the information controls described above. What was once envisioned as a seamless web of information has become, instead, something much more fragmented and distorted. These barriers have tangible impacts on academic freedom, frustrating and denying the pursuit of information. Scholars can

experience entirely different “Internets” depending not only on the country in which they are located, but also the internet service provider, device, or even application they use. Restrictions on access to controversial content, such as that related to terrorism, can inhibit important research on the topic itself (Tanczer et al. 2016). The most basic of functions that the Internet was meant to provide for academics—an entry point to a common pool of shared resources—is now littered with a growing thicket of opaque barriers.

### Growing Role of Internet Intermediaries

One of the biggest changes associated with the Internet has been the emergence of large private companies in which data and services are concentrated: companies such as *Facebook*, *Google*, and *Twitter*. These companies have become important gatekeepers of information. They are the principal avenues through which information is accessed, archived, and shared—with important implications for academic research.

First, their proprietary algorithms can shape, distort, and limit access to information and freedom of speech in critical ways. Beyond compliance with government regulations described earlier, companies push and pull information as part of their core business model that involves fine-grained surveillance of users for advertisement promotion (Flyverbom, Deibert, and Matten 2017). The implications of this for academic inquiry can be seen most simply in the use of search engines. Whereas, a few decades ago, an academic’s search might have begun in the indexes of the library, today they begin with a search engine such as *Google*. *Google’s* and other companies’ search engines do not produce unbiased results but rather results on the basis of proprietary algorithms (i.e., the rules that govern the search methods). Algorithm inputs can include browsing history, prior search results, user geolocation, and more. The actual results of specific searches can thus vary by user and location, shaped by the company’s commercially driven algorithms (Epstein and Robertson 2015).

A second way in which these companies affect academic inquiry is through reliance on their services. Many academics and universities use *Google*, *Microsoft*, *Dropbox*, and other cloud service providers to host their information or email services (see Franklin in this forum). Information that used to be stored on desktops or behind locked doors has been pushed to the “cloud.” While the metaphor of the “cloud” suggests something intangible, in practice it means data stored on servers in some specific physical location, transmitted through cables or other media, in some cases crossing several national jurisdictions. While there are unquestionable gains in one form of security and convenience, there are substantial tradeoffs in privacy and other types of security. The Snowden disclosures showed vividly how American and other national security agencies access customer data contained in clouds through lawful access requests and other means (Bohaker et al. 2015). Academics who rely on cloud services can unwittingly expose their sensitive data not only to governments, but also to numerous third parties with whom companies share that information.

Third, these companies control massive repositories of data that are actually relevant to critical research topics. The less researchers know about how this data is used to shape and limit users’ communications experiences, the less they can authoritatively claim to know about what are arguably some of the most important public policy issues of the day, from privacy, to censorship and surveillance, to disinformation, or radical extremism. Who exactly can access information companies consider proprietary is something that the companies themselves dictate, not always transparently or fairly (Boyd and Crawford 2011).

Lastly, and relatedly, companies can affect the nature of research more directly, by funding certain types of research while excluding support for others. Internet

companies have become among the wealthiest companies in the world. *Apple*, *Alphabet* (the parent company of *Google* and *YouTube*), *Facebook*, and *Microsoft* have market valuations in excess of hundreds of billions of dollars. As recent controversies have shown (Solon 2017), companies whose business model rests on surveillance of users' online behaviors are unlikely to sponsor research that undermines that model or helps users become aware of just how much they are giving away. Companies will also not likely look favorably on research that highlights embarrassing collusion with governments on surveillance or censorship.

### Mass Surveillance

The Internet's initial architects almost certainly did not foresee the way it has become one of the greatest tools of mass surveillance in human history. There were three separate but complementary driving forces in this unintended development. The first is the explosion in state surveillance practices in which digital data analysis is a key component—a trend accelerated with the events of September 11, 2001, and continuing with the seemingly unending war on terror. The second is the rise of the “datafication” economy, at the heart of which is the exchange of personal information for free services and the value-added analysis of that data for advertisement (Dijck 2014). The third is a new culture of auto-surveillance—the voluntary sharing of fine-grained details of personal lives. Internet users leave digital traces wherever they go and whatever they do, even traces of which they are unconscious, such as the metadata that is broadcast by their mobile devices as they carry them in their pockets. These digital traces are vacuumed up, analyzed, shared, and sold by both states and governments, fueling a new cybersecurity industry where big data meets big brother (Deibert 2013).

Although it is too early to conclude definitively about its impact, there are signs this new era of mass surveillance will negatively influence academic freedom. In a pioneering study of the topic, Penney (2016) analyzed editorial contributions to sensitive Wikipedia topics and found that those contributions markedly declined in the wake of the June 2013 Snowden disclosures. People behave differently when they suspect observation. They are less likely to take risks for fear of legal or other sanctions. Overall, this chilling effect induces conformity and self-censorship, both contrary to principles of academic freedom.

While the climatic impacts observed by Penney (2016) are noteworthy, there may be other more direct implications of mass surveillance for academic freedom and security. Governments or companies that know what a person is studying can take steps to “neutralize” the research, even if a scholar or student resides in a different country. In this instance, academics communication patterns could put study subjects or partners at risks, and result in adverse consequences for individuals in places abroad (van Baalen 2018).

### Targeted Digital Espionage

Mass surveillance refers to wholesale collection of large volumes of data. Targeted digital espionage refers to clandestine operations aimed at collecting data from specific individuals or organizations by compromising networks or devices. Numerous governments are known to conduct targeted digital espionage, against each other, businesses, and civil society. Over the last ten years, the interdisciplinary *Citizen Lab* (2014) has documented an epidemic of targeted digital espionage campaigns against a broad cross-section of civil society groups, including journalists, activists, lawyers, human rights defenders, and academics. These operations undermine civil society organizations' core missions, sometimes as a nuisance or resource drain, more seriously as a major risk to individuals (Scott-Railton 2016).

Academics are especially vulnerable to targeted digital espionage. Scholars share information, click on attachments, open emails, and access online resources perhaps more intensively than any other sector of society. As a professor in a typical day, I may receive dozens of emails containing attachments from students, fellow researchers, foundations, or others, many of whom I do not know personally or trust. As a professional expert on digital security, I am aware of the risks and take precautions. But many of my colleagues are not. Meanwhile, there is very little systematic digital security support for academics (Tanczer et al. 2016). Some departments have a single IT person who is overwhelmed with a range of tasks, while others may have no one. Trainings are virtually nonexistent, and those that do happen are often one-off experiences with little ongoing support. Folk wisdom is passed around, not all of which is reliable and some of which is counterproductive. Ironically, the very principles that underpinned the Internet's original success—the sharing of scarce resources in a largely neutral fashion on the basis of trust—have become vectors for large-scale insecurity. Academics involved in or researching controversial topics are particularly at risk of targeted digital espionage and may not even know it.

### **Conclusion: Moving Forward**

Scholars find themselves working in an infrastructure no longer of their own choosing. While that infrastructure can still facilitate research, it has also become a hindrance and even a threat. It might be tempting in light of these trends to become a Luddite, to question the utility of all technology and detach from the digital world altogether. Not only would that choice be highly impractical, it would do a disservice to the original motivating principles that gave rise to the Internet in the first place. In a tightly compressed world with many shared problems, academics need a shared and secure commons of information and communications. Rather than reject the Internet, we need to rehabilitate and rescue it.

First and at a most basic level, digital security requires more systematic attention. Fortunately, some companies have already started to raise the security bar for all users, which in turn will affect academics. There are also more security products being designed that are user friendly, which will empower users to be safer online. But new products and applications alone will not suffice; academic behavior needs to change as well. Academics are accustomed to freely sharing digital information and clicking on documents, attachments, and links with carefree abandon. Sharing is still essential, but norms and practices around exactly *how* we share will require systematic rethinking. Digital hygiene—as discussed in more depth by Kazansky and Milan (in this forum)—must be seen as foundational to, rather than an accessory to, academic life. Universities and departments should make the necessary investments in digital security accordingly to protect academic inquiry from the threats described above. Professional associations and journals also have an important role to play as norm entrepreneurs in this respect.

Second, the broader trends described will require a longer-term and more comprehensive approach. Here it is important to remind ourselves as academics that the Internet was largely born out of the university. The university as an institution, and each of the specific disciplines that comprise it, have a special obligation to play to protect and preserve the commons of information as an arena of access to information, freedom of speech, and privacy. This will require more direct engagement with Internet governance from the international level through all layers of the Internet, down to the forums within which standards and regulations are set. The headlong rush into cybersecurity has securitized these forums in ways that have privileged private sector and secretive government agencies (Deibert 2015). Academics must reinsert themselves into these processes and push for greater transparency and accountability (Franklin in this forum).

Beyond advocating for principles, academics should work collaboratively to expose rights-infringing practices of both states and companies. Rigorous, evidence-based research is a powerful means to shed light on what is happening beneath the surface, whether the latter involves proprietary algorithms, commercial spyware, or nation-state surveillance (Bodo et al. 2017). Part of this effort should involve shoring up defenses against emerging threats to certain modes of analyses that will be essential to such a mission. Reverse engineering—broadly construed as “hacking” in the original sense of the term—should not only be seen as a right of inquiry but an essential ingredient of a critical democratic society. You cannot question what you cannot see or know.

Engaging in scientific research of all kinds is inextricably linked to access to information, free expression, and privacy. While the Internet was created by academics to help facilitate these principles, it has transmogrified into an entirely different creature that now threatens to undermine them. The time has come to take it back.

## **Digital Communication, Surveillance, and Academic Freedom in the Transnational Universes of Competing Homo Academicus(es) Institutions**

DIDIER BIGO

*King's College London, Sciences Po Paris*

In line with my fellow coauthors, I consider it is central for academics to learn how to manage their digital communications and to have an informed knowledge about the technical measures required to protect their and their participant's data from third-party intrusions. However, too few understand that we do not only have to train researchers on the requisite for digital security in sensitive domains of inquiry, but we also must question how universities' administrative authority over academics may itself turn into a form of control and be reframed for the purpose of internal surveillance.

We are far from a social universe in which education is considered a “public service” and a necessary public expenditure; where one's mother tongue is defended against the hegemonic position of large-scale, English-speaking education institutions (Altbach 2008); or where pedagogy takes precedence over global branding techniques. Rather, education has become a profitable activity—one where competition on delivering diplomas has converted teaching and learning into a “sale” (Jessop 2018) and where the top universities invest increasingly in noneducational resources and introduce mediated administrative specialists that intervene into the face-to-face relation between teachers and students.

This reconfiguration of power inside the university—with its top administration more or less independent from its academic staff—has played out around the mastering of digital and distant technologies (Lupton, Mewburn, and Thomson 2017). Thus, I want to highlight why surveillance in academia is the result of the previous acceptance of digitization, datafication, and evaluation. The present essay embeds this surveillant transformation within the context of the Anglo-American higher education sector and is split into two parts.

First, I discuss the importance of protecting scholarly communication from the danger of external commercial and malicious access or internal bureaucratic oversight and recording. Tools of countersurveillance for complicating the collection of personal data and protecting privacy against institutional logics exist (Kazansky and Milan in this forum). Yet, these techniques are by themselves not the solution

against online surveillance within the higher education sector and will not save “academic freedom” as such.

Second, I will question the conditions allowing academics to critique institutional powers in the contemporary climate. Indeed, an internal bureaucracy of surveillance and evaluation practices of pedagogic activities are prevalent. Yet, they are only a visible part of some more profound transformations of the everyday life of the different “homo academicus(es)” that populate the transnational field of higher education to date (Bourdieu 1988).

Together, both points direct scholars to scrutinize the neoliberal, controlling changes academic institutions are undergoing. But, in terms of reflexivity, this is not enough. Researchers and professors have to critically evaluate the forms of symbolic power and violence existing inside the university and untangle a discourse presenting the academy as either a “community” led by the pastorate of top administration or as the innocent “prey” of external forces of capitalism. To achieve this, we have to use and defend our academic freedom to act collectively in order to alter our conditions of work and accept that compliance is not the only way of behaving in this surveillant environment.

