Media and Communication

Open Access Journal | ISSN: 2183-2439

Volume 5, Issue 1 (2017)

Post-Snowden Internet Policy

Editors

Julia Pohle and Leo Van Audenhove

COGITATIO

Media and Communication, 2017, Volume 5, Issue 1
Post-Snowden Internet Policy

Published by Cogitatio Press
Rua Fialho de Almeida 14, 2º Esq.,
1070-129 Lisbon
Portugal

Academic Editors
Julia Pohle, WZB Berlin Social Science Center, Germany
Leo Van Audenhove, Vrije Universiteit Brussel, Belgium

Editors-in-Chief
Epp Lauk, University of Jyväskylä, Finland
Raul Reis, Emerson College, USA

Available online at: www.cogitatiopress.com/mediaandcommunication

Table of Contents

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 outrage 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.

COGITATIO

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 7–16
DOI: 10.17645/mac.v5i1.814

Article

Outrage without Consequences? Post-Snowden Discourses and Governmental Practice in Germany

Stefan Steiger [1],*, Wolf J. Schünemann [2] and Katharina Dimmroth [3]

[1] Institute of Political Science, Heidelberg University, 69115 Heidelberg, Germany;
E-Mail: stefan.steiger@ipw.uni-heidelberg.de
[2] Institute of Social Sciences, Hildesheim University, 31141 Hildesheim, Germany;
E-Mail: wolf.schuenemann@uni-hildesheim.de
[3] Institute of Political Science, Rheinisch-Westfälische Technische Hochschule Aachen, 52074 Aachen, Germany;
E-Mail: katharina.dimmroth@ipw.rwth-aachen.de

* Corresponding author

Submitted: 31 October 2016 | Accepted: 20 January 2017 | Published: 22 March 2017

Abstract
In 2013 Edward Snowden's disclosures of mass surveillance performed by US intelligence agencies seriously irritated politicians and citizens around the globe. This holds particularly true for privacy-sensitive communities in Germany. However, while the public was outraged, intelligence and security cooperation between the United States and Germany has been marked by continuity instead of disruption. The rather insubstantial debate over a so-called "No-Spy-Agreement" between the United States and Germany is just one telling example of the disconnect between public discourse and governmental action, as is the recent intelligence service regulation. This article considers why and where the "Snowden effect" has been lost on different discursive levels. We analyze and compare parliamentary and governmental discourses in the two years after the Snowden revelations by using the Sociology of Knowledge Approach to Discourse (SKAD) to dissect the group-specific statements and interpretive schemes in 287 official documents by the German Bundestag, selected ministries and agencies within the policy subsystem. These will be analyzed in reference to actual governmental practice.

Keywords
cyber security; discourse analysis; dispositive analysis; German–US intelligence cooperation; surveillance

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).

1. Introduction

When the Snowden revelations exposed the extensive surveillance practices established by the US National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ) in June 2013, international criticism loomed large. Among US allies, Germany has been one of the most vocal critics of the revealed surveillance measures. Chancellor Angela Merkel most prominently expressed German discomfort in October 2013, when she said "spying among friends is completely unacceptable" (Troianovski, Gorman, & Torry, 2013). While criticism was also expressed in parliament and a commission of inquiry was set up in early 2014, actual cooperation with the US remained relatively stable. Furthermore, in 2016 the federal government proposed a new legislative framework for the German foreign intelligence agency Bundesnachrichtendienst (BND) that was approved by the German Bundestag in October of the same year. The new law, according to many experts (Bäcker, 2016; Papier, 2016; Wetzling, 2016), legalizes extensive governmental surveillance practices and may even be unconstitutional.

It is this seemingly paradoxical mismatch between harsh criticism and stable cooperation that we are going to analyze within the scope of this article. Our main research questions are therefore: How is it possible that Germany was a vocal critic of the revealed spy practices and nevertheless maintained a stable cooperation with the US? As even a superficial look into the public and political debates in Germany reveals, there has clearly been a "Snowden effect" in Germany, which has brought the issue of mass surveillance to the fore of public policy. Why has it not led to a significant change in regulation or the practices of governmental agencies? Where and why did the Snowden effect get lost within different discourse formations (parliamentary, governmental)?

Up to now, research on governmental reactions to the Snowden revelations has been published only scarcely. When discussed, German government reactions have been covered with a focus on arguments legitimizing surveillance measures (Schulze, 2015). We will go further by also analyzing the parliamentary debate and investigating the practical implications of possible discursive shifts with a deeper look into the dispositives (institutions, regulations and practices). In the existing literature, one can identify slightly different perspectives on the German reaction to the disclosed practices. These views seem to be facilitated by an emphasis on either practical consequences or rhetoric. Emphasizing the harsh criticism following the revelations, Bersick, Christou and Yi (2016, pp. 176–177) state that:

> In the case of Germany, the Snowden affair even undermined the general belief in the normative foundations of the US–German relationship and gave rise to previously unheard-of criticism of the United States by German members of the federal cabinet.

