Editorial

Post-Snowden Internet Policy: Between Public Outrage, Resistance and Policy Change

Julia Pohle 1,* and Leo Van Audenhove 2,3

1 Internet Policy Project Group, WZB Berlin Social Science Center, 10785 Berlin, Germany; E-Mail: julia.pohle@wzb.eu
2 IMEC-SMIT Studies on Media, Information and Telecommunication, Vrije Universiteit Brussel, 1050 Brussels, Belgium; E-Mail: leo.van.audenhove@vub.ac.be
3 Co-Lab for e-Inclusion and Social Innovation, University of the Western Cape, Cape Town, 7535, South Africa

* Corresponding author

Submitted: 28 February 2017 | Published: 22 March 2017

Abstract

This editors’ introduction provides a short summary of the Snowden revelations and the paradoxical political and public responses to them. It further provides an overview of the current academic debate triggered by the Snowden case and the documents leaked by him and introduces the articles featured in this issue on post-Snowden Internet policy.

Keywords
digital; intelligence agency; Internet policy; policy change; privacy; Snowden; surveillance; whistleblowing

Issue

This article is part of the issue “Post-Snowden Internet Policy”, edited by Julia Pohle (WZB Berlin Social Science Center, Germany) and Leo Van Audenhove (Vrije Universiteit Brussel, Belgium).

© 2017 by the authors; licensee Cogitatio (Lisbon, Portugal). This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

It was late May 2013 when a 30-year-old American computer professional walked through the arrivals hall of Hong Kong International Airport. In his luggage he carried four laptop computers, enabling him to access some of the US government’s most highly-classified secrets. He was about to commit the biggest act of whistleblowing in the history of modern intelligence agencies, to be named after him: the Snowden revelations.

The man behind the disclosures, Edward Snowden, had worked with US intelligence agencies since 2006 and started his job as a subcontractor to the National Security Agency (NSA) for the companies Dell and Booz Allen Hamilton in 2009 (Ray, 2016). During that time, he began collecting data and information on the NSA’s secret surveillance programmes. Convinced that these practices were excessive and invasive in nature, he decided to reveal them to the public, as he could not “in good conscience allow the US government to destroy privacy, Internet freedom and basic liberties for people around the world with this massive surveillance machine they’re secretly building” (Greenwald, MacAskill, & Poitras, 2013). During his stay in Hong Kong, Snowden met with two Guardian journalists, Glenn Greenwald and Ewen MacAskill, and the documentary filmmaker Laura Poitras, to whom he consigned thousands of classified NSA documents. On June 5th, The Guardian started to report on the leaked material. Shortly afterwards, Snowden went public of his own accord, arguing that he did not need to hide, having done nothing wrong.

Over the following months, several other important news outlets around the world obtained access to the leaked documents and reported on their content, most prominently Der Spiegel, The Washington Post, The New York Times, O Globo and Le Monde. In several countries, these continuous publications provoked a chorus of outrage by policy-makers, the media, civil society activists and the general public. So far, however, they have not been followed by effective limitations to state surveillance and better safeguards to protect the right to privacy. Quite the contrary, most governments—including
those who publicly spoke out against the US practices—
seem reluctant to seriously review their own intelligence
frameworks. Instead, over the last years, many of them
legalised existing practices and strengthened their coop-
eration with the US and other foreign services (see also Tréguer, 2017).

This “paradoxical mismatch between harsh criticism
and stable cooperation” (Steiger, Schünemann, & Dimroth, 2017), meaning the discrepancy between discourse
and policy change, is one of the many important fact-
ors that make the Snowden revelations, their content
and their consequences a highly relevant research topic
for communication sciences. Not only on the political
level but also in academia, the disclosures have acceler-
ated a necessary debate about the future of Internet pol-
icy and the importance of data protection in an increas-
ingly globalised world interconnected by digital infra-
structures. The intense public and academic discussions
about the documents leaked by Edward Snowden show
that his revelations are unprecedented. Indeed, they pro-
vide insights into a wide network of surveillance tools,
programmes and actors covering at least three different dimensions: Firstly, they revealed the scale and extent
of surveillance, meaning the massive quantity of the col-
clected data and the vast number of people who are being
systematically surveilled; secondly, they provide exten-
sive information about the kind of data that is being in-
tercepted and collected, ranging from metadata (i.e. who
communicated with whom and when) to the content of
phone calls and emails; and thirdly, they reveal the actual
practices of surveillance, i.e. the different programmes
and cooperation mechanisms that allow for the vastness
of surveillance in place and the integration and process-
ing of the collected data.