### **When Online Communication Becomes Online Surveillance**

Academic freedom means a positive liberty, an “obligation” for scholars to be creative, original, and even dissident in their research and teachings. A scholar is not a coach nor a repeater; our independence implies an intellectual obligation to challenge conformist majorities, be they from government, companies, or civil society. Yet, academic freedom is increasingly being contested, especially online (Falk 2007; Mittelman 2007; Tanczer et al. 2016). Universities manage the traffic as well as monitor the metadata and content of emails or web searches of students and staff (Perrino 2013). The surveillance in terms of the interpretation of previous data has the possibility to build up suspicion of engaging in political behavior.

In particular, the situation of academics in Turkey, Mexico, and Cameroon has been worrying, with scholars spied upon, censored, and even imprisoned (Chuh 2018). These chilling effects impact liberal democracies as much as others, and digital technologies have made state control quicker and easier than ever before. The Scholars at Risk monitor report restrictions across many states in which online discussions are kept and read as indicators of allegiance or political defiance (Scholars at Risk Network 2017).

Framed under legal requirements, the collated information is also used to assess the degree of obedience of academics to some administrative decisions by reporting declaration of dissent. This allows contemporary universities to become places where mundane technologies are transformed into sociopolitical instruments and forms of symbolic power asserting a certain kind of governance. For example, during the 2017–2018 UK industrial actions, British universities created a chilling environment by obliging their staff to declare through electronic means whether they were planning to participate in the strike. Some institutions were accused of registering the presence of staff members by monitoring electronically the opening of office doors, with such measures used to destabilize the solidarity between academics. Despite their illegitimacy (University and College Union 2013), such techniques of both off- and online surveillance have become accepted as a “normal” practice across many institutions.

The use of “safe and integrated” technologies that trace pedagogical activities such as “lecture capture” are hereby noteworthy. Justified in the name of commendable impetuses such as widening access and support for handicapped students, the gathered video and audio recordings are kept for months, even years. In the current competitive academic environment, the footage has also been repurposed for scholars’ performance assessment and shown to function as



strike-breaking material, with some UK universities reportedly having attempted to “replace” striking academics with recordings of their courses made previously (Edwards et al. 2018). Similarly, many universities use email systems provided by major US companies such as *Microsoft* or *Google* and disregard privacy concerns deriving from reliance on commercial vendors in the name of cost effectiveness (Franklin in this forum).

Such surveillant digitized practices are implemented under the terminology of “community,” used to refer to the collectivity of people working at the university. This description has been reinforced by the utilization of multiple email lists, as if they were a manifestation of the existence of such a shared understanding. However, the idea of a “community” plays into the hands of a managerial surveillance capitalist logic to disregard disagreements and to discipline individuals that dissent. The “solutionism” by the “community” has replaced the notion of the distribution of wealth and a fair repartition for the workers all along the line. Hence, we have seen the differential of money and privileges at the top administration going hand in hand with this “community” discourse, especially when online technologies have become effectively a substitute for face-to-face relations. This shift deriving from neoliberal ideals allows for a concentration of power in certain buildings and places and a culture of “managing at distance by spreadsheets.”

Counter practices as discussed by my coauthors certainly disrupt parts of this dynamic, and alternative communication channels outside the university control exist. Yet, a call to counter practices supposes consciousness about the multiple tactics used to trace digital content and inherently contradicts our acceptance of surveillance in the name of necessity of digitization. Academics in the Global North may consider themselves as privileged by having access to speedy Internet and diverse technologies that help them to manipulate large amount of data swiftly. However, we cannot universalize the positions of Global North academics as if they represent the global higher education sector, nor are they better than others in terms of pedagogy. More, we must discuss digitization in terms of what we lose rather than solely what we win.

The unreflective strive for digitization is best seen in the preparations of lectures via PowerPoint and other presentation software. Even if slideshows are loved by students, they do not prepare them with better understanding of content and disincentivizes critique and inquiry (Worthington and Levasseur 2015). Indeed, one has to remember that PowerPoint was invented for commercial purposes, with the sequence of the slides aimed at creating an unconscious acceptance of the text by the audience (Marx 2006). The calibration of pedagogy via online PowerPoint lectures is—in some ways—the first attack on academic freedom by normalizing easiness and by creating the earlier mentioned reproducibility of lecture content. The use of PowerPoints is a move away from the Socratic method in which questioning drives the importance of learning, which fundamentally refuses any form of standardization.

The reliance on digital tools and virtual environments also centers on a belief in efficiency, democracy, and accessibility. Nonetheless, they are more a dramaturgy of the scene of higher education playing a world utopia of knowledge for everyone than the description of local and international practices. The latter are constituted of symbolic struggles in the field of higher education and its transnationalization whose effect has been a reconfiguration of power and the development of “palace wars” between Anglo-American universities (Dezalay and Garth 2002).

### **Administrative Logics in the Digitized Environment**

The abovementioned digitization, which allows for the monitoring and controlling of scholars’ communication and practices, goes together with administrative logics of university managements that flourish on entrepreneurial ideals, internal



bureaucratic oversight, and a generalized institutional competition. Datafication and evaluation are the outcome of this trend toward “academic capitalism” (Jessop 2018, 104) and give scholars the impression of being permanently under observation and affected by a series of modalities that operate mundanely.

For instance, Kauppi and Erkkilä (2011) show how this competitive doxa is the effect of the struggle over higher education and the practices of ranking. An industry of ranking has emerged and transformed the relations of symbolic capital between researchers and professors as well as their sense to belong to a collective scholarly group (Erkkilä 2013). Individual rewards are far easier to win by academics’ simply adjusting their ideas to the institution they operate in and by following the suggestions and requirements of their administration. This creates barriers for allying with colleagues faced with different realities or located in non-English-speaking universities such as in the Global South.

In addition, the managerial hypocrisy over academics also works at the heart of some ethics committees and other governance mechanisms. Review boards often mainly act as insurance policies or “institutions of censorship and control” for administrators keen on pushing any fault on staff or students’ shoulders if they have taken too much risk for themselves in a specific situation (Sluka 2018, 1). Additionally, rising organizational regulations change the symbolic powers between students, academics, and the university executive and further lead to a form of control that deprives scholars of their judgments and opportunities for action. Thus, by disaggregating the direct asymmetric relations one might actually uncover the introduction of “parasitic” logics that justify an exponential growth of levels of administrators (Serres 2007).

The other structural transformation that works against academic freedom is the process of normalization induced by the mechanism of permanent evaluations at multiple scales (MacDonald 2017). Like the increasing digitization of data, “evaluation” seems by definition a democratic tool and is, as such, always considered positive. It allegedly limits “mandarinate” (clientelism) of old professors, creates “fair conditions,” and narrows discrepancies by assuring equality between different actors including students and staff. And indeed, the reliance on statistical tools together with the disaggregation of education into measurable parts is steadily becoming an element of the doxa that underpins the transnational field of higher education.

Yet, evaluation processes applied to “pedagogy” have shown to create forms of disciplinarization and surveillance embedded in the logic of competition between universities as much as students and staff. Numbers and statistics are there to “correct” the effects of practices of pedagogy. Everything needs to be transferred into figures and graphs, with institutions striving for a smooth ascending curve of success that will never turn back. In the course of this, distant administrators and their technologies of ranking, indicators, and matrices supersede face-to-face relations, creating hierarchies of “best producers” on this profiled market for diplomas (Erkkilä 2013).

Evaluation is, therefore, not a neutral technique and has the capacity to disembody and dissociate human relations. It is a politics that works against education and implies an asymmetry of power, in particular between professors and students. Clients or consumers—as some universities call their students—have certainly the right to feel protected against discretionary logics. However, what does it mean for the freedom of academics when the latter implies a reliance on practices that foster the “harmonization of marks,” where administrative bodies do not accept heterogeneities and rather govern by “regularities,” where discrepancies between the marking of diverse academics is erased, and where the grade distribution is dependent on previous years’ statistics, independently of the inner quality of a year’s cohort (Bachan 2017)?

The competition via ranking and evaluation is not only happening in the space of our classrooms. It upsets also the space of publications by trying to impose through the popularity of an audience an inner differentiation of excellence where older journals that had time to build their reputations profit from a structural advantage over new ones. In this surveillant climate, heterodox positions—that often can be the most creative ones—are marginalized and orthodox positions—that frequently align with the logic of certain “old” universities—are reinforced (Hamati-Ataya 2011). This finds its repercussion in citation practices, where references to innovative ideas barely move beyond a small circle of scholars and creates an impetus for academics to curb their ideas along the lines of the “most important” journals of their disciplines. Hence, the scientometry, which was promoted as an allegedly equalitarian tool, imposes—discipline by discipline—a restricted and hierarchized list of publications.

Individual researchers are not safe from the effects of evaluations either. By scoring individuals online with a personal record (Melgaço and Lyon in this forum) and asking for their impact, private companies challenge universities on their control over personnel. This datafication of academia affects recruitment by constructing specific profiles adjusted to each “job.” Young scholars with some of the most original trajectories are excluded from interviews because they have not yet ticked the boxes of the long list of requirements, with some scholars even being disregarded because they are too qualified for the job. This politics of numbers results in a dehumanization and shows what “unfreedom” means in “advanced liberal societies” where no one is “responsible” for the structural conditions that govern higher education institutions.

Academic freedom is certainly a value at stake in such an environment that some have called the “neoliberalization and marketization” of the university (Chubb and Watermeyer 2017, 2360). Many authors have traced the sociogenesis of such practices (Bennett 2017); they insist on the specificity of the subtle modes of coercion that modern education continue to use in its different pedagogical models (Lenoir 2006). Evaluation and datafication, thus, rhyme with practices of distinction as much as the search for the average, and build on the idea that “authority” must be controlled, and that the freedom of academics has to be regulated if it does not fit the goals of the institutions. Hence, academics may better begin to adjust to their new economic roles with recipes on how to succeed in this environment most likely coming from industry.

### Conclusion: Moving Forward

All the discussed factors around digitization, datafication, and evaluation explain the loss of freedom and the development of online surveillance internally in universities. They are products of the competition between universities who want to become “profitable” and hope to attract (international) students who can pay fees. Dispositions of academics have therefore guided toward an *allegiance* to their “company,” their “community”—the university. Academics must feel that they struggle together against other entities. They must build team spirit not on an intellectual basis, but by belonging to a physical place. They must participate in the race on ranking as their own future may depend on the rating of their (previous) university.

The embeddedness of this “inside and outside” dynamic and the effects of this competition both obliges and accelerates compliance. New lecturers may believe they have to give in to this administrative authority and its surveillant practices. This in turn also limits the resistance of old professors’ hysteresis of dispositions in an environment that begins to be hostile to the very idea of education and is more concerned with the sale of diploma as a product in a global market of higher education.

As this essay and the contributions of my coauthors show, this reconfiguration of power inside the university plays out around the mastering of digital technologies as well as datafied practices and inherently is underpinned by a doxa of “deresponsibilization.” This “unfreedom” comes from the acceptance that no one has a choice to go against the system and its rapid transformations. It assumes that resistance is useless and that academia has to adjust to the client’s desire and the expectations of its administrators. And indeed, soon artificial intelligence may be the *deus ex machina* of higher education, but let me end by a proposal to fight back collectively. First, academic freedom begins with the patient deconstruction of these digitized and marketized “necessities,” using the memories of what the institution of the university has been in the past as a model for what it should be in the future. Second, academic freedom revives by the rejecting of administrative authorities and allying with younger colleagues, students, and colleagues and students in non-English-speaking universities. Third, academic freedom wins by critically engaging with online and digital technologies that are increasingly used against us to monitor our outputs, control our processes, and manage us by distance. I am not sure if we will win, but at least we will finally oppose our surveillant conditions.