Other scholars emphasized that practical relations (especially security cooperation) between the US and Germany remained stable in the aftermath of the revelations. Segal (2016, p. 150) concludes that "even at the zenith of the public backlash, cooperation between the US and German intelligence agencies never stopped". Segal tentatively argues that this reaction was motivated by the German "dependence on US intelligence capabilities" (Segal, 2016, p. 143), but his claim is not built on significant empirical data from the German administration or parliament. We would like to substantiate this debate and take those findings as a starting point for our analysis. We agree with Bersick et al. (2016) that leading politicians in Germany voiced strong criticism against the US (and the UK) regarding the revelations, and we also acknowledge in concurrence with Segal (2016) that practical implications remained marginal, as is clearly underlined by the latest developments. But together, both observations set the puzzle that we are investigating.

In order to provide an answer to our research questions, the article will proceed in four steps. The next section lays out our framework for discourse analysis and specifies our methodological approach. To illustrate the reluctant German reactions, the third section presents a short analysis of the most important practical events following the Snowden revelations; this part sheds light on the measures the German government has actually taken to deal with the revelations. Our empirical analysis of governmental and parliamentary discourse is then presented in the fourth section. A final conclusion sums up our findings.

2. Discourses, Dispositives and What Happens in between: Theory and Methodology

Discourse research has gained ground in political science in recent years (pars pro toto: Hajer, 2002; Howarth, Norval, & Stavrakakis, 2000; Wodak & Krzyzanowski, 2008). Even in international relations and security studies, discourse analysis (DA) has become more popular, and the scope of DA methodology has considerably broadened (for cyber security and online communication issues see for instance: Balzacq, 2011; Gorr & Schünemann, 2013; Xiao Wu, 2012). First of all, we adhere to a Foucauldian discourse theory (Foucault, 2002), which makes the discourse a socio-historically specific knowledge formation that appears materially manifested in social communication. Moreover, we apply an approach developed from the combination of Foucauldian discourse theory and the Sociology of Knowledge tradition in sociology. The Sociology of Knowledge Approach to Discourse ([SKAD] Keller, 2008) has been developed by German sociologist Reiner Keller since the late 1990s. One crucial advantage of SKAD in relation to other discourse analytical approaches is that it brings the actor back into focus. SKAD furthermore provides the analyst with a research framework encompassing a set of basic interpretive schemes, which complement the interpretive analytics otherwise adopted from Foucault.

Corpus-building is one of the first and most important steps of any solid discourse research. For this study, we chose an actor-oriented approach. This was relatively easy for the parliamentary debate, as we selected all Bundestag protocols dealing with cyber security issues by using the search function of the official Bundestag database, entering the search terms "cyber security" and "cyber attack". We cut and parsed the resulting protocols to include only the sections that dealt with the relevant issue, since a single Bundestag debate may deal with a variety of topics. For governmental actors and agencies, we identified ministries and investigative authorities as the key actors in German cyber security policy, i.e. the policy subsystem (Sabatier, 1988). The identified actors were the Federal Government, the Federal Foreign Office, the Federal Ministry of the Interior, the Federal Ministry of Defense, the Federal Ministry for Economic Affairs and Energy, the Federal Ministry of Justice and Consumer Protection and the Federal Office for Information Security. We continued our document-gathering by entering the same query terms of "cyber security"

("Cybersicherheit") and "cyber attack" ("Cyberangriff") using the search functions provided by the ministries' websites. The query terms had been intuitively selected and then validated using the "relative query term relevance" (RQTR) method proposed by Costas Gabrielatos (2007). The period of analysis spans the two years following the Snowden revelations, i.e. June 1, 2013, to May 31, 2015. The governmental documents we identified by using our query terms ranged from official ministry reports, interviews and speeches to press releases. Our final corpus for analysis consisted of 287 documents in total, 156 of which came from government offices and 131 from parliament.

As to our interpretive analysis, we analyze our corpus first for the recurrent statements and then look, in accordance with SKAD methodology, for all sorts of interpretive schemes (some call them frames) included therein. These patterns of interpretation can again be divided into subtypes such as narratives, classifications or subject positions (Keller, 2008). While statements are thus the basic analytical unit for a discourse analysis, being based on the social actors' worldview, i.e. how people make sense of the world around them, the interpretive scheme is the overarching analytical category towards which the more concrete and specific interpretive codes of the researcher are oriented. Our case, for example, raises the question of whether the newly disclosed surveillance activities amount to illegal espionage and a breach of trust, or whether they are seen and justified as a legitimate part of a protective role and, thus, an example of successful intelligence cooperation.

