Pohle, Julia; Van Audenhove, Leo

Post-Snowden internet policy: between public outrage, resistance and policy change

Media and Communication

Provided in Cooperation with:
WZB Berlin Social Science Center

Suggested Citation: Pohle, Julia; Van Audenhove, Leo (2017) : Post-Snowden internet policy: between public outrage, resistance and policy change, Media and Communication, ISSN 2183–2439, Cogitatio, Lisbon, Vol. 5, Iss. 1, pp. 1-6, https://doi.org/10.17645/mac.v5i1.932

This Version is available at:
https://hdl.handle.net/10419/161621

COGITATIO

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 1–6
DOI: 10.17645/mac.v5i1.932

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 Februray 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).

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 cooperation 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 factors 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 accelerated a necessary debate about the future of Internet policy and the importance of data protection in an increasingly globalised word interconnected by digital infrastructures. The intense public and academic discussions about the documents leaked by Edward Snowden show that his revelations are unprecedented. Indeed, they provide 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 collected data and the vast number of people who are being systematically surveilled; secondly, they provide extensive information about the kind of data that is being intercepted 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 processing 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 services within the so-called Five Eyes network (comprising Australia, Canada, New Zealand, the UK and the USA). In addition, they shed light on the US cooperation with European intelligence agencies, such as the German *Bundesnachrichtendienst* (BND) and the French *Direction Générale De La Sécurité Extérieure*. Furthermore, the leaked documents demonstrate that the NSA and its allies not only intercept telecommunication and Internet 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 companies, 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, Rosenbach, & Stark, 2014), such as the IMF, World Bank, Human Rights Watch and Amnesty International, and monitored 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 international repercussions. In September 2013, the report that the NSA had spied on Brazil's president Dilma Rousseff and the Brazilian oil company Petrobas 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. Similarly, 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 response to these incidents, Germany and Brazil submitted a joint UN resolution entitled "Right to Privacy in the Digital 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 intelligence 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 information themselves by way of rather dubious methods. As a consequence, many countries, including the US, implemented 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 Snowden, has gone out of control, the system has been consolidated. The UK, for instance, passed its Investigatory Powers Act in November 2016 to clarify the investigatory powers of the British law enforcement and intelligence agencies (Hintz & Dencik, 2016). But rather than limiting these powers, the act has been accused of legalising a "range of tools for snooping and hacking by the security services" that were already being used but previously 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 surveillance 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 disclosures 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

Aust, S., & Ammann, T. (2016). *Digitale Diktatur: Totalüberwachung, Datenmissbrauch, Cyberkrieg*. Berlin: Ullstein.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144.

Borradori, G. (2016). Between transparency and surveillance: Politics of the secret. *Philosophy & Social Criticism*, *42*(4/5), 456–464.

Branum, J., & Charteris-Black, J. (2015). The Edward

Snowden affair: A corpus study of the British press. *Discourse & Communication*, *9*(2), 199–220.

Brevini, B. (2017). Metadata laws, journalism and resistance in Australia. *Media and Communication*, *5*(1), 76–83.

Brownlee, K. (2016). The civil disobedience of Edward Snowden: A reply to William Scheuerman. *Philosophy & Social Criticism*, *42*(10), 965–970.

Clement, A., & Obar, J. A. (2016). Keeping internet users in the know or in the dark: An analysis of the data privacy transparency of Canadian internet carriers. *Journal of Information Policy*, *6*, 294–331.

Contu, A. (2014). Rationality and relationality in the process of whistleblowing: Recasting whistleblowing through readings of Antigone. *Journal of Management Inquiry*, *23*(4), 393–406.

Deibert, R. (2015). The geopolitics of cyberspace after Snowden. *Current History*, *114*(168), 9–15.

Di Salvo, P., & Negro, G. (2016). Framing Edward Snowden: A comparative analysis of four newspapers in China, United Kingdom and United States. *Journalism*, *17*(7), 805–822.

Ermoshina, K., & Musiani, F. (2017). Migrating servers, elusive users: Reconfigurations of the Russian Internet in the post-Snowden era. *Media and Communication*, *5*(1), 42–53.

Fenster, M. (2015). Transparency in search of a theory. *European Journal of Social Theory*, *18*(2), 150–167.

Flyverbom, M. (2015). Sunlight in cyberspace? On transparency as a form of ordering. *European Journal of Social Theory*, *18*(2), 168–184.

Gardner, L. C. (2016). *The war on leakers: National security and American democracy, from Eugene v. Debs to Edward Snowden*. New York, NY: The New Press.

Geist, M. (2015). *Law, privacy and surveillance in Canada in the post-Snowden era*. Ottawa: University of Ottawa Press.

Giroux, H. A. (2015). Totalitarian paranoia in the post-Orwellian surveillance state. *Cultural Studies*, *29*(2), 108–140.

Gjerding, S., Moltke, H., Geist, A., & Poitras, L. (2014, January 30). NSA spied against UN climate negotiations. *Information*. Retrieved from https://www.information.dk/udland/2014/01/nsa-spied-against-un-climate-negotiations

Greenwald, G., MacAskill, E., & Poitras, L. (2013, June 11). Edward Snowden: The whistleblower behind the NSA surveillance revelations. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Gürses, S., Kundnani, A., & Van Hoboken, J. (2016). Crypto and empire: The contradictions of counter-surveillance advocacy. *Media, Culture & Society*, *38*(4), 576–590.