## University Life Corporatizing the Digital: Academic Agency Interrupted?

M.I. FRANKLIN

*Goldsmiths University of London*

Despite the furor around the Snowden revelations of mass online surveillance in 2013, state-sanctioned, data-gathering, and long-term storage of communications records have become the norm in liberal, capitalist polities. Not only government agencies but also commercial service providers now Hoover up and store vast amounts of personal information, ostensibly for our own good. The “chilling,” (self-)censoring effects these practices create, have gained a foothold in the increasingly porous domains of digitized, networked scholarly research, knowledge exchange, and university teaching.

However, academia as a whole has been alarmingly slow in responding to the corrosive consequences that disproportionate levels of surveillance have on individual rights and freedoms and those that relate to scholarship (e.g., freedom of association, of information, and of expression). In everyday university life, a creeping paralysis underpins the relative diffidence of many academics, departments, and institutional managements toward these issues. While student assignments, research proposals, scholarly writing, and the myriad of communications that sustain these activities become predominately digital, the time and resources needed to consider the institutional, personal, and professional implications of state-led and corporatized practices of online surveillance are in short supply.

One immediate response to the prying eyes of 24/7 digitized management tools and the ubiquity of mobile, commercial services is the deployment of readily available and constantly improving encryption tools across the spectrum of research, learning, and teaching. These can help to better protect our and other people’s privacy when emailing, browsing, and researching. Yet, the important work done by so-called Cryptoparty events notwithstanding (Tanczer 2017), the working knowledge of staff and students about *why* encryption may be relevant and *which* tools work best for particular contexts and needs is still not widespread. On-campus and curriculum-based opportunities to learn, debate, and acquire the requisite level of know-how go begging.

An increase in the prominence and proactiveness of government agencies within Internet policy-making has been throwing these “disconnects” into relief. This shift encapsulates Foucault-influenced historiography of how liberal institutions—schools, hospitals, prisons, and universities—operate as disciplining agents for the purposes of state-sanctioned surveillance, security, and population control, practices that are now digital and networked, by design (Dawson 2006; Franklin 2013; Haskins and Jacobsen 2017). It signals a different trajectory after the twinning of government disinvestment in public service media and public education with the embedding of corporate ideas and its related consumer goods that connect personal, digital communications with business and learning. The “neoliberal university” has been coming-of-age as commercial social media platforms corner the global market, “linking in” the hearts and minds of students and scholars in so doing (Giroux 2013; Ergül and Coşar 2017; Bigo in this forum).

The civil liberties implications of this partnership between commercial and governmental actors has been a primary focus of digital privacy and human rights advocacy for the online environment (Internet Rights and Principles Coalition 2018). The relationship also goes to the heart of what is happening at universities around the globe: managements unilaterally automate (“centralize”) fundamental aspects to the working academic environment (from recruitment through to attendance registers, through to marking and feedback) and to outsource the core information and communications services to sustain university life at the infrastructural level of operations (Deibert in this forum). However, as I and other contributors to this forum argue (Bigo; Melgaço and Lyon in this forum), the subcontracting of data-storage and core-service provisions such as email, calendars, or academic reference lists to private companies undermines the ethos of public education, intellectual freedoms, as well as our (digital) autonomy.

Within this context, how can we—students and academic staff—(re)discover our autonomy as humans but also digital, networked agents? How can we gain the requisite knowledge to counteract? Indeed, how can we refresh our ability to tackle the lack of transparency and accountability in decision-making about internet design, terms of access and use, and data management? Becoming more tech-savvy is certainly one way to provide alternatives and increase our room for maneuver (Reeder et al. 2017). That said, this sort of approach is neither self-explanatory nor immediately available for staff and students who consider themselves “not techie.”

### How Did We Get Here?

Global businesses, the tech giants of today—*Google, Amazon, Facebook, Apple,* and *Microsoft*—have been consolidating their influence across the education sector (Redmond 2014; Kaelin 2017). Corporate marketing on the “convenience” of cloud-based data access and storage has reached cash-strapped university managements and the individual “Internet users” comprising of academic staff as much as students.

We have been made to believe that our data—our scholarly imaginations and, by association, the outputs of our labor—are more secure in commercial hands than they could possibly be in-house, on campus servers, or local forms of storage. This move away from internal, publicly funded services to outsourced, privately run providers had major implications for the power geometries that underpin the relationship between teaching and learning, research and knowledge exchange, and access to resources and information.

The increasing reliance on external proprietary services to facilitate *where* and *how* teaching and learning takes place, but also to manage the knowledge—as data—that is produced by these interactions is a key factor in any discussion of the interconnection between surveillance, censorship, and encryption. Take, for example, “old-school” email. Far from becoming obsolete, emails are an essential feature of

university life. Email interactions are booming and so is the big business of gate-keeping email-server and data-storage facilities accordingly (Melgaço and Lyon in this forum). The volume of traffic is expected to reach 12,864 *petabytes* per month in 2018 (Statistica 2018), with one forecast projecting that a total of 246 billion emails will be sent in 2019, equaling an increase of 3 percent (Radicati Group 2015, 2).

Daily email exchanges span the spectrum from banal to sensitive information. Their content may include—frequently unwittingly—personal information about students (ID or name), admissions and enrolment documentation (digital scans of passports), examination results (marks and comments), mitigating circumstances evidence (health records), and geolocation information (from automated attendance registrars). Hence, decisions around the management of these expanding datasets, their terms of use and access, as well as the compliance with a range of national and international regulations have important implications—implications for those who generate these data, those who are the subjects of the information produced, and those who would like to access these data at a later date. Changes in the governance of email services alone affect not just teaching and research staff or departmental and senior managers. It also covers students as their “lifelong,” outsourced, yet university-branded email addresses become corporate proxies.

Moving from the classical, office-based computer screen to the classroom, halls of residence, and libraries, there too an array of web-based teaching tools are in use. Students operate their mobile phones or other networked devices at will and during class. They also tend to opt for easy-to-use, commercial technologies such as *Google Scholar* rather than institutional services such as academic journal aggregators (Flavin 2016). This means that locational data, student information, copyrighted content, alongside a plethora of metadata are being circulated beyond the campus and frequently spread across commercial apps that now drive how we learn and how we teach. This amounts to a corrosion of institutional autonomy and of global academia’s digital archive. Although this is a foregone conclusion in technological terms, it is a political and economic decision—in which powerful corporate actors join forces with law enforcement and intelligence agencies—at the design and public policy level.

In addition to the expansion of industrial influences, the UK Investigatory Powers Act (2016) exemplifies the return of the state in the once “deregulated” domain of telecommunications and media. The gathering and storing of communications data before probable cause has been established is now enabled (Necessary and Proportionate Campaign 2014; Pillay 2014). It does so under the guise of national security, with effects for civil liberties and the higher education sector specifically (Tanczer 2016). While the Act has been challenged, ruled incompatible with EU law in 2018, such legislations are tantamount to the criminalization of everyday life and exposes intellectual endeavor and scholarly exchange to unnecessary and excessive forms of scrutiny. These measures also govern the conditions under which university managements make decisions, how university-based Internet access is provided, which devices (computers, library cards) are issued, and have ethical implications for funded research.

The erosion of our capabilities to *want* and *know how* to take action, let alone having the time and resources to do so, accompanies the ways in which ordinary “users” become positioned as ignorant and passive rather than active agents. Meanwhile, as the workplace goes mobile, the cost-attractiveness of private cloud storage sees IT departments—whose managements engage with and consider the priorities of service “providers” and senior administrators—take procurement decisions without fully informed consent of students and staff. Put another way: we are seeing the ceding of both institutional and personal agency; “data actors” are being positioned and conditioned into behaving like passive “data consumers” as vested interests dictate the terms of Internet-dependent scholarship (Feenberg 1999; Tanczer et al. 2016; Alim et al. 2017).



### Conclusion: Moving Forward

The geopolitical and technoeconomic context in which all contributors to this series are writing is one marked by, what I have argued is an emerging (global) *Internet governmentality complex* (Franklin 2013). In it, states are but one—and not even the most powerful—actor making decisions about the Internet’s design, use, access, and content management. As students, teaching staff, and the university managements continue to exchange not just implicitly but explicitly sensitive information with one another, the gap between those becoming aware of encryption as a personal and political issue and those who do not know—or care to know—is widening. The main obstacle at the individual level—and with that to organizing any forms of collective action—is that most people take the path of least resistance. Convenience is a powerful form of persuasion in this respect.

This is one reason why advocating the need for encryption, or providing “to-do” lists for changing our privacy settings, will not go far without preparing the ground first. As predominately technical, behavioral responses at the individual rather than the institutional or epistemic-community level, these moves imply changes of routine, habits, and time-investment, in order to learn how to use encryption tools. It requires we consider how and where we manage our files and how we compile content or maintain online correspondence. We have arguably reached an historical conjuncture in which crypto-skills are becoming a necessity for the sustaining of a healthy scholarly life. It is time for educating, mobilizing, and organizing ways to address the widespread state of digital inertia among academics and student bodies.

By way of contributing to recommendations from other authors, allow me to make the following observations for the ordinary, cryptophobic scholar/student: first, recall that encryption is a technique that need not be deployed immediately. Knowing *how to* does not require you to *have to*. As Foucault (1977) reminds us, knowledge is power. Thus, simply considering the pros and cons of any form of encryption, or even how to enact low-tech forms of obfuscation (Brunton and Nissenbaum 2015), can be a form of reempowerment at the individual level, as part of research collaborations, and in the classroom.

Second, we need to include these considerations as part of the ethical dimensions to research design, especially when working in precarious research fields (Peter and Strazzari 2017; Sluka 2018; Kazansky and Milan in this forum). In this regard we need to consider privacy settings and encryption tools as more than techniques. They are also an imaginary, comprising elements of both resistance and concession to the big business and geopolitics of our digital, networked times (Bigo in this forum).

Third, note that encryption is already part of our daily lives. All sorts of transactions are made possible by its deployment in online services for banks, insurance companies, local and national governments, inland-revenue departments, as well as the health and education sectors. This puts things in perspective, prevents people from rejecting the idea out-of-hand (e.g., students have expressed unease with encryption training) or from insisting that we must proceed to encrypt everything we do. Making this clear offers an opportunity to open up the “black box” of online privacy and to take stock of our needs and knowledge together.

Fourth, this also means finding ways to mobilize around any departmental or institutional decisions that move access to and control of data into the hands of private forces without due consultation or considerations of viable alternatives. We thereby need to keep abreast of the negative consequences that are possible, what advantages and disadvantages these tools offer, and the short- and long-term implications they may have on our own work. As time-consuming as any changes in our logging-on and logging-off habits may be, as critical scholars, mentors, and educators, we have not only a legal but also an ethical responsibility toward those we engage with

and encounter. Conversely, departmental and institutional managers also need to be able to defend decisions to outsource, downgrade, or upgrade staffs' computing provisions. Statutory and voluntary programs for ensuring privacy and information security need to be developed in association with staff and students, and the time required to discuss these issues and implement these changes have to be factored in to the working and teaching week. It further demands that universities' IT departments need to become much more familiar with emerging jurisprudence around rights and freedoms online in globally networked settings.

Knowledge about these four dynamics and their relevance can contribute to inculcating better information-security practices in the higher education sector and to regain a sense of agency in this emerging *Internet governmentality* apparatus. Learning hands-on skills such as how to install or set up a particular encryption software is and should be part of our teaching and wider conversation as well as daily practice. Yet, we have yet to create constructive and supportive rather than punitive educational encounters, and our responses need to be diverse and adaptable.