In addition to SKAD, the Foucauldian term of the dispositive is also of particular importance for this study. The dispositive—in the Foucauldian sense and as adopted by Keller—is an umbrella term for all sorts of power-effects through which a discourse leaves its lasting mark on the world and/or the organization of a given society. While the discourse is a practice itself and it appears as materialized practice as well, it is still necessarily transient as knowledge elements are being processed all the time and never reach a fixed state. However, they do have long lasting effects on the world and the ordered living of a society through established practices, regulations, and institutions. The dispositive thus includes "material objects (buildings, technologies, etc.), practices (such as the execution of punishments) and elements in the form of texts (such as the adoption of laws)" (Keller, 2013, pp. 78–79). Changes in regulatory discourses on public security will likely lead to institutionalization and intervention into the material world or into the rulebook of a society. The same can be expected of data protection or cyber security issues. The "privacy by design" guideline, for instance, which has become almost common sense in many regulatory discourses, is increasingly being institutionalized in laws or guidelines that could be labeled as a data protection dispositive. The sequential and causal logic is not as clear-cut as the examples so far suggest. Of course, dispositives have repercussions for discourses as well. The concept of the dispositive encompasses not only the effects discourses have on the world but also the very infrastructure of discourse production: "The concept of dispositive means the bundle of measures that carries a discourse and transposes it into real-world consequences" (Keller, 2007, p. 50, translation by the authors). This also makes sense and can be illustrated with reference to the cyber security subsystem. The dispositive includes privileged speaker positions (such as the ministers of the interior or the chancellery) as well as fora of discourse production (such as the "NSA-Untersuchungsausschuss" or the Parliamentary Control Committee).

3. German Reactions to the Snowden Revelations

In one of her first public reactions to the revelations in July 2013, Chancellor Merkel already expressed her concerns by highlighting that not all technical possibilities should actually be used to facilitate surveillance, but she also expressed sympathy for different needs for security in the US and Germany (Federal Government, 2013). In this statement, she also announced a program to enhance privacy in order to deal with the new situation. One of the program's key elements took shape in cooperation with the Brazilian government. Both Chancellor Merkel and then President Dilma Rousseff were among the most prominent surveillance targets and were therefore very critical of the practices revealed by Snowden. Together both governments drafted a UN-resolution to ensure privacy in the digital age. Resolution 68/167 was passed by the United Nations General Assembly after some debate in December 2013 (UN, 2013). The resolution emphasized:

> that unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and to freedom of expression and may contradict the tenets of a democratic society. (UN, 2013, p. 2)

The passing of the resolution also closely coincided with a new embarrassment for the German government when surveillance of Angela Merkel's cell phone was disclosed in October (Smale, 2013). While this reaction is connected to privacy concerns frequently articulated in public and parliamentary discourses, it is remarkable that the intergovernmental UN General Assembly was selected as a regulatory forum. Given the non-binding character of UN resolutions, it does not imply any change in practice, not even by the German government as one of the initiators of the resolution.

In contrast, the establishment of a commission of inquiry (the "NSA-Untersuchungsausschuss") by the German Bundestag in January 2014 can be seen as a concrete step to re-evaluate the established intelligence cooperation. Its task is not only to further investigate accusations against the US and British intelligence agencies but to also clarify the activities of German agencies. Another concrete measure, which even entailed a change of practices, came when the federal government, after negotiations on a "no-spy-agreement" had failed, changed its practice of contracting a foreign provider by recalling contracts with Verizon in June 2014. Until then the government had tasked the US-based enterprise with providing services for its telecommunications infrastructure. Consequently, Verizon was replaced by Deutsche Telekom (Hudson, 2014). The decision to replace a US-based company by a German competitor can be seen as clearly rooted in the pursuit of digital sovereignty (see DA below).

In contrast, the temporal and partial disruptions of the German–US intelligence cooperation that started in May 2015 (Connolly, 2015), while being an obvious change in the practices of information sharing, were more of symbolic value. Information sharing was halted when it became public that the NSA had used its cooperation with the German BND to spy on targets within Germany and the European Union (EU). But the change only affected the cooperation in Bad Aibling and, following an investigation, cooperation was re-established in January 2016 (Mascolo, 2016).

Finally, in June 2016 the German government presented a new legal framework for the foreign surveillance activities of the BND (Federal Chancellery, 2016). Since the draft enabled easier information sharing between intelligence agencies and weakened previously established limitations on data collection (Papier, 2016), it was met with considerable criticism. NGOs and journalists argued that the government had legalized previously illegal activities and thereby enhanced the surveillance capabilities of the German intelligence agency (Deutscher Journalisten-Verband, 2016; Meister, 2016). Furthermore, critique was also expressed by representatives of the Organization for Security and Co-operation in Europe (OSCE) and the UN (OSCE, 2016; UN, 2016). Nevertheless, the government remained committed to the new legislative framework and parliament finally passed the new law in October 2016.