Hintz, A., & Dencik, L. (2016). The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review*, *5*(3). doi:10.14763/2016.3.424

Keiber, J. (2015). Surveillance hegemony. *Surveillance & Society*, *13*(2), 168–181.

Kumar, P. (2017). Corporate privacy policy changes during PRISM and the rise of surveillance capitalism. *Media and Communication*, *5*(1), 63–75.

Lagasnerie, G. de. (2016). *Die Kunst der Revolte: Snowden, Assange, Manning*. Berlin: Suhrkamp.

Lee, N. (2013). *Counterterrorism and cybersecurity: Total information awareness*. New York, NY: Springer.

Lieber, R. J. (2014). Security vs. privacy in an era of terror and technology. *Telos*, *2014*(169), 144–149.

Lippert, R. K. (2015). Thinking about law and surveillance. *Surveillance & Society*, *13*(2), 292–294.

Lowe, D. (2016). Surveillance and international terrorism intelligence exchange: Balancing the interests of national security and individual liberty. *Terrorism and Political Violence*, *28*(4), 653–673.

Lucas, G. R. (2014). NSA management directive #424: Secrecy and privacy in the aftermath of Edward Snowden. *Ethics & International Affairs*, *28*(1), 29–38.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, *1*(2).

Lyon, D. (2015). The Snowden stakes: Challenges for understanding surveillance today. *Surveillance & Society*, *13*(2), 139–152.

MacAskill, E. (2016, November 19). "Extreme surveillance" becomes UK law with barely a whimper. *The Guardian*. Retrieved from https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper

Madison, E. (2014). News narratives, classified secrets, privacy, and Edward Snowden. *Electronic News*, *8*(1), 72–75.

Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. *Media and Communication*, *5*(1), 29–41.

Marres, N., & Moats, D. (2015). Mapping controversies with social media: The case for symmetry. *Social Media + Society*, *1*(2), 1–17.

Marsden, C. (2014). Hyper-power and private monopoly: The unholy marriage of (neo)corporatism and the imperial surveillance state. *Critical Studies in Media Communication*, *31*(2), 100–108.

Moran, C. (2015). Turning against the CIA: Whistleblowers during the "Time of Troubles". *History*, *100*(340), 251–274.

Ni Loideain, N. (2015). EU law and mass internet metadata surveillance in the post-Snowden era. *Media and Communication*, *3*(2), 56–62.

Nocetti, J. (2015). Contest and conquest: Russia and global Internet governance. *International Affairs*, *91*(1), 111–130.

Paquette, L. (2013). The whistleblower as underdog: What protection can human rights offer in massive secret surveillance? *The International Journal of Human Rights*, *17*(7/8), 796–809.

Paterson, N. E. (2014). End user privacy and policy-based networking. *Journal of Information Policy*, *4*, 28–43.

Peffer, S. L., Bocheko, A., Del Valle, R. E., Osmani, A., Peyton, S., & Roman, E. (2015). Whistle where you work? The ineffectiveness of the Federal Whistleblower Protection Act of 1989 and the promise of the Whistleblower Protection Enhancement Act of 2012. *Review of Public Personnel Administration*, *35*(1), 70–81.

Poitras, L., Rosenbach, M., & Stark, H. (2014, March 29). "A" for Angela: GCHQ and NSA targeted private German companies and Merkel. *Der Spiegel*. Retrieved from http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html

Qin, J. (2015). Hero on Twitter, traitor on news: How social media and legacy news frame Snowden. *The International Journal of Press/Politics*, *20*(2), 166–184.

Ray, M. (2016). Edward Snowden. In *Encyclopaedia Britannica*. Retrieved from https://www.britannica.com/biography/Edward-Snowden

Rios, K., & Ingraffia, Z. A. (2016). Judging the actions of "whistle-blowers" versus "leakers": Labels influence perceptions of dissenters who expose group misconduct. *Group Processes & Intergroup Relations*, *19*(5), 553–569.

Scheuerman, W. E. (2014). Whistleblowing as civil disobedience: The case of Edward Snowden. *Philosophy & Social Criticism*, *40*(7), 609–628.

Scheuerman, W. E. (2016). Digital disobedience and the law. *New Political Science*, *38*(3), 299–314.

Schulze, M. (2017). Clipper meets Apple vs. FBI—A comparison of the cryptography discourses from 1993 and 2016. *Media and Communication*, *5*(1), 54–62.

Snowden, E. (2016, November 13). The UK has just legalized the most extreme surveillance in the history of western democracy. It goes farther than many autocracies. *Twitter*. Retrieved from https://twitter.com/snowden/status/799371508808302596

Steiger, S., Schünemann, W., & Dimmroth, K. (2017). Outrage without consequences? Post-Snowden discourses and governmental practice in Germany. *Media and Communication*, *5*(1), 7–16.

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. *Journalism & Mass Communication Quarterly*, *93*(2), 296–311.

Tréguer, F. (2017). Intelligence reform and the Snowden paradox: The case of France. *Media and Communication*, *5*(1), 17–28.

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.