Privacy may be a universal right, but it is not culturally absolute. Even within Western, liberal settings there needs to be space for robust debates and dissent within any proposed "training," for instance, around the broader human rights implications of local, institutional, and national policy decisions that affect how we access and use the Internet and our personal devices. Taking a cue from Feenberg (1999), as educators and researchers we need to consider the interrelationship between the normalization of online surveillance, concomitant developments in forms of digital/networked censorship, and citizens' responses through encryption as one form of resistance ad civil disobedience at the online-offline nexus. With this in mind, we may generate a momentum and the amount of energy required for a "renewal of agency in the technical sphere" (Feenberg 1999, 102).

To sum up, encryption is part of a larger whole in the debate on surveillance and censorship in academia. All of us need to make the first step in raising awareness at our own desktop, in our workplace, and in the classroom. Through these means, we may create spaces that ultimately lead to changes in altering passive mind-sets and fatalist attitudes that let private gatekeepers dictate the terms of access and use to our own scholarly imaginations, and those of others. And to achieve this, we should be reminded that like all human rights, those supporting academic freedoms, were hard won. Their legal and political sustainability remains fragile and under threat from 24/7 online surveillance.

## Surveillance and the Quantified Scholar: A Critique of Digital Academic Platforms

LUCAS MELGAÇO

*Vrije Universiteit Brussel*

DAVID LYON

*Queen's University*

The daily work of an academic today—whether professor, researcher, student, or other staff member—increasingly is mediated by digital platforms. Yet, while these platforms claim to, in different ways, increase scholars "efficiency" and "impact," in this essay we argue that they also increase the quantification of academic labor, the "microentrepreneurship of the self" (Hall 2016), and the presence of intrusive surveillance.

Three dystopian examples, two from popular media and one from a trendy academic digital platform, set the tone for our argumentation. In Dave Eggers's novel



*The Circle* (2013), Mae Holland, a new employee at a tech company, is welcomed with a score of 10,328: her participation ranking. Still low, she will be able to push it up through active engagement on social media. Her goal is to reach the “T2K,” the select group of the top 2,000 employees. In “Nosedive,” a *Black Mirror* episode, Lacie, a young and seemingly successful woman, is on her way to an interview for her dream apartment. She has a score of 4.2, awarded to her on social media following interactions she has had with people, posts she published, and positive comments she received. She can only be selected as a tenant if she manages to increase her rating to 4.5. On *ResearchGate*, we see David, senior professor, and Lucas, assistant professor, with scores of 27.08 and 13.48, respectively. David’s score is higher than 82.5 percent of *ResearchGate*’s members; Lucas’s 55 percent. Their ranking depends mainly on publications, citations, online interactions, and their quantity of followers. To many readers these examples may appear to be fiction. But for the more than 13 million scholars (according to *ResearchGate*’s claimed subscribers), the last case is a “reality” that they should presumably take seriously.

*ResearchGate* is only one of the many platforms that have become an integral part of university life. These range from multipurpose production platforms such as *Microsoft Office365*, to platforms that help students rank their professors (*Rate my Professors*, *Professor Performance*), assist teachers in their educational activities (e-learning platforms such as *Moodle*, *Canvas*, or *Brightspace*), or facilitate the job of administrative staff (*PeopleSoft*, *Banner ERP*). The use of many of these platforms is often unavoidable or mandatory as it might be the only means of communication offered by a specific institution.

Scholars may voluntarily engage with other platforms, not only because they are useful instruments that make academia more efficient, but also because they have become inherent to their identity within the higher education sector. Today, the virtual presence of scholars in cyberspace seems to be considered almost as important as their physical presence (Herrmann 2015). Additionally, the disclosure of their research and its visibility is comparable to their actual production. Publish or perish gives way to upload or perish. While for some this “digital performance” may be critical, for others the reasons for using these platforms is more prosaically practical: wishing to share their work and to be aware of others (Van Noorden 2014).

Publishing platforms are clearly not unique illustrations of the surveillance dimensions of contemporary universities (Dawson 2006; Lorenz 2012; Melgaço 2015). Obvious other examples include the proliferation of campus video systems; the use of badges, ID cards, and electronic keys (that generate an access log to labs and offices); as well as the increasing use of e-learning platforms (Edwards et al. 2018). Scholars such as Burrows (2012) and MacDonald (2017) have also highlighted the controlling aspect of academic audit procedures.

Yet, rather than focusing on how surveillant higher education has become, this essay examines the consequences and the impacts of this scholarly surveillance system. First, we discuss the banalization of digital platforms and argue that university surveillance is a typical example of both Zuboff’s (2015, 2019) “surveillance capitalism” and Lyon’s (2017, 2018) “surveillance culture.” Surveillance capitalism is an economic system that monetizes data acquired through surveillance. Surveillance culture is the product of everyday experience of and engagement with surveillance. Second, we look at platforms that are aimed at fostering networking and the visibility of academic publications. We discuss how they relate to visibility, scoring, and control. The essay concludes with a reflection on the potential alternatives to for-profit platforms and more broadly the future of a quantified academia. It also asks further questions to demonstrate why this is an area badly demanding thorough research and analyses.

### University Surveillance as Surveillance Capitalism and Surveillance Culture

In an age of surveillance capitalism, it is hardly surprising that universities would be implicated in the rampant quantification and scoring typical to social media and other platforms. Surveillance capitalism, according to Zuboff (2015, 2019), is constituted by “unexpected and often illegible mechanisms of extraction, commodification, and control that effectively exile persons from their own behavior while producing new markets of behavioral prediction and modification.” She argues that reliance on the electronic text helps create a new “division of learning,” a nexus of power common to all corporate entities today. The logic of accumulation organizes the field, defining “objectives, successes, failures, and problems” (Zuboff 2015, 77). It then determines what is measured and is passed over, as well as who is valued, and how resources are allocated.

Hall (2015) points out that despite the name *Academia.edu*—which sounds like a network created by academics—this site is constructed for corporate profit. As its founder and CEO Richard Price says, the goal is to provide “trending research data to R&D institutions that can improve the quality of their decisions by 10–20 percent” (Hall 2015). Hall (2016) further critiques that universities, such as the global taxi technology company Uber and the online hospitality service *Airbnb*, encourage everyone to become “microentrepreneurs of the self.” The latter describes exactly what the scholarly platforms represent. For Sterne, a professor who felt “obliged” to set up an *Academia.edu* account, the issue is rather the “gamification of research” in which scholarly progress is seen akin to *Facebook* “likes” or *Twitter* retweets (Wagman 2016).

From what little evidence exists, it appears that some scholars are concerned about the effects this “dataveillance” (Clarke 1988) has on their careers or about the possibility that these platforms may take unfair advantage of their information. Others, however, are content with the academic platforms and ask few questions about them. This is consistent with the use of social media in general: there is a gratitude for the affordances that these platforms offer and barely any serious concern about the negative consequences they create for users. Similarly, a critique of the limits of academic freedom or the power the university (or the companies that run such platforms) has over a scholar’s everyday life is essentially absent (Lyon 2018).

Even those aware of surveillance capitalism may in many cases surrender to surveillance culture. Indeed, the two authors of this essay both have profiles on *Academia.edu* and *ResearchGate* and are users of different for-profit productivity platforms. Fitzpatrick (2015) has something to add to this discussion:

The problem, of course, is that many of us face the same dilemma in our engagement with *Academia.edu* that we experience with *Facebook*. Just about everyone hates *Facebook* on some level: we hate its intrusiveness, the ways it tracks and mines and manipulates us, the degree to which it feels mandatory. But that mandatoriness works: those of us who hate *Facebook* and use it anyway do so because everyone we’re trying to connect with is there . . . I’ve heard many careful, thoughtful academics note that they’re sharing their work there because that’s where everybody is.

Despite their seductive aspect, one should bear in mind that all such platforms are created to make profit, especially from users who participate without pay. This monetizing potential is an example of surveillance capitalism at universities. At the same time, the familiarity of social media platforms and other aspects of digital life mean that their existence within the university seem less incongruous. Today, a culture of surveillance exists (Lyon 2017, 2018) within which many practices that may once have been eschewed by the academy are being normalized.

The major difficulties accompanying this development have yet to be fully researched, not least, because the algorithms underpinning these platforms are not publicly available. However, as seen with other social media, there is plenty of evidence that such platforms are addictive in character and unfair in outcomes. Due to their for-profit nature, incentives to join and return frequently are structurally built-in and created to stimulate the brain in specific ways (Alter 2017). Thus, what invites scholars into publishing platforms such as *ResearchGate* is the logic underpinning all social media: they seek exposure, affirmation, and prestige through the increase of their research score.

Additionally, the inequalities baked in to academic media need exploring in more depth. However, the very fact that “reputational” scores can be raised simply by interacting more frequently with the platform indicates fundamental flaws in fairness. Like university rankings themselves, such platforms may produce bizarre outcomes, ones that could disadvantage certain professors, just as some universities lose out (O’Neil 2016, chap. 3; Bigo in this forum).

Another aspect of academic platform usage is that the drive for “efficiency” may prompt more publishing but less interest in the quality of the content released. Of course, measurements such as the impact factor exist supposedly to raise quality over quantity. But the validity of measurements that only consider how *often* someone was cited is dubious when there is no indication of *why* this person was quoted. Also, books and other smaller publications (like newspaper articles or other more accessible texts directed to practitioners and the lay audience) are normally not included in this count. Thus, the surveilled university (or the surveilled publishing process) pushes scholars to produce outcomes in one specific way—that of alleged “impact,” with performance being everything.

### Publishing Platforms and the Search for Impact

Publishing platforms are networking tools that allow for the global connection of scholars and universities and serve as a display for academic production. They are not only virtual spaces for researchers to make their publications more visible, but also are comprised of other social media functions (Lupton et al. 2017). These include functionalities such as the announcement of events and job opportunities, the publishing of questionnaires and quizzes, and the direct chat between members.

Similar to other social networking sites, publishing platforms require that users create and feed their avatar with personal data. They are also comparable in their strategies to get users increasingly connected and engaged—hooked—by sending reminders and all sorts of notifications. Most importantly, they have very similar business models in which users do not pay for the service with cash but by donating their valuable personal (or academic) information. The focus is on the user and how they will benefit from increased interaction with the system, and not on the constant monitoring of users, let alone the algorithms that determine their “reputations.”

As far as scholars are concerned, the main purpose of such research platforms remains, nonetheless, in maximizing the so-called impact of academics’ publications. Through such sites, academics can monitor the performance of their publications by following how many views, downloads, and citations their publications generated. Both *Google Scholar* and *ResearchGate* go a step further and offer tools to quantify scholars’ production and “impact” by showing their h-index (an author metric based on the scholar’s most cited works and the number of citations they have received by peers). In possession of these scores, scholars can not only evaluate and self-surveil their own performance but also compare it to and monitor that of their peers.

Not satisfied with the h-index alone, *ResearchGate* also created the “RG Score.” It includes other variables beyond publications such as scholars’ engagement with

the platform (participation by asking questions or giving answers in the platform forums) or their popularity, which is calculated by the number of followers they have (Yu et al. 2016). According to the *ResearchGate* website, the “RG Score takes all your research and turns it into a source of reputation.” A scholar’s RG score is highly visible on the platform as it appears right after someone’s name (even before the person’s academic affiliation). It is a sort of digital business card that, according to the website, “[a]s an integral feature of ResearchGate, . . . can’t be turned off or hidden.” Such academic metrics are consequently not so different from the fictional cases of Mae and Lacie and their struggle with imposed scores mentioned at the start of this essay.

The criticism around the lack of transparency of the RG score (Kraker, Jordan, and Lex 2015) does not seem to prevent it being used in the course of job selection processes. As the site explains, once someone posts a new job ad, the platform will help with the sorting of candidates by displaying not only their publications, but also by ranking them based on quantifiable measures like the h-index and the RG score. Furthermore, it seems very plausible to infer that such scores have an impact not only on the way scholars are perceived by their peers, but also by the way scholars see themselves. Still, those suffering from what Clance and Imes (1978) named the *impostor phenomenon* could find some consolation by following *ResearchGate* tips on how to increase their result: “[s]hare anything from negative results to raw data or full-fledged publications; [c]reate a project, or add an update to your existing project(s); [a]sk a question or give another researcher a helpful answer; [f]ollow other researchers; [c]omment on and recommend your peer’s research, projects, and questions.” There is room to “game” the RG score.