As this short summary clearly shows, the German government responded quite reluctantly to the revelations and resorted to more symbolic reactions. In 2016 the government even began to enhance surveillance capabilities. These developments were enabled by different governmental and parliamentary discourses that will be analyzed in the following section.

4. Post-Snowden Discourses Compared: The Debates in the German Bundestag and the Governmental Discourse

In the course of our discourse analysis in the wake of the Snowden revelations, we identified five recurrent discursive elements that seem particularly important for understanding what happened to the Snowden effect in German policy-making. Therefore, we compare how the respective discursive elements differ between the statements of parliamentary and governmental speakers. What is modified and in what way? What gets lost? What is added? How does all this influence the (un)likelihood of a change in practices?

4.1. Reduced Need to Act—The Parliamentary Discourse

4.1.1. The Fundamental Problem—The Tense Relation between Freedom and Security

One of the prevalent discursive trends in parliament after the Snowden revelations strikes at the very heart of the matter, explicitly addressing the tension between freedom and security, which most speakers agree needs to be re-balanced either towards security (with regard to terrorism and potential attacks) or towards freedom. Determining the measures necessary to balance the security and physical wellbeing of the citizens with their right to freedom and privacy is of course the key issue for politicians of all affiliations in the context of the NSA affair.

Most parliamentary speakers tend to come down on the side of freedom:

> These rights to freedom must be protected—against an overly powerful surveillance state, for example—because the quest for complete security leads to tyranny and a lack of freedom. To quote an American, Benjamin Franklin: Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety. Manfred Grund, CDU/CSU (Deutscher Bundestag, 2014)

This speaker stands out in particular as his statements provide one of the few explanations for the emphasis on one societal good over another:

> Freedom is a very important good. It is in fact the most important good of our constitution. There's a reason the enumeration of civil liberties is at the very beginning of our constitution. Manfred Grund, CDU/CSU (Deutscher Bundestag, 2014)

This is one of the clearest examples of a parliamentarian explaining the prioritization of freedom over security. The Grundgesetz serves as a point of reference, since the rights ensuring freedom for the average German citizen are the first to be documented in the constitution. Additionally, a notable moment in parliamentary discourse is brought about when one of the members references the "super fundamental right of security", a term coined by Interior Minister Friedrich, to make the opposing argument:

> In our negotiations and discussions we'll now make it very clear that there is a super fundamental right

> to freedom in the United States as well as here at home, and we'll make it clear that the Federal Government [of Germany] isn't perceiving this affair as being concluded by a long shot. Michael Hartmann, SPD (Deutscher Bundestag, 2014)

The call for freedom isn't particularly surprising given the massive privacy invasions the Snowden revelations brought to light. Nonetheless, while the importance of freedom is invoked, in many cases its absolute value is diluted by mentioning its close relationship with security concerns. The very existence of the freedom v. security framing points to the fact that none of the speakers are disregarding the importance of security as a societal good. This implies a preparedness for concessions and may indicate parliamentary tolerance for non-action on the part of the government.

4.1.2. Digital Sovereignty—The Struggle for Digital Autonomy

With digital sovereignty, we coded one remarkable interpretive scheme through which the current distribution of power in cyberspace and the German dependence on other forces (above all the US) is vehemently challenged. The respective demand is made quite often in parliamentary debate. It is almost always rooted in the context of the EU regulatory framework, in which higher autonomy seems achievable. Hence, speakers mostly call to develop a European digital strategy:

> Ladies and Gentlemen, in light of the excessive data-gathering by the NSA, it is our central task in Germany and Europe to reclaim sovereignty over what is done with our data. We need legal and technical means to do that. Günter Krings, CDU/CSU (Deutscher Bundestag, 2014)

The argument for a renewed sovereignty in the digital realm also points to the problem of the asymmetrical dependence on the US. This dependence is stated explicitly in the following example:

> This is not about IT-nationalism, but if we take an honest look at the situation, we have to admit that we're dependent on US or Asian software and hardware in many instances. We need our own initiatives in the areas of research and development. Lars Klingbeil, SPD (Deutscher Bundestag, 2014)

It is acknowledged that other state actors such as the US and Asian countries possess more resources in the area of digital development, something Germany isn't able to compete with, at least at the moment. Developing the ability to counter these dependencies is given high importance in the wake of the Snowden revelations. The text sequences coded with the digital sovereignty scheme are the ones that most clearly challenge the current relations and practices between Germany and the US regarding security issues and intelligence.