Although the Snowden revelations focus on the
NSA as a main actor, they also touch on practices of the British Government Communications Headquarters
(GCHQ) and the US alliances with other intelligence ser-
VICES within the so-called Five Eyes network (compris-
ing Australia, Canada, New Zealand, the UK and the
USA). In addition, they shed light on the US coopera-
tion with European intelligence agencies, such as the Ger-
man Bundesnachrichtendienst (BND) and the French Di-
rection Générale De La Sécurité Extérieure. Furthermore,
the leaked documents demonstrate that the NSA and
its allies not only intercept telecommunication and In-
ternet content and metadata themselves, for instance
through GCHQ’s TEMPORA programme. Via the PRISM
programme, the NSA also accesses and collects Internet
communications from at least nine US Internet compa-
nies, such as Google and Facebook, allegedly in parts
without their knowledge. What was particularly shocking
to many was that the NSA and its allies not only surveilled
non-US citizens domestically and abroad (and US citizens
communicating with foreigners) but also spied on world
leaders and international organisations (Poitras, Rosen-
bach, & Stark, 2014), such as the IMF, World Bank, Hu-
man Rights Watch and Amnesty International, and mon-
itored the preparation of global events, for instance the
2009 Copenhagen summit on Climate Change (Gjerding,
Moltke, Geist, & Poitras, 2014).

It was in particular the surveillance of political and
economic institutions of allied nations that caused inter-
national repercussions. In September 2013, the report
that the NSA had spied on Brazil’s president Dilma Rouss-
eff and the Brazilian oil company Petrobras prompted
Rousseff to cancel her planned US visit and led to the
installation of a parliamentary commission of inquiry
and an investigation by the Brazilian federal police. Simi-
larly, after news broke that the BND gave NSA access to
mass surveillance metadata in Germany and that the NSA
had monitored the communication of Chancellor Angela
Merkel, a parliamentary committee of inquiry on the NSA
was established at the German Bundestag in March 2014,
a committee that has yet to finish its work. As another re-
tponse to these incidents, Germany and Brazil submitted
a joint UN resolution entitled “Right to Privacy in the Di-
gital Age”, which was adopted by the UN General Assembly
in December 2013.

In spite of the wide-spread indignation by political
actors and civil society, the Snowden revelations have
not led to extensive and tangible policy changes (see
also Steiger et al., 2017). Some of the governments
that found themselves under US surveillance came to
realise—either through further leaked NSA documents
or through their own investigations—that their own in-
telligence agencies have been playing a rather inglorious
role with regard to the revealed practices. Not only had
many of them benefitted from the intelligence collection
by the US services, they often also gathered excessive in-
formation themselves by way of rather dubious methods.
As a consequence, many countries, including the US, im-
plemented surveillance reforms in reaction to the leaks.
Yet most of the reforms rather served to adapt the legal
foundations to the already existing practices or even to
expand the agencies’ authority for surveillance. At the
same time, new oversight powers were limited in scope.
Instead of reforming a system that, according to Snow-
den, has gone out of control, the system has been con-
solidated. The UK, for instance, passed its Investigatory
Powers Act in November 2016 to clarify the investiga-
tory powers of the British law enforcement and intelli-
gence agencies (Hintz & Dencik, 2016). But rather than
limiting these powers, the act has been accused of legal-
isation a “range of tools for snooping and hacking by the
security services” that were already being used but pre-
viously ruled illegal by the investigatory powers tribunal
(MacAskill, 2016). Snowden himself supported the civil
society objections against the passed act by commenting
that “the UK has just legalised the most extreme surveil-
ance in the history of western democracy. It goes further
than many autocracies” (Snowden, 2016).

Of course, the reform of intelligence legislation was
not the only response triggered by Snowden’s disclo-
sures and the wider debate on mass surveillance. Over
the last years, we could witness a variety of changing
practices, policies and discourses that can—in one way or another—be related to post-Snowden contentions. In the light of the role of big Internet corporations for signals intelligence, it is interesting to interpret recent changes in these corporations’ policy and encryption practices in the post-Snowden context, for example their resistance to granting authorities access to their data and devices, as witnessed in the struggle between Apple and the FBI over unlocking an iPhone in spring 2016 (see the contributions of Kumar, 2017; and Schulze, 2017). Similarly, it is possible to see a connection between the actions of policy makers and the changing role of national and international courts, such as the European Court for Human Rights, as last institutional resorts against governmental and corporate power in the digital sphere. In addition, the debate about the NSA documents also led to new practices and different kinds of cooperation on the side of civil society, for instance in the form of national and transnational activist movements against Internet surveillance or resistance tactics by Internet users allowing them to bypass censorship and surveillance (see Ermoshina & Musiani, 2017). Lastly, the actions of Edward Snowden, who gave up a comfortable life in Hawaii in exchange for criminal charges and temporary exile in Russia, and the harsh response by the US administration provoked the (re)emergence of national and transnational debates on the importance and challenges of whistleblowing. While the US authorities filed charges against Snowden under the 1917 US Espionage Act, he received important awards in other countries, such as the German Whistleblower Prize in August 2013. This led to a new level of public and political awareness regarding the lack of sufficient whistleblower protection in many countries around the world, including the most liberal democracies (see also Brevini, 2017).