Publishing platforms should be considered in their complexity. They are certainly a means of connecting with other like-minded scholars and of overcoming the limitations of distance in seeing where networks of similar scholarship emerge. They may also offer incentives to research and publish in particular areas and provide some sense of satisfaction in discovering that others are interested in one’s work. Yet, here again, we see the surveillance culture in operation. At the same time, these academic platforms may simply support the growing consensus of the corporate-style, metrics-driven university with its pressure to publish and its particular obsession with research that might make money through patents and business deals. And without the researchers in question even knowing about it, the platforms may already be profiting from the knowledge gained through prepublished information and that of cutting-edge research in some areas.

### Conclusion: Moving Forward

Surveillance at universities is a major issue in this era of surveillance capitalism and its corresponding surveillance culture. It involves many different aspects, actors, and types, with the focus of this essay having centered on the use of platforms in the higher education realm. The main reason for our reliance on these systems seems to be a strive for efficiency and impact, whether in regard to platforms for teaching, e-learning, publication, and project management, or simply the sharing of information. Current pressures for universities to increase their relevance, efficacy, and research outputs further intensifies this pursuit of quantification and the reliance on scores.

The currently available platforms are largely profit-making enterprises that encourage academics to market themselves as “microentrepreneurs” and are in their very nature highly surveillant. At the same time, as these platforms increase productivity and heighten the level of academic production, they can also overwhelm scholars with notifications and requests, incentivizing them to upload all sorts of data and reports.

The surveillance that occurs is organized by the companies that run these platforms. Their privileged access and overview allow them to sell information about “trending” research to other corporations. Users with access can merely “follow” what academics are doing. While these controlling processes are ambiguous, the situation could be improved if more transparency were offered and if opportunities were given for academics to help run these platforms democratically. Thus, a move to open access and alternative nonprofit platforms—which have been already proposed (Geltner 2015)—would definitely be welcomed.

Further research is also badly needed. For example, how do the scores that platforms such as *ResearchGate* attribute to scholars change the way they see themselves and the way their peers refer to them? Do the scores change the chances of someone getting a new position or being considered for a job interview? Given the relative lack of research in this area, it is difficult to come to firm conclusions. Nevertheless, it is clear that ambivalence about these new tools will continue as long as the platforms themselves remain uncommunicative about their business models and as long as academics see the perceived advantages without the likely downsides.

Within the university, the quest for research metrics are unabated and reflected in both internal rankings of scholars and the external rankings of universities both nationally and internationally. The existence of commercial academic platforms that echo such features simply serves to normalize such processes without necessarily raising questions about the quality of research thus created and promoted. Worryingly, academics themselves increasingly will be seen primarily in terms of their scores rather than in terms of other more qualitative factors. If this pattern continues, peer-review may give way to ranking systems less amenable to checking and verification, tending toward professor popularity and celebrity status.

What can be read about in fiction such as *The Circle* or watched in *Black Mirror* has now found its counterparts in university life. Performance and productivity become the keys to university teachers’ “success,” seen in constant feedback loops provided by systems such as *Google Scholar*, *ResearchGate*, or *Academia.edu*. This is the surveillance culture we face in higher education. Monetization and behavioral modification occur as the platform corporations scrape data donated by prestige-seeking academics, bringing profits to the companies and changing practices to scholars. This is the surveillance capitalism we are subjected to inside higher education.

However, not all is hopeless, considering that changes discussed above are at an early stage and not set in stone. Positive transformations may occur, given the potential promises also noted above. But these will require a deeper understanding of what is happening along with the determination to seek platform transparency and opportunities for faculty governance. At present, the here-mentioned systems are all-too-often merely reflecting the erosion of academic influence and reach within the university sector. However, they may well offer potential affordances and could be a starting point for genuine scholarly activities and improved teaching methods that, if organized imaginatively and democratically, could revitalize the university as a place for creative, independent, and critical thought and action.

## **Infrastructure and Protocols for Privacy-Aware Research**

BECKY KAZANSKY AND STEFANIA MILAN

*University of Amsterdam*

In 2014, a group of human rights defenders known as the “Zone 9 bloggers” was detained and later prosecuted in Ethiopia over their use of a learning resource on



privacy and digital security called “Security in a Box” (Amnesty International 2017). In 2017, a number of human rights defenders from organizations such as Amnesty International were imprisoned in Turkey for participating in training on information management. In both cases, individuals engaged in human rights work were faced with legal charges over teaching or learning how to encrypt communications, a practice considered increasingly essential by transnational civil society amid pervasive surveillance (Front Line Defenders 2017). This worrying development stretches beyond so-called high-risk contexts. In the last few years, we have seen an upsurge of “cryptowars,” and even countries with strong rule of law are questioning whether “ordinary” individuals should have the right to keep their communications confidential (Ball 2015).

As academics, we are not immune to these debates. Our own research tools and practices may be subject to monitoring and censorship, with various scholars warning about the increasing “securitization” of research (Tanczer 2016; Peter and Strazari 2017). Building on the earlier contributions to this forum, we therefore reflect on the challenges that derive from operating in an environment of pervasive “surveillance capitalism” (Zuboff 2015, 2019), where—at least potentially—“social science is police science,” as “it is never clear who is going to use” data generated through scientific research (Hintz and Milan 2010, 839). As the final essay in this forum, we explore a set of practices that may help academia to engage in responsible empirical research amid the surveillance and censorship processes our fellow coauthors have highlighted.

We draw on the insights gained from our research into the consequences of surveillance on democratic agency and citizen participation.<sup>1</sup> The many ways in which users seek to resist monitoring practices prompt researchers to carefully consider the ethics of engagement with “the field” and to treat ethics as an exercise that must be resilient over time and different geographies. This entails recursively interrogating and adopting routines and habits throughout the research cycle, considering factors such as risk assessment and mitigation, data protection and privacy, as well as data management and storage (Sluka 2018).

While our particular research interests may “force” us to actively consider privacy and security, we argue that any researcher working with human subjects must take this subject matter seriously. Our engagement with participants exposes them to vulnerabilities of various kinds—ranging from the datification and reification of their behavior to surveillance. Far from prescribing a formula for privacy-aware research, and much like Franklin in this forum, we invite scholars to adapt their infrastructure and practices to their respective contexts, expertise, resources, and needs.

Over the next pages, we offer our experience of examining actions by politically engaged people who are made vulnerable through the nature of their work and their technological dependencies, catalog some of the steps taken to set up our digital infrastructure and workflow to address privacy and security priorities, and reflect on the role of “engaged research” and the question of infrastructure in the neoliberal university (see the essays by Deibert and Bigo in this forum).

### Engaged Research as Situated, Context-Aware Research

Our point of departure is the questioning of the category “vulnerable subjects.” According to the European Commission, “[v]ulnerable categories of individuals” include “children, patients, people subject to discrimination, minorities, people unable to give consent, people of dissenting opinion, immigrant or minority

---

<sup>1</sup> Research for this essay was supported by a Starting Grant of the European Research Council awarded to Stefania Milan as Principal Investigator (StG-2014\_639379 DATACTIVE). We thank the DATACTIVE team for contributing to designing the infrastructure and protocols described here and the DATACTIVE Ethics Advisory Board for their feedback. Both authors have equally contributed to this article.

communities, sex workers, etc.” (European Commission Directorate-General for Research & Innovation 2016, 9). While political activists per se are not explicitly included in this definition, we argue that vulnerability is context-dependent. What might be a perfectly acceptable practice today might not be tomorrow. And what is allowed in a given country might not be in another. Think of encryption technologies: tools such as the instant messaging app *Telegram* are restricted in countries such as Russia and Iran (Deahl 2018), but usable—albeit sometimes under political scrutiny—in most Western democracies.

Due to this ambiguity around the consequences of our research and actions, we include all our participants without distinction into the “vulnerable subjects” category. This implies that we accept all the consequences this move entails—some of which have the power to slow down our analysis and add red tape to our work. It should also be said that, while the choice of the term “vulnerable” mirrors its use in data-protection language, it is not intended to minimize the agency and autonomy of the individuals and communities designated as such; instead, the classification is meant to help accord additional protections in response to long-standing inequalities and emergent risks.

To account for the sensitivity and awareness of time, geography, and context vis-à-vis the vulnerability of our subjects, our team adopts an “engaged” approach to research (Milan 2010, 2014). Thus, we carefully and continuously interrogate the impact that our empirical inquiry might have on the people and communities we study, while striving to indirectly contribute to their causes. Engaged research is therefore inherently *situated*. It brings the researchers to the same level of those being researched and anchors the research process to the evolving challenges of the field. This necessitates, for example, that we focus as much as possible on research questions that are relevant to both the researchers and the research subjects. We further seek appropriate opportunities for coinquiry, exchange, and collaboration and take great care with how we collect, handle, and present data about identities, projects, and networks.

Most importantly though, this engaged research dynamic alters the timeline of our commitment to ethics. This is specifically important for international relations and security studies scholars who often face serious ethical challenges in their practice (Baele et al. 2018). Research ethics is no longer merely a series of “box-ticking exercises” at the inception of a project, but become a permanent interrogation and an ongoing dialogue (Milan and Milan 2016). In this respect, engaged research is *context-aware*: on the one hand, it dialogues with and listens to the concerns of the field, while on the other hand, it is—by its own nature—dynamic and elastic, forcing academics to keep alert and to respond to novel challenges as they arise.

### The Question of Infrastructure

As discussed at length by our colleagues in this forum, universities have migrated their digital infrastructure, including email, learning systems, and shared drives to the platforms of major corporations that unilaterally set their terms of service. How can researchers respect the privacy of research subjects if, for instance, data is not securely stored?

For our research project, we devised a “secure” infrastructure and protocols for our work. Many of these practices echo and complement guidance provided by other scholars and institutions (Aldridge, Medina, and Ralphs 2010; Marwick et al. 2016; Tanczer et al. 2016; van Baalen 2018). To this end, the team engaged in a particular kind of *risk assessment*, working through a number of scenarios for how the life cycle of collection and dissemination of data might take place. This exercise allowed us to note points along the research process at which privacy and security concerns may arise and to discuss contingencies that could appear during fieldwork and travel. We evaluated our storage and communication needs and then assessed



possible *Free/Libre Open-Source Software* (FLOSS) tools that would meet them. FLOSS' openness and ability to respond to security threats made us consider it over proprietary competitors (Boulanger 2005).

The infrastructure for our research—including servers, mailboxes, and mailing lists—are now stored outside the university network with a local, privacy-aware provider. *OwnCloud*, an open-source alternative to commercial cloud services such as *Dropbox*, allows us to store data and files in a decentralized manner on our private server. Instead of industry-led collaborative writing platforms such as *Google Docs*, we set up a password-protected *etherpad*, whose contents are not retrievable by search engines. Using some of this infrastructure requires patience and dedication on our part, as the user interfaces are not as developed as those of their commercial counterparts. Yet, taking infrastructure seriously permits us to considerably reduce vulnerabilities and points of exposure.

### Devising Working Protocols for Engagement with the Field

But securing infrastructure alone—especially when its use is not immediately self-evident—is not sufficient enough to protect the privacy and security of our participants. Thus, we have collectively developed communication, fieldwork, and data-handling protocols and implemented an internal workflow requiring members to use encryption to communicate as well as to share and store data. These rules of conduct are applicable to IR scholars working empirically and can be implemented by individuals as well as members of a large research team.