4.1.3. Cyber Angst—The New Level of Threat in the Digital Age

A frequently appearing narrative in both discourses underscores the elevated need for security in reaction to a higher threat level in the digital age affecting both states and citizens. This narrative, which we coded with the term "cyber angst", explores the many potential threats cyberspace poses to a state's security. This includes possible terrorist attacks on critical infrastructure as well as criminal activity in the cyber realm. The narrative serves a securitization logic (Buzan, Waever, & de Wilde, 1998), as it is prone to justifying extraordinary surveillance measures. So-called cyber angst, particularly regarding critical infrastructure, is a crucial narrative in the governmental discourse. It is also found in the parliamentary debate:

> We need online security, especially within the area that's important for our society and country. Communication on a state level must be safe. If we want to uphold critical infrastructure it has to be safe from hacking, attacks and espionage. Hans-Peter Uhl, CDU/CSU (Deutscher Bundestag, 2013a)

4.1.4. Post Privacy—It's a New World

There is another narrative that might serve to reduce the severity and thus lessen the impact of the Snowden revelations within the parliamentary debate. Like cyber angst, it is also rooted in the newness and paradigm-shifts that are ascribed to internet development and the digital era. Cyberspace is depicted by some advocates as such a new and foreign world that some normative prescriptions, as central as they may be, cannot fully apply. This narrative implies that modern societies have moved towards a post-privacy age. Following that argument, the actions of the US government are not justified per se, but the societal norm of privacy that is in danger is depicted as already compromised:

> We shouldn't let citizens believe that they're still safe from espionage if they disclose private matters online. We have to make that clear, especially to young people using Facebook and Twitter among other things. We have to tell them that everything they put online stays there and that there's no digital eraser. That's an illusion. We have to tell people that. Hans-Peter Uhl, CDU/CSU (Deutscher Bundestag, 2013a)

The post-privacy narrative comes with another important implication: the blame for a privacy breach is put not only on firms or state agencies that conduct surveillance, but is also attributed to online users who freely share private information on the internet. The responsibility shifts to citizens, as they are expected to know that information shared online at any time might be the target of corporate or government espionage. Given the overwhelming regulatory demands that internet communication confronts us with, the best line of defense is seen in self-regulation instead of government intervention.

4.1.5. Asymmetrical Dependence in the Security Realm

An effective interpretive scheme that potentially reduces any activism supporting a path-breaking turn in security cooperation with the US is the continued reminder that Germany is highly dependent on US intelligence in security matters. This asymmetrical dependence is brought up many times:

> Every single one of us knows that attacks in Germany were prevented by US intelligence, that's part of the truth of this debate. But we also have to think about how we'll prevent future surveillance. Michael Grosse-Brömer, CDU/CSU (Deutscher Bundestag, 2013b)

This statement addresses a need to prevent surveillance in Germany, while at the same time stating the absolute necessity of US–German cooperation in the security realm to prevent terrorist attacks. This discursive element is the most overt in explaining Germany's continued intelligence and security cooperation with the United States in spite of the Snowden revelations. The bottom line of this logic seems to be that while Germany condemns the surveillance, there simply is no other option to safeguard domestic security apart from cooperating with the US. Additionally, there is an element of gratefulness towards the US for its role in preventing attacks in Germany, which may inhibit harsh criticism of their surveillance activities. One speaker addresses the impossibility of truly faulting the US for its actions while at the same time relying on them for intelligence:

> It won't impress the Americans if we rightly and legitimately criticize their actions in the NSA affair, but at the same time, in Germany and Europe, allow our own defense efforts to erode to the point that we always have to ask for data and insights from the US agencies when things get serious. Günter Krings, CDU (Deutscher Bundestag, 2013b)

If we follow this argument, German officials are in no position to criticize the US for its surveillance activities as they provide the very same intelligence that has kept German citizens safe in the past. The speaker states that even the legitimate criticism will more than likely fall on deaf ears in the US if its allies in Europe take few measures to ensure their own safety and are thus reliant on their partner overseas. The implied solution is the development of intelligence capabilities by Germany and other European states to lessen the dependence on US intelligence and gain some equality in the security relationship and open a dialogue on these matters.

4.2. Refused Need to Act—The Governmental Discourse

4.2.1. The Fundamental Problem—The Tense Relation between Freedom and Security

Explicit reflections on the relationship between security and freedom are even more frequent in the governmental discourse. There are distinct differences to the way parliamentarians discussed it. Representatives in the Bundestag mainly prioritize freedom over security, while government officials talk about security as a transcendental good, i.e. a good without which other goals, including freedom, cannot be achieved:

> Security is the prerequisite for freedom. Hans-Dieter Heumann (Federal Academy for Security Policy, 2015)

When even freedom is seen and depicted as dependent on security, it is not far to the statement of then Minister of the Interior Hans-Peter Friedrich emphasizing security as a "super fundamental law" (Bewarder & Jungholt, 2013). If there can be no freedom without security, the mass surveillance by the US government could even be portrayed as a way of ensuring freedom instead of endangering it. While this is not uttered explicitly, the implications help to understand why meaningful change in cooperative practices with the US is not only regarded as not feasible, but also as not necessary in the end. Furthermore, one governmental document addresses the varying response to the freedom v. security struggle in different countries and puts this down to different historical experiences:

> The balance of freedom and security takes various shapes in different states for historical reasons. (Ministry of the Interior, 2013)

Even though it is only implied here, the idea is that the US surveillance is rooted in historical experiences that make them more likely to come down on the side of security, particularly the terrorist attacks of 9/11. This is a sympathetic view that seeks to somewhat justify US intelligence activities, as they have been employed after a traumatic event that would cause a state to be hypervigilant in security matters.