The many processes and discussions triggered by the Snowden revelations are also reflected by the growing body of academic literature that has emerged since the first disclosures in summer 2013. This literature can be roughly grouped into four research streams, each focussing on a different aspect of the manifold issues at stake in the post-Snowden environment:

Unsurprisingly, the first and largest stream of research is marked by an analytical interest in surveillance and its societal repercussions. Not only in law but in many other social sciences, the Snowden revelations led academics to analyse the legal aspects of surveillance, be it the existing legal frameworks and their reformation (e.g. Geist, 2015; Ni Loideain, 2015) or the general relationship of surveillance, law and civil liberties, including the right to privacy (e.g. Clement & Obar, 2016; Lippert, 2015; Lucas, 2014; Paterson, 2014). Others reflected on the interplay between technology, surveillance and power (e.g. Bauman et al., 2014; Lyon, 2014, 2015) and the broader societal and (geo)political consequences of mass surveillance (e.g. Aust & Ammann, 2016; Giroux, 2015; Keiber, 2015; Marsden, 2014). Closely related are also abstract discussions and empirical analyses of the alleged contrast between security and liberty (e.g. Lieber, 2014; Lowe, 2016).

Besides the political and academic discussions on mass surveillance and privacy, the second stream of post-Snowden research focusses on the public reaction to the NSA revelations. While a number of authors analysed the reporting on Snowden and competing discourses in national and international media (e.g. Branum & Charteris-Black, 2015; Di Salvo & Negro, 2016; Madison, 2014), others used diverse conceptual approaches to assess how Snowden and his leaks were framed in social media (e.g. Marres & Moats, 2015; Qin, 2015) and what effect his revelations had on democratic discourse and free expression within these digital channels (Stoycheff, 2016).

Moving away from the surveillance nexus and the responses triggered by the Snowden disclosures, the third stream of research deals with the highly political issues of civil disobedience in general and whistleblowing in particular. In this context, many authors discuss the particularities of the growing phenomenon of digital disobedience (e.g. Lagasnerie, 2016; Scheuerman, 2016), the problem of counter-surveillance as a form of resistance (Gürses, Kundnani, & Van Hoboken, 2016) and the question whether Snowden’s deeds can be characterised as acts of civil disobedience (Brownlee, 2016; Scheuerman, 2014). Focussing on whistleblowing as a particular form of resistance, other contributions range from historical perspectives on national security leaks (Gardner, 2016; Moran, 2015) to the problem of legal protection (e.g. Paquette, 2013; Peffer et al., 2015) and the question of how acts of whistleblowing are conducted, framed, and perceived (e.g. Contu, 2014; Rios & Ingraffia, 2016). Others again centre on the increasingly politicised issue of transparency and its role in modern societies (e.g. Borradori, 2016; Fenster, 2015; Flyverbom, 2015).

The fourth and last research stream takes a much broader perspective than the others by looking at the Snowden revelations in the larger context of national and global Internet policy (e.g. Deibert, 2015). Under this umbrella, scholars closely followed the changing perception of and policy towards the Internet as a political space, for instance in terms of cybersecurity (e.g. Lee, 2013) or global Internet Governance (Nocetti, 2015).

The contributions of this thematic issue add to all of these research streams through conceptual considerations and empirical case studies. With their focus on state and non-state policy, however, they contribute to one of the currently understudied repercussions of the Snowden contentions, namely the concrete changes in Internet policy and their interrelation with specific discourses, issues and actors in the aftermath of the Snowden revelations.