#### *First Contact*

Our communication protocol outlines steps that can be taken for contacting research subjects. We offer participants a secure channel for communication contingent on their particular situation and needs, while always aiming for the option that exposes data the least. Due to the earlier-mentioned concerns over the use of encryption when planning correspondence with people from different regions, it is important to first research the legality of privacy-enhancing tools in any given context. Following this due diligence check, should the use of encryption technologies be available, then we seek initial contact using the open-source implementation of *Pretty Good Privacy* to encrypt our email. We consequently search for retrievable, publicly broadcasted encryption keys, which often can be found on personal websites or on so-called “Public Key Servers.” The latter is a database where individuals can upload their public key and equals a searchable phonebook.

When such a key is not available, the team attaches their own encryption key to the message. We invite and encourage participants to make use of secure communication technologies and also offer to move the discussion to alternate communication channels such as a secure FLOSS-messaging application (*Signal*) or an online video-calling system (*Jit.si*, *TOX*). When an email needs to be sent “in clear”—meaning unencrypted—we leave out details such as travel information, location, and meeting time. Such sensitive information is only communicated over secure channels. This specifically applies for sites other than large conferences, such as meetings with organizations and informal gatherings.

#### *Travel*

Academics also must pay attention to the security of their data and communications when travelling. We, thus, ask researchers to pay close attention any time their laptops, mobile phones, or recording devices are moved to a different location. We operate on the premise that data is not physically transported across borders but is backed up to an encrypted server prior to the start of a journey. Under particular

circumstances, scholars may even choose to travel with a different, newly configured device.

#### *Data Anonymization*

Data collected for research purposes tends to “proliferate” (Aldridge et al. 2010, 3), amplifying the vulnerabilities for research subjects. To counter this spread of data across different devices, individuals, and physical locations, the team addresses issues around privacy, anonymity, and deidentification of research subjects from the beginning of the research process all the way to publication. As soon as interviews are completed, data is backed up and stored encrypted and so are transcripts. Full anonymization is ensured by a code system; interviewee names are securely stored in an analogue manner and presided over by the principal investigator. Avoiding reidentification goes beyond simply taking the names out of a dataset. Rather, it means anticipating how the aggregation of specific details may give away the identity of research subjects even when names are not mentioned explicitly or solely quantitative data is reported (Goroff 2015). This is particularly important when a study’s underlying research data is made publicly available (G. Alter and Gonzalez 2018).

#### *Open-ended Debriefing*

Following fieldwork and travel, the team also reflects on the experiences and challenges with these protocols, allowing for modifications to be made. This process continues throughout the data analysis phase up to the completion of the project, allowing us to abide to our engaged research approach.

### **Protocols in Practice**

A fundamental caveat is that the here-mentioned tools are a secondary consideration to the research protocols we implement. Like Tanczer et al. (2016, 351) have previously emphasized, as technology changes, “instruments, practices, and procedures have to adapt.” Continuous diligence is required to respond to their shifting utility and security settings. This also means staying abreast of technological developments and continuously updating our software and infrastructure providers. We thereby rely on the latest recommendations of digital rights organizations such as the Electronic Frontier Foundation’s *Surveillance Self-Defense* tool or Tactical Technology Collective’s *Security in a Box*.

Of course, many of the available encryption tools continue to be difficult to use and oftentimes attract controversy among security experts over their relative merits (Schneier, Seidel, and Vijayakumar 2016). As indicated by digital rights organizations as well as by our own research (Kazansky 2015, 2016), privacy-aware instruments should be selected by weighing the contextual details against the skill level and requirements of researchers and participants. A priority is placed on well-maintained and vetted FLOSS. Thus, we abstain from presenting our protocols as “hard and fast” rules. Research is by its very own nature messy, with such processes also calling for continuous renegotiation.

Academics should also anticipate that some participants might not be familiar with many of the encryption systems or find them inappropriate or even unsafe in their context. Our own experiences with more than 200 informants to date teach us that using encryption tools entails navigating different comfort levels, requirements, and workflows. While many informants have responded with encrypted emails, a significant number of informants have not. Some have instead responded back through commercial platforms or secure messaging services. However, we do not want to read these results too pessimistically: ambivalence around the use of encryption tools is well-documented (Whitten and Tygar 2005) and may also be attributable to the nature of correspondence as interlocutors might not always have

their encryption keys on hand (e.g., when using a smartphone). Indeed, it may not even be a matter of literacy or expertise, for even preeminent security experts do not use reliably the tools they invented (Franceschi-Bicchierai 2015).

### Conclusion: Moving Forward

Hence, finding the balance between the mechanics of data collection and analysis as well as the imperative to protect participants from monitoring and repression is tricky. While our team studies a realm of social action that by its own nature exposes politically engaged individuals to vulnerabilities of various kinds, we believe it rests upon the entire research community to find ways in which academia can be mindful of the increasing risks to our research subjects.

To conclude, we want to emphasize three takeaways in the hope that the higher education sector will change its practices and include some “digital hygiene” measures in its research toolbox. First, although it might take some time to amend established ways of organizing research and fieldwork, digital security and privacy concerns and potential solutions should be an essential concern for all institutional review boards. Advocating for institutional changes to create the necessary conditions, including funding, to engage in “secure” research will therefore be an important step. Second, there is no single best protocol for protecting research from censorship or surveillance. Processes and tools have to be integrated into our routines and will always be dependent upon contingent priorities and constraints—whether institutional, financial, temporal, or a lack of expertise. However, and third, the lack of resources and expertise are not necessarily barriers. Many solutions are not “high-tech”; for instance, preferring privacy-respecting services such as email providers or collecting and storing data purely offline are valid, low-tech measures accessible to anyone. Thus, the choice to secure our subjects data is ours, and many academics already are actively making this choice.

### References

- ABBATE, JANET. 1999. *Inventing the Internet*. Inside Technology. Cambridge, MA: MIT Press.
- 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: 3–9.
- ALIM, FRIDA, NATE CARDOZO, GENNIE GEBHART, KAREN GULLO, AND AMUL KALLIA. 2017. “Spying on Students: School Issued-Devices and Student Privacy.” San Francisco: Electronic Frontier Foundation. Accessed August 8, 2019. <https://www.eff.org/files/2017/04/13/student-privacy-report.pdf>.
- ALTBACH, PHILIP G. 2008. “The Imperial Tongue: English As the Dominating Academic Language.” *International Educator* 17: 56.
- ALTER, ADAM. 2017. *Irresistible: The Rise of Addictive Technology and the Business of Keeping Us Hooked*. New York: Random House.
- ALTER, GEORGE, AND RICHARD GONZALEZ. 2018. “Responsible Practices for Data Sharing.” *American Psychologist* 73: 146–56.
- AMNESTY INTERNATIONAL. 2017. “Ethiopia: Fresh Trial for Two Zone-9 Bloggers Flies in the Face of Justice.” *Amnesty International*, April 6. Accessed August 8, 2019. <https://www.amnesty.org/en/press-releases/2017/04/ethiopia-fresh-trial-for-two-zone-9-bloggers-flies-in-the-face-of-justice/>.
- ANONYMOUS. 2017. “State Vs. Academy: The Academy Under Surveillance.” *Surveillance & Society* 15: 550–56.
- BACHAN, RAY. 2017. “Grade Inflation in UK Higher Education.” *Studies in Higher Education* 42: 1580–600.
- BAELE, STEPHANE J., DAVID LEWIS, ANKE HOFFLER, OLIVIER C. STERCK, AND THIBAUT SLINGENEYER. 2018. “The Ethics of Security Research: An Ethics Framework for Contemporary Security Studies.” *International Studies Perspectives* 19: 105–27.
- BALL, JAMES. 2015. “Cameron Wants to Ban Encryption – He Can Say Goodbye to Digital Britain.” *Guardian*, January 13. Accessed August 8, 2019. <https://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror>.
- BBC NEWS. 2018a. “US Sanctions Iranian Hackers for ‘Stealing University Data.’” *BBC News*, March 23. Accessed August 8, 2019. <http://www.bbc.com/news/world-us-canada-43519437>.

- . 2018b. “Matthew Hedges: British Academic Pardoned By UAE.” *BBC News*, November 26. Accessed August 8, 2019. <https://www.bbc.com/news/uk-46341310>.
- BENNETT, LIZ. 2017. “Social Media, Academics’ Identity Work, and the Good Teacher.” *International Journal for Academic Development* 22: 245–56.
- BENTLEY, MICHELLE. 2018. “Enough Is Enough: The UK Prevent Strategy and Normative Invalidation.” *European Journal of International Security* 3: 326–43.
- BODO, BALÁZS, NATALI HELBERGER, KRISTINA IRION, FREDERIK ZUIDERVEEN BORGESUIS, JUDITH MOLLER, BOB VAN DE VELDE, NADINE BOL, BRAM VAN ESS, AND CLAES DE VREESE. 2017. “Tackling the Algorithmic Control Crisis—the Technical, Legal, and Ethical Challenges of Research Into Algorithmic Agents.” *Yale Journal of Law and Technology* 19: 133–80.
- BOHAKER, HEIDI, LISA AUSTIN, ANDREW CLEMENT, AND STEPHANIE PERRIN. 2015. “Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World.” Toronto: University of Toronto. Accessed August 13, 2019. <https://tspace.library.utoronto.ca/handle/1807/73096>.
- BOULANGER, AYMEN. 2005. “Open-Source Versus Proprietary Software: Is One More Reliable and Secure than the Other?” *IBM Systems Journal* 44: 239–48.
- BOURDIEU, PIERRE. 1988. *Homo Academicus*. Translated by Peter Besselaar. Cambridge: Polity Press.
- BOYD, DANAH, AND KATE CRAWFORD. 2011. “Six Provocations for Big Data.” In *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, 1–17. Oxford: Oxford Internet Institute. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1926431](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431).
- BRADY, ANNE-MARIE. 2017. “Magic Weapons: China’s Political Influence Activities Under Xi Jinping.” Woodrow Wilson Center. Accessed August 8, 2019. <https://www.wilsoncenter.org/article/magic-weapons-chinas-political-influence-activities-under-xi-jinping>.
- BRUNTON, FINN, AND HELEN NISSENBAUM. 2015. *Obfuscation: A User’s Guide for Privacy and Protest*. Cambridge, MA: MIT Press.
- BURROWS, ROGER. 2012. “Living with the H-Index? Metric Assemblages in the Contemporary Academy.” *Sociological Review* 60: 355–72.
- CHANGCHIT, CHULEEPORN. 2017. “Interview with Lionel Cassin. Information Security Officer, Texas A&M University-Corpus Christi on Security and Privacy Issues Facing the University.” *Journal of Information Privacy and Security* 13: 97–98.
- CHUBB, JENNIFER, AND RICHARD WATERMEYER. 2017. “Artifice or Integrity in the Marketization of Research Impact? Investigating the Moral Economy of (Pathways To) Impact Statements within Research Funding Proposals in the UK and Australia.” *Studies in Higher Education* 42: 2360–72.
- CHUH, KANDICE. 2018. “Pedagogies of Dissent.” *American Quarterly* 70: 155–72.
- CICCARIELLO-MAHER, GEORGE. 2017. “After December 31st, 2017, I Will No Longer Work At Drexel University.” *Twitter* (blog). December 28. Accessed August 13, 2019. <https://twitter.com/ciccmaher/status/946435825755148288>.
- CITIZEN LAB. 2014. “Communities @ Risk: Targeted Digital Threats Against Civil Society.” Citizen Lab. Accessed August 13, 2019. <https://targetedthreats.net/>.
- CLANCE, PAULINE ROSE, AND SUZANNE IMES. 1978. “The Imposter Phenomenon in High Achieving Women: Dynamics and Therapeutic Intervention.” *Psychotherapy Theory, Research, and Practice* 15: 241–47.
- CLARKE, ROGER. 1988. “Information Technology and Dataveillance.” *Communications of the ACM* 31: 498–512.
- COUREA, ELENI. 2018. “University Alerts Students to Danger of Leftwing Essay.” *Observer*, November 11. Accessed August 8, 2019. <https://www.theguardian.com/education/2018/nov/11/reading-university-warns-danger-left-wing-essay>.
- CRAM, IAN, AND HELEN FENWICK. 2018. “Protecting Free Speech and Academic Freedom in Universities.” *Modern Law Review* 81: 825–73.
- CRETE-NISHIHATA, MASASHI, JEFFREY KNOCKEL, BLAKE MILLER, JASON Q. NG, LOTUS RUAN, LOKMAN TSUI, AND RUOHAN XIONG. 2017. “Remembering Liu Xiaobo: Analyzing Censorship of the Death of Liu Xiaobo on WeChat and Weibo.” Citizen Lab. Accessed August 13, 2019. <https://citizenlab.ca/2017/07/analyzing-censorship-of-the-death-of-liu-xiaobo-on-wechat-and-weibo/>.
- DADA, TINUOLA, AND PETER MICEK. 2017. “Launching STOP: The #KeepItOn Internet Shutdown Tracker.” *Access Now*, September 7. Accessed August 8, 2019. <https://www.accessnow.org/keepiton-shutdown-tracker/>.
- DAWSON, SHANE. 2006. “The Impact of Institutional Surveillance Technologies on Student Behaviour.” *Surveillance & Society* 4: 69–84.
- DEAHL, DAN. 2018. “Iran Has Banned Telegram After Claiming the App Encourages ‘Armed Uprisings.’” *Verge*, May 1. Accessed August 8, 2019. <https://www.theverge.com/2018/5/1/17306792/telegram-banned-iran-encrypted-messaging-app-russia>.