4.2.2. Digital Sovereignty—The Struggle for Digital Autonomy

Standing in contrast to the other recurrent elements, demands for digital autonomy or sovereignty are articulated in a clearer fashion within the governmental discourse than in the parliamentary debate. The idea that Germany must achieve a sort of digital sovereignty—

mostly in cooperation with the EU—to break free of US influence was supported even by the German Minister for the Interior de Maizière:

> Our political leverage is significantly defined by our technological capabilities. Therefore, we have to do everything possible to maintain IT capabilities in order to keep and further build our own technological platforms….The government is going to develop a strategy to secure national competitiveness. I've already said that this is a modern form of patriotism. Thomas de Maizière (Ministry of the Interior, 2014a)

In this speech, de Maizière also emphasized that the EU is crucial to achieving this goal. This also shows that even though the need for independence from US cooperation is acknowledged, Germany is not seen as being capable of achieving this goal alone, i.e. outside of the cooperative framework of the EU. The idea of building a European counterbalance to US hegemony in digital matters is one of the few ways in which the Snowden revelations seem to have had a disruptive effect on US–German cooperation.

4.2.3. Cyber Angst—The New Level of Threat in the Digital Age

The narrative that cyberspace is exposing states and their citizens to a higher level of risk is much more frequently used in the governmental discourse than in parliament. There are also differences in the way how it is told. Moreover, the implied claims are presented with much more certainty as are the derived solutions:

> A stable, secure, open and free internet offers great opportunities: for economic growth and development, for good governance and democracy, as well as for social exchange between people around the world. At the same time, it confronts us with new threats: Numerous states are pursuing military cyber-capabilities, which might lead to an atmosphere of mutual distrust and conflict. Private actors have shown great skill in abusing the net for criminal purposes. Terrorists have been using the internet for their means. Norbert Riedel (Ministry of Foreign Affairs, 2015a)

This quote offers insight into the way this particular narrative unfolds. While some positive effects of the cyber age are acknowledged, the dangers posed by this new way of dealing with the world are exposed at the same time. In this instance, two different kinds of threats are addressed: the atmosphere of distrust created by this new way states can attack each other and the possibility of terrorists and criminals using the internet for their own purposes. In its entirety, this narrative creates an atmosphere of fear and implicitly justifies using extraordinary means—e.g. mass surveillance—to ensure the security of a state or society. This comes down to a securitization logic with government officials as the prime securitizing agents (Buzan et al., 1998).

4.2.4. Post Privacy—It's a New World

While the cyber angst narrative is more important for the governmental discourse than for the parliamentary one, the opposite is true of the narrative according to which cyberspace has brought about a kind of post privacy era, as it is much less prominently represented in governmental discourse than it is in the parliamentary debate. Nevertheless, the narrative is employed as well:

> In a changing world that requires answers for the continued digitalization of our society and newly developing areas of organization, we cannot simply fall back on our ordinary patterns of behavior and keep rigid systems that don't live up to the challenges of this day and age. Norbert Riedel (Ministry of Foreign Affairs, 2015b)

In this instance, the narrative of cyberspace as a new frontier is used to challenge the outdated strategies used to deal with these new circumstances. From this perspective, a more extreme argument would be possible by which the revealed mass surveillance of the NSA is seen as a coping technique employed to deal with the new challenges cyberspace poses to states and their governments.

4.2.5. Asymmetrical Dependence in the Security Realm

In contrast to the previous example, there is not much difference in how the idea of an asymmetrical security relationship between Germany and the US appears in governmental and parliamentary discourses. Rather, this seems to be more or less common sense:

> The United States is our most important partner and our closest ally. The security cooperation with our US partners is irreplaceable in regards to our domestic and external security. That's especially true for the fight against terrorism. This is the reason we want to continue and deepen our cooperation. Thomas de Maizière (Ministry of the Interior, 2014b)

The demand in this quote from Minister of the Interior de Maizière is very clear: given the high dependence of German security on US intelligence information, there is no other option to guarantee the security of Germany than to continue the close security cooperation with the US. He even goes further by expressing a desire to deepen the already existing cooperation instead of reducing it. The way de Maizière frames the cooperation doesn't imply that it is a necessary evil brought about by Germany's own lack of intelligence capabilities in certain areas. On the contrary, he explicitly names the US as the closest partner and ally, a role that German government officials apparently take no objection to even in the wake of the Snowden revelations. Considering how the actions of the US government have widely been interpreted as a betrayal of its allies, this hints at a relationship that runs very deeply indeed.