The first two articles explore how two national governments that were equally involved in parts of the practices revealed by the NSA documents responded to public demands for more surveillance oversight. Steiger et al. (2017) assess German parliamentary and governmental documents to discuss the misfit between the public out-
rage over the Snowden revelations and the actual reform of policies and practices in Germany. They identify recurrent elements in parliamentary and governmental discourses facilitating the authorities’ reluctance to act, such as the tense relationship between freedom and security, the priority given to digital sovereignty and post-privacy narratives. Félix Tréguer (2017) also analyses the response of a European country, in this case France, to the debate on mass surveillance, using a different conceptual and methodological approach and a different focus. His case study of post-Snowden intelligence reform in France examines how the gap between existing legal frameworks and actual surveillance practices is being closed through new legalisation. After the Paris attacks of January 2015, the French government passed the Intelligence Act, which can be considered the most extensive piece of legislation ever adopted in France to regulate secret state surveillance. Although the paradoxical practice to legalise surveillance practices in the midst of post-Snowden contention is not unique to France and can be viewed as part of a wider international trend, Tréguer also sees it as a chance for the emerging privacy movement to use these legalisation strategies to roll back surveillance practices.

Shifting the focus away from liberal democracies renegotiating the limits of mass surveillance, two contributions focus on the country that since 2013 has been granting exile to Edward Snowden although its own Internet approach is often heavily criticised for running counter to Snowden’s fight for transparency and freedom. Taking a holistic and historical perspective on Russian information and Internet policy, the contribution of Nathalie Maréchal (2017) draws a picture of the networked authoritarianism practiced in Russia. The author considers Russia’s domestic information controls policy and its role in global Internet governance processes as part of its foreign policy seeking to (re-)establish itself as a major geopolitical player. She therefore argues that the geopolitics of information will become increasingly important in the years to come. The contribution by Ksenia Ermoshina and Francesca Musiani (2017) looks at Russian Internet policy from a different angle by assessing the country’s state-centred style of Internet governance and users’ way of dealing with it from a perspective of Science and Technology Studies. Thus, it not only addresses the Russian way of “Internet governance by infrastructure” but also analyses the various resistance tactics that Russian users have developed to counter these governance mechanisms. Investigating individual and collective forms of resistance, the article focuses on the materiality of tactics employed, spanning from infrastructure-based countermeasures to the migration of hardware and people.

The following two contributions to this thematic issue are shifting the focus from the relations between governments and civil society towards government interaction with the private sector. In a comparative analysis, Matthias Schulze (2017) contrasts two cryptography discourses from 1993 and 2016 to analyse the competing discourses on whether the government should be able to monitor secure and encrypted communication. Based on the securitisation framework, the author assesses how security threats were constructed within these discourses and compares the arguments of proponents and critics of exceptional access. The contribution of Priya Kumar (2017) likewise focusses on private-sector actors and their concern for data protection. His contribution investigates the changes in the privacy policies of the nine companies involved in the PRISM programme plus Twitter in order to trace how company practices concerning user information have shifted over the last years. Showing that company disclosure of tracking for advertising purposes increased, the author concludes that public debates about post-Snowden privacy rights cannot ignore the role that companies play in legitimizing surveillance activities to create market value.

The implications of tightening security legislation for journalists and the lack of whistleblower protection for their sources are at the core of Benedetta Brevini’s (2017) contribution. Analysing the changing legal framework in Australia after the Snowden leaks, the author interprets the changes as a threat to the work of journalists who increasingly find themselves the targets of bulk data collection. Brevini concludes with a warning that to Australian journalism, a space for agency to resist public metadata retention’s schemes might be needed more than ever—but is missing.

Acknowledgements

The publication of this issue was financially supported by the Open Access fund of the Leibniz Association and is co-sponsored by the Communication Policy and Technology (CP&T) Section of the International Association for Media and Communication Research (IAMCR). We thank the authors of this issue, the staff of Media and Communication and the many external reviewers who commented on the manuscripts submitted for this issue.

Conflict of Interests

The authors declare no conflict of interests.

References


About the Authors

**Julia Pohle** is a senior researcher in the Internet policy project group at the WZB Berlin Social Science Center. She holds a PhD in Communication Studies from the Vrije Universiteit Brussel. She currently serves as Vice-Chair for the Communication Policy and Technology Section of the International Association for Media and Communication Research (IAMCR) and as a member of the Steering Committee of the German Internet Governance Forum (IGF-D). Her research focuses on Internet policy, global communication governance, Science and Technology Studies and digitalisation.

**Leo Van Audenhove** is a professor and head of department at the Department of Communication Studies of Vrije Universiteit Brussel. He is a researcher at imec-SMIT—Studies on Media, Innovation and Technology at the same university. He is extra-ordinary professor at the University of the Western Cape. In 2013, he was instrumental in setting up the Knowledge Centre for Media Literacy in Flanders, of which he subsequently became the director. The centre was established by government as an independent centre to promote media literacy in Flanders. His research focuses on Internet governance, media literacy, e-inclusion and ICT4D.