- DEIBERT, RONALD J. 1998. "Virtual Resources: International Relations Research Resources on the Web." *International Organization* 52: 211–21.
- . 2013. *Black Code: Inside the Battle for Cyberspace*. Toronto: Random House.
- . 2015. "Authoritarianism Goes Global: Cyberspace Under Siege." *Journal of Democracy* 26: 64–78.
- DEIBERT, RONALD J., JOHN PALFREY, RAFAEL ROHOZINSKI, AND JONATHAN ZITTRAIN. 2008. *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.
- DEZALAY, YVES, AND BRYANT G. GARTH. 2002. *The Internationalization of Palace Wars: Lawyers, Economists, and the Contest to Transform Latin American States*. Chicago: University of Chicago Press.
- DIJK, JOSE VAN. 2014. "Datafication, Dataism, and Dataveillance: Big Data Between Scientific Paradigm and Ideology." *Surveillance & Society* 12: 197–208.
- DUKALSKIS, ALEXANDER. 2018. "The Chinese Communist Party Has Growing Sway in Western Universities." Democratic Audit UK, January 4. Accessed August 13, 2019. <http://www.democraticaudit.com/2018/01/04/the-chinese-communist-party-has-growing-sway-in-western-universities/>.
- DUNCAN, JANE. 2018. "Criminalising Academia: The Protection of State Information Bill and Academic Freedom." *Communication* 44: 107–29.
- EDWARDS, LILIAN, LAURA MARTIN, AND TRISTAN HENDERSON. 2018. "Employee Surveillance: The Road to Surveillance Is Paved with Good Intentions." APC 2018, 1–30. Accessed August 13, 2019. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3234382](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3234382).
- ELSE, HOLLY. 2017. "CUP Row 'Shows Need for New Approach to Chinese Censors.'" *Times Higher Education (THE)*, August 21. Accessed August 13, 2019. <https://www.timeshighereducation.com/news/cup-row-shows-need-for-new-to-approach-chinese-censors>.
- ENYEDI, ZSOLT. 2018. "Democratic Backsliding and Academic Freedom in Hungary." *Perspectives on Politics* 16: 1067–74.
- EPSTEIN, ROBERT, AND RONALD E. ROBERTSON. 2015. "The Search Engine Manipulation Effect (SEME) and Its Possible Impact on the Outcomes of Elections." *Proceedings of the National Academy of Sciences* 112: E4512–21.
- ERGÜL, HAKAN, AND SIMTEN COŞAR, eds. 2017. *Universities in the Neoliberal Era: Academic Cultures and Critical Perspectives*. London: Palgrave Macmillan.
- ERKKILÄ, TERO, ed. 2013. *Global University Rankings Challenges for European Higher Education*. Basingstoke: Palgrave Macmillan.
- EUROPEAN COMMISSION DIRECTORATE-GENERAL FOR RESEARCH & INNOVATION. 2016. "H2020 Programme Guidance: How to Complete Your Ethics Self-Assessment." European Commissions. Accessed August 13, 2019. [http://ec.europa.eu/research/participants/data/ref/h2020/grants\\_manual/hi/ethics/h2020\\_hi\\_ethics-self-assess\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf).
- FALK, RICHARD. 2007. "Academic Freedom Under Siege." *International Studies Perspectives* 8: 369–75.
- FATTAH, RANDA ABDEL. 2018. "How a Sri Lankan Student's Arrest on Terror Charges Exposes a System Built to Suspect Minorities." *Conversation*, November 9. Accessed August 13, 2019. <https://theconversation.com/how-a-sri-lankan-students-arrest-on-terror-charges-exposes-a-system-built-to-suspect-minorities-106613>.
- FEENBERG, ANDREW. 1999. *Questioning Technology*. London; New York: Routledge.
- FITZPATRICK, KATHLEEN. 2015. "Academia, Not Edu." Last modified October 26, 2015. Accessed August 13, 2019. <https://kfitz.info/academia-not-edu/>.
- FLAVIN, MICHAEL. 2016. "Home and Away: The Use of Institutional and Non-Institutional Technologies to Support Learning and Teaching." *Interactive Learning Environments* 24: 1665–73.
- FLYVERBOM, MIKKEL, RONALD J. DEIBERT, AND DIRK MATTEN. 2017. "The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business." *Business & Society*, August: 1–17.
- FOUCAULT, M. 1977. *Discipline and Punish*. London: Tavistock.
- FRANCESCHI-BICCHIERAI, LORENZO. 2015. "Even the Inventor of PGP Doesn't Use PGP." *Motherboard*, September 2. Accessed August 13, 2019. [https://motherboard.vice.com/en\\_us/article/vbw9a/even-the-inventor-of-pgp-doesnt-use-pgp](https://motherboard.vice.com/en_us/article/vbw9a/even-the-inventor-of-pgp-doesnt-use-pgp).
- FRANKLIN, M.I. 2013. *Digital Dilemmas: Power, Resistance, and the Internet*. Oxford: Oxford University Press.
- FRONT LINE DEFENDERS. 2017. "Free Human Rights Defenders Detained in Turkey." *Front Line Defenders*, July 12. Accessed August 13, 2019. <https://www.frontlinedefenders.org/en/free-human-rights-defenders-detained-turkey>.
- GALPIN, CHARLOTTE. 2018. "Video Must Not Kill the Female Stars of Academic Debate." *Times Higher Education (THE)*, November 8. Accessed August 13, 2019. <https://www.timeshighereducation.com/opinion/video-must-not-kill-female-stars-academic-debate>.
- GELTNER, G. 2015. "Upon Leaving Academia.edu." *Mittelalter: Interdisziplinäre Forschung und Rezeptionsgeschichte*, December 7. Accessed August 13, 2019. <https://mittelalter.hypotheses.org/7123>.



- GILMORE, JOANNA. 2017. "Teaching Terrorism: The Impact of the Counter-Terrorism and Security Act 2015 on Academic Freedom." *Law Teacher* 51: 515–24.
- GIROUX, HENRY A. 2013. "Public Intellectuals Against the Neoliberal University." *Truthout*, October 29. Accessed August 13, 2019. <https://truthout.org/articles/public-intellecutuals-against-the-neoliberal-university/>.
- GOROFF, DANIEL L. 2015. "Balancing Privacy Versus Accuracy in Research Protocols." *Science* 347: 479.
- HALL, GARY. 2015. "Does Academia.Edu Mean Open Access Is Becoming Irrelevant?" Last modified October 18, 2015. Accessed August 13, 2019. <http://www.garyhall.info/journal/2015/10/18/does-academiaedu-mean-open-access-is-becoming-irrelevant.html>.
- . 2016. *The Uberfication of the University*. Minneapolis: University of Minnesota Press.
- HAMATI-ATAYA, INANNA. 2011. "Contemporary 'Dissidence' in American IR: The New Structure of Anti-Mainstream Scholarship?" *International Studies Perspectives* 12: 362–98.
- HASKINS, ANNA R., AND WADE C. JACOBSEN. 2017. "Schools As Surveilling Institutions? Paternal Incarceration, System Avoidance, and Parental Involvement in Schooling." *American Sociological Review* 82: 657–84.
- HEROLD, BENJAMIN. 2018. "How (and Why) Ed-Tech Companies Are Tracking Students' Feelings - Education Week." *Education Week*, June 20. Accessed August 13, 2019. <https://www.edweek.org/ew/articles/2018/06/12/how-and-why-ed-tech-companies-are-tracking.html>.
- HERRMANN, RACHEL. 2015. "Why Your Department Needs Social Media." *Chronicle of Higher Education*. August 31. Accessed August 13, 2019. <https://www.chronicle.com/article/Why-Your-Department-Needs/232759>.
- HINTZ, ARNE, AND STEFANIA MILAN. 2010. "'Social Science Is Police Science.' Researching Grassroots Activism." *International Journal of Communication* 4: 837–344.
- HOPE, ANDREW. 2018. "Creep: The Growing Surveillance of Students' Online Activities." *Education and Society* 36: 55–72.
- INTERNET RIGHTS AND PRINCIPLES COALITION. 2018. "The Charter of Human Rights and Principles for the Internet" 6th Edition, Accessed August 13, 2019. [internetrighsandprinciples.org/site/wp-content/uploads/2019/09/IRP\\_booklet\\_Eng\\_6ed\\_4Nov2018.pdf](http://internetrighsandprinciples.org/site/wp-content/uploads/2019/09/IRP_booklet_Eng_6ed_4Nov2018.pdf).
- JESSOP, BOB. 2018. "On Academic Capitalism." *Critical Policy Studies* 12: 104–9.
- KAELIN, MARK. 2017. "Microsoft Office 365: The Smart Person's Guide." *TechRepublic*, May 31. Accessed August 13, 2019. <https://www.techrepublic.com/article/microsoft-office-365-the-smart-persons-guide/>.
- KAUPPI, NILO, AND TERO ERKKILÄ. 2011. "The Struggle Over Global Higher Education: Actors, Institutions, and Practices." *International Political Sociology* 5: 314–26.
- KAZANSKY, BECKY. 2015. "Privacy, Responsibility, and Human Rights Activism." *Fibreculture Journal* 26: 189–207.
- . 2016. "Digital Security in Context: Learning How Human Rights Defenders Adopt Digital Security Practices." *Tactical Technology Collective*. Accessed August 13, 2019. <https://secresearch.tacticaltech.org/digital-security-in-context-learning-how-human-rights-defenders-adopt-digital-security-practices.html>.
- KOZIOL, MICHAEL. 2018. "'National Interest Test' to Align Research with Security and Strategic Priorities." *Sydney Morning Herald*, November 10. Accessed August 13, 2019. <https://www.smh.com.au/politics/federal/national-interest-test-to-align-research-with-security-and-strategic-priorities-20181110-p50f89.html>.
- KRAKER, PETER, KATY JORDAN, AND ELIZABETH LEX. 2015. "The ResearchGate Score: A Good Example of a Bad Metric." *LSE Impact Blog*, December 9. Accessed August 13, 2019. <http://blogs.lse.ac.uk/impactofsocialsciences/2015/12/09/the-researchgate-score-a-good-example-of-a-bad-metric/>.
- LENOIR, REMI. 2006. "Scientific Habitus: Pierre Bourdieu and the Collective Intellectual." *Theory, Culture & Society* 23: 25–43.
- LIANG, FAN, VISHNUPRIYA DAS, NADIYA KOSTYUK, AND MUZAMMIL M. HUSSAIN. 2018. "Constructing a Data-Driven Society: China's Social Credit System As a State Surveillance Infrastructure." *Policy & Internet* 10: 415–53.
- LORENZ, CHRIS. 2012. "If You're So Smart, Why Are You Under Surveillance? Universities, Neoliberalism, and New Public Management." *Critical Inquiry* 38: 599–629.
- LUPTON, DEBORAH, INGER MEWBURN, AND PAT THOMSON. 2017. "The Digital Academic: Identities, Contexts and Politics." In *The Digital Academic: Critical Perspectives on Digital Technologies in Higher Education*, edited by Deborah Lupton, Inger Mewburn and Pat Thomson, 1–19. Abingdon: Routledge.
- LYON, DAVID. 2017. "Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity." *International Journal of Communication* 11: 824–42.
- . 2018. *The Culture of Surveillance: Watching as a Way of Life*. Cambridge, MA: Polity Press.