5. Conclusion

Considering the outrage the Snowden revelations provoked in German public discourse, one could have expected that politicians would react to it with a bundle of measures to reform policies, institutions and practices in the security realm. From this perspective, it seemed likely that especially the close security cooperation with the US would be restrained by more privacy-sensitive regulation in this field. However, as we all know by now, the consequences of the Snowden revelations for the German–US intelligence collaboration have been few and far between. Security cooperation with the US remained stable most of the time, and the government even extended the capabilities of German intelligence agencies with a new legal framework for foreign surveillance. The reforms that have been carried out are rather symbolic in nature, but some even legalize the revealed practices instead of trying to forbid them. This discrepancy between public statements and government action is the puzzle that our research started with. We approached the problem with a discourse analytical framework. Relying on the Sociology of Knowledge Approach to Discourse, we comparatively analyzed parliamentary and governmental discourses in Germany after the Snowden revelations.

In our empirical sections, we identified five recurrent elements that could be found in parliamentary and governmental discourses that facilitated the reluctant reactions in different ways. The first one included all general and/or explicit reflections on the tense fundamental relationship between freedom and security and is thus rather indifferent regarding the expected consequences; the debate seems to favor neither side overwhelmingly and an absolute call for security is rarely made. Additionally, we found a push for digital sovereignty or autonomy which clearly effected a change of practice with the German government canceling its contract with Verizon. While this element certainly influenced the move away from a contractor based in the US, the dependencies addressed also include concerns about Asian companies, therefore leading to more nuanced thoughts about which dependencies might be less problematic and how to avoid them altogether.

While the two elements mentioned above can potentially either increase or decrease cooperation with the US, we also found three recurrent elements which all serve to reduce the perceived severity of the NSA scandal and thus prevent more resolute efforts to reduce cooperation with the US. The first one we called cyber angst. This element expresses a diffuse anxiety about the new threats in our increasingly digital world. Fears are stoked about state and non-state actors using cyberspace to forward their (malicious) goals at the expense of German society, leading to calls for a more active state response and more cooperation among trusted allies. The second element consists of post-privacy narratives. These focus on the distinct newness of cyberspace and argue that standards established in the offline world might not be suitable for the digital world; far reaching surveillance measures may eventually be normal conduct in the new medium. Furthermore, the state might not be the most dangerous actor in this field after all, since big companies are also engaged in extensive data collection. A reluctant response was further facilitated by the argument of asymmetrical dependence. This element emphasizes the German dependence on the US in the realm of security policy. Proponents of this argument stress the fact that cooperation with US intelligence agencies helps to protect German citizens. This is often combined with a reference to the important role the US has played in German history. It is argued that even if surveillance might be problematic, the US is not the most dangerous threat to Germany, since there are far more problematic actors that need to be countered. This argument thereby also seamlessly connects to the cyber angst narratives.

All in all, given the initial public outrage, the alleged Snowden effect seems to have diminished over time through an apparent cascade in sequential logic in the public discussions examined here. We could identify a considerable difference between the discourses in parliament and government. The need for change or stronger regulation seems reduced already by what is said and argued in the parliamentary debates. Any call for a considerable regulation that might cause a disruption in German–US security cooperation is almost completely disregarded in the governmental discourse.

Acknowledgements

We acknowledge financial support by Deutsche Forschungsgemeinschaft and Ruprecht-Karls-Universität Heidelberg within the funding programme Open Access Publishing.

Conflict of Interests

The authors declare no conflict of interests.

References

Bäcker, M. (2016). Stellungnahme zu dem Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes. *Deutscher Bundestag*. Retrieved from http://www.bundestag.de/blob/459630/1ddfe2451c0fd067872976d0f0467882/18-4-653-g-data.pdf

Balzacq, T. (2011). A theory of securitization. Origins, core assumptions, and variants. In T. Balzacq (Ed.), *Securitization theory. How security problems emerge and dissolve* (pp. 1–30). London: Routledge.

Bersick, S., Christou, G., & Yi, S. (2016). Cybersecurity and EU–China relations. In. E. J. Kirchner, T. Christiansen, & H. Dorussen (Eds.), *Security relations between China and the European Union* (pp. 167–186). Cambridge: Cambridge University Press.

Bewarder, M., & Jungholt, T. (2013, July 16). Friedrich erklärt Sicherheit zum "Supergrundrecht". *Welt*. Retrieved from https://www.welt.de/politik/deutschland/article118110002/Friedrich-erklaert-Sicherheit-zum-Supergrundrecht.html

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Rienner.