- MACDONALD, ROBERT. 2017. "‘Impact,’ Research and Slaying Zombies: The Pressures and Possibilities of the REF." *Journal of Sociology and Social Policy* 37: 696–710.
- MARWICK, ALICE E, LINDSAY BLACKWELL, AND KATHERINE LO. 2016. "Best Practices for Conducting Risky Research and Protecting Yourself from Online Harassment." Data & Society Research Institute. Accessed August 13, 2019. [https://datasociety.net/pubs/res/Best\\_Practices\\_for\\_Conducting\\_Risky\\_Research-Oct-2016.pdf](https://datasociety.net/pubs/res/Best_Practices_for_Conducting_Risky_Research-Oct-2016.pdf).
- MARX, GARY T. 1988. *Undercover: Police Surveillance in America*. Berkeley: University of California Press.
- . 2006. "Mots Et Mondes De Surveillance, Contrôle Et Contre-Contrôle à L’ère Informatique." *Criminologie* 39: 43–62.
- MELGAÇO, LUCAS. 2015. "Multiple Surveillance on the Digitized Campus." *Radical Pedagogy* 12: 27–51.
- MILAN, CHIARA, AND STEFANIA MILAN. 2016. "Involving Communities As Skilled Learners: The STRAP Framework." In *Methodological Reflections on Researching Communication and Social Change*, edited by Norbert Wildermuth and Teke Ngomba, 9–28. Basingstoke: Palgrave Macmillan.
- MILAN, STEFANIA. 2010. "Towards an Epistemology of Engaged Research." *International Journal of Communication* 4: 856–58.
- . 2014. "The Ethics of Social Movement Research." In *Methodological Practices in Social Movement Research*, edited by Donatella della Porta, 446–64. Oxford: Oxford University Press.
- MILLS, KURT. 2002. "Cybernations: Identity, Self-Determination, Democracy, and the ‘Internet Effect’ in the Emerging Information Order." *Global Society* 16: 69–87.
- MITTELMAN, JAMES H. 2007. "Who Governs Academic Freedom in International Studies?" *International Studies Perspectives* 8: 358–68.
- MUHAMAD, WARDANI, NOVIANTO BUDI KURNIAWAN, SUHARDI, AND SETIADI YAZID. 2017. "Smart Campus Features, Technologies, and Applications: A Systematic Literature Review." In *2017 International Conference on Information Technology Systems and Innovation*, 384–91. Bandung: IEEE.
- NAMER, YUDIT, AND OLIVER RAZUM. 2018. "Academic Freedom Needs Active Support." *Lancet* 392: 556.
- NECESSARY AND PROPORTIONATE CAMPAIGN. 2014. "International Principles on the Application of Human Rights to Communications Surveillance." *Necessary and Proportionate*, May 2014. Accessed August 13, 2019. <https://necessaryandproportionate.org/>.
- OLUKOTUN, DEJI. 2017. "We Need to Stop Shutting Down the Internet for School Exams." *Access Now*, May 16. Accessed August 13, 2019. <https://www.accessnow.org/need-stop-shutting-internet-school-exams/>.
- O’NEIL, CATHY. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Broadway Book.
- OWENS, BRIAN. 2017. "Cybersecurity for the Travelling Scientist." *Nature News* 548: 123.
- PEISERT, SEAN, AND VON WELCH. 2017. "The Open Science Cyber Risk Profile: The Rosetta Stone for Open Science and Cybersecurity." *IEEE Security Privacy* 15: 94–95.
- PENNEY, JON. 2016. "Chilling Effects: Online Surveillance and Wikipedia Use." *Berkeley Technology Law Journal* 31: 1–58.
- PERRINO, NICO. 2013. "Universities: Where You Go to Learn – and Be Monitored | Nico Perrino." *Guardian*, October 22. Accessed August 13, 2019. <https://www.theguardian.com/commentisfree/2013/oct/22/online-social-media-surveillance-university-campuses>.
- PETER, MATEJA, AND FRANCESCO STRAZZARI. 2017. "Securitisation of Research: Fieldwork Under New Restrictions in Darfur and Mali." *Third World Quarterly* 38: 1531–50.
- PILLAY, NAVI. 2014. "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights." A/HRC/27/37. Geneva: Human Rights Council.
- REDMOND, TONY. 2014. "Office 365 By the Numbers - an Ever-Increasing Trajectory." *IT Pro*, July 31. Accessed August 13, 2019. <https://www.itprotoday.com/office-365/office-365-numbers-ever-increasing-trajectory>.
- REEDER, ROBERT W., IULIA ION, AND SUNNY CONSOLVO. 2017. "152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users." *IEEE Security Privacy* 15: 55–64.
- RUTH, DAMIAN, SUZE WILSON, OZAN ALAKAVUKLAR, AND ANDREW DICKSON. 2018. "Anxious Academics: Talking Back to the Audit Culture Through Collegial, Critical and Creative Autoethnography." *Culture and Organization* 24: 154–70.
- SCHNEIER, BRUCE, KATHLEEN SEIDEL, AND SARANYA VIJAYAKUMAR. 2016. "A Worldwide Survey of Encryption Products (February 11, 2016). Berkman Center Research Publication No. 2016-2." Berkman Center Research. Accessed August, 13, 2019. <https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf>.
- SCHOLARS AT RISK NETWORK. 2017. "Academic Freedom Media Review Archive." Scholars at Risk. Accessed August 13, 2019. <https://www.scholarsatrisk.org/academic-freedom-media-review-archive-2017/>.
- SCOTT-RAILTON, JOHN. 2016. "Security for the High-Risk User: Separate and Unequal." *IEEE Security & Privacy* 14: 79–87.



- SERRES, MICHEL. 2007. *The Parasite*. Minneapolis: University of Minnesota Press.
- SLUKA, JEFFREY ALAN. 2018. "Too Dangerous for Fieldwork? The Challenge of Institutional Risk-Management in Primary Research on Conflict, Violence, and 'Terrorism.'" *Contemporary Social Science* 1–17. DOI: 10.1080/21582041.2018.1498534.
- SOLOON, OLIVIA. 2017. "Google Spends Millions on Academic Research to Influence Opinion, Says Watchdog." *Guardian*, July 13. <https://www.theguardian.com/technology/2017/jul/13/google-millions-academic-research-influence-opinion>.
- SPILLER, KEITH, IMRAN AWAN, AND ANDREW WHITING. 2018. "'What Does Terrorism Look Like?' University Lecturers' Interpretations of Their Prevent Duties and Tackling Extremism in UK Universities." *Critical Studies on Terrorism* 11: 130–50.
- STATISTICA. 2018. "Data Volume of Global Consumer Web Usage, e-Mails and Data Traffic from 2016 to 2021." Statista. Accessed August 13, 2019. <https://statinvestor.com/data/35224/global-e-mail-and-web-traffic/>.
- TANCZER, LEONIE MARIA. 2016. "The 'Snooper's Charter' is a Threat to Academic Freedom." *Guardian*, December 1. Accessed August 13, 2019. <https://www.theguardian.com/higher-education-network/2016/dec/01/the-snoopers-charter-is-a-threat-to-academic-freedom>.
- . 2017. "Digital Skills in Academia: Let's CryptoParty!" *OpenDemocracy*, April 6. Accessed August 13, 2019. <https://www.opendemocracy.net/leonie-tanczer/digital-skills-in-academia-let-s-cryptoparty>.
- TANCZER, LEONIE MARIA, RYAN McCONVILLE, AND PETER MAYNARD. 2016. "Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics." *Journal of Global Security Studies* 1: 346–55.
- GUARDIAN. 2018. "We Deplore This Attack on Freedom of Expression in Brazil's Universities." *Guardian*, November 1. Accessed August 13, 2019. <https://www.theguardian.com/world/2018/nov/01/we-declare-this-attack-on-freedom-of-expression-in-brazils-universities>.
- RADICATI GROUP. 2015. "Email Statistics Report 2015–2019." Radicati Group. Accessed August 13, 2019. <https://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf>.
- UNIVERSITY AND COLLEGE UNION. 2013. "Do I Have to Tell My Employer That I Am Taking Strike Action?" UCU, October 24. Accessed August 13, 2019. <https://www.ucu.org.uk/article/5299/Do-I-have-to-tell-my-employer-that-I-am-taking-strike-action>.
- VAN BAALLEN, SEBASTIAN. 2018. "'Google Wants to Know Your Location': The Ethical Challenges of Fieldwork in the Digital Age." *Research Ethics* 24: 1–17.
- VAN DER SLOOT, BART. 2017. "Als Wetenschapper Op 'goed Gesprek' Bij De AIVD: Mag Het Een Tandje Professioneler?" *De Volkskrant*, August 29. Accessed August 13, 2019. <https://www.volkskrant.nl/gs-bbb7d87a>.
- VAN NOORDEN, RICHARD. 2014. "Online Collaboration: Scientists and the Social Network." *Nature* 512: 126.
- WAGMAN, SHAWNA. 2016. "Some Academics Remain Skeptical of Academia.Edu." *University Affairs* (blog), April 12. Accessed August 13, 2019. <https://www.universityaffairs.ca/news/news-article/some-academics-remain-skeptical-of-academia-edu/>.
- WHITE, SCOTT G. 2008. "Academia, Surveillance, and the FBI: A Short History." *Surveillance and Governance: Crime Control and Beyond* 10: 151–74.
- WHITTEN, ALMA, AND J.D. TYGAR. 2005. "Why Johnny Can't Encrypt. A Usability Evaluation of PGP 5.0." In *Security and Usability: Designing Secure Systems That People Can Use*, edited by Lorrie Faith Cranor and Simson Garfinkel, 679–702. Sebastopol, CA: O'Reilly.
- WORTHINGTON, DEBRA L., AND DAVID G. LEVASSEUR. 2015. "To Provide Or Not to Provide Course Power-Point Slides? The Impact of Instructor-Provided Slides Upon Student Attendance and Performance." *Computers & Education* 85: 14–22.
- YU, MIN-CHUN, YEN-CHUN JIM WU, WADEE ALHALABI, HAO-YUN KAO, AND WEN-HSIUNG WU. 2016. "Research-Gate: An Effective Altimetric Indicator for Active Researchers?" *Computers in Human Behavior* 55: 1001–6.
- ZITTRAIN, JONATHAN. 2008. *The Future of the Internet. And How to Stop It*. New Haven, CT: Yale University Press.
- ZITTRAIN, JONATHAN L., ROBERT FARIS, HELMI NOMAN, JUSTIN CLARK, CASEY TILTON, AND RYAN MORRISON-WESTPHAL. 2017. "The Shifting Landscape of Global Internet Censorship." *Internet Monitor* 2017–4. Berkman Klein Center for Internet & Society.
- ZUBOFF, SHOSHANA. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30: 75–89.
- . 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.