Connolly, K. (2015, May 7). German secret service BND reduces cooperation with NSA. *The Guardian*. Retrieved from https://www.theguardian.com/world/2015/may/07/german-secret-service-bnd-restricts-cooperation-nsa-us-online-surveillance-spy

Deutscher Bundestag. (2013a). Stenografischer Bericht 249. Sitzung Berlin, Mittwoch, den 26. Juni 2013. *Deutscher Bundestag*. Retrieved from http://dip21.bundestag.de/dip21/btp/17/17249.pdf

Deutscher Bundestag. (2013b). Stenografischer Bericht 2. Sitzung Berlin, Montag, den 18. November 2013. *Deutscher Bundestag*. Retrieved from http://dip21.bundestag.de/dip21/btp/18/18002.pdf

Deutscher Bundestag. (2014). Stenografischer Bericht 7. Sitzung Berlin, Mittwoch, den 15. Januar 2014. *Deutscher Bundestag*. Retrieved from http://dip21.bundestag.de/dip21/btp/18/18007.pdf

Deutscher Journalisten-Verband. (2016, September 16). BND-Gesetz. Kein Schutz für Journalisten. *Deutscher Journalisten-Verband*. Retrieved from http://www.djv.de/startseite/profil/der-djv/pressebereich-download/pressemitteilungen/detail/article/kein-schutz-fuer-journalisten.html?cHash=cad80f8c0f4108ced1be30a704676f24&type=500

Federal Academy for Security Policy. (2015). Cyber-Realität zwischen Freiheit und Sicherheit. *Federal Academy for Security Policy*. Retrieved from https://www.baks.bund.de/en/node/513

Federal Chancellery. (2016). Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes. *Bundeskanzleramt*. Retrieved from https://www.bundesregierung.de/Content/DE/_Anlagen/2016/06/2016-06-28-entwurf-bnd-gesetz.pdf?__blob=publicationFile&v=1

Federal Government. (2013). Deutschland ist ein Land der Freiheit. *Bundesregierung*. Retrieved from https://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html;jsessionid=FA5B3F77DAD45E2755C7E47F46DED066.s7t2?nn=437032#Start

Foucault, M. (2002). *Archaeology of knowledge*. London and New York, NY: Routledge.

Gabrielatos, C. (2007). Selecting query terms to build a specialized corpus from a restricted-access database. *ICAME Journal*, *31*, 5–43.

Gorr, D., & Schünemann, W. J. (2013). Creating a secure cyberspace: Securitization in Internet governance discourses and dispositives in Germany and Russia. *International Review of Information Ethics*, *20*(12), 37–51.

Hajer, M. A. (2002). Discourse analysis and the study of policy making. *European Political Science*, *2*(1). Retrieved from http://www.maartenhajer.nl/upload/Hajer%20EPS.pdf

Howarth, D., Norval, A. J., & Stavrakakis, Y. (Eds.). (2000). *Discourse theory and political analysis. Identities, hegemonies and social change*. Manchester: Manchester University Press.

Hudson, A. (2014, June 26). German government cancels Verizon contract in wake of U.S. spying row. *Reuters*. Retrieved from http://www.reuters.com/article/us-germany-security-verizon-idUSKBN0F11WJ20140626

Keller, R. (2007). *Diskursforschung. Eine Einführung für SozialwissenschaftlerInnen*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Keller, R. (2008). *Wissenssoziologische Diskursanalyse. Grundlegung eines Forschungsprogramms*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Keller, R. (2013). *Doing discourse research: An introduction for social scientists*. London: SAGE Publications.

Mascolo, G. (2016, January 8). BND und NSA kooperieren wieder in Bad Aibling. *Süddeutsche Zeitung*. Retrieved from http://www.sueddeutsche.de/politik/abhoerskandal-bnd-und-nsa-kooperieren-wieder-in-bad-aibling-1.2810828

Meister, A. (2016, June 30). Das neue BND-Gesetz—Alles, was der BND macht, wird einfach legalisiert und sogar noch ausgeweitet. *Netzpolitik.org*. Retrieved from https://netzpolitik.org/2016/das-neue-bnd-gesetz-alles-was-der-bnd-macht-wird-einfach-legalisiert-und-sogar-noch-ausgeweitet/

Ministry of Foreign Affairs (2015a). Rede des Beauftragten für Cyber-Außenpolitik, Botschafter Dr. Norbert Riedel, bei der Tagung der Freedom Online Coalition in Ulan Bator (Mongolei). *Ministry of Foreign Affairs*. Retrieved from http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2015/150504-Riedel_Freedom_Online_Coalition_Conference.html

Ministry of Foreign Affairs (2015b). Es braucht neue Regeln fürs Internet—Deutschland und Brasilien im Einsatz für Privatsphäre und Sicherheit. *Ministry of Foreign Affairs*. Retrieved from http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Interviews/2015/150330_Cyber_Privatsphaere.html

Ministry of the Interior. (2013, August). Maßnahmen für einen besseren Schutz der Privatsphäre. Fortschrittsbericht vom 14. August 2013. *Ministry of the Interior*. Retrieved from http://www.bmwi.de/BMWi/Redaktion/PDF/ST/massnahmen-fuer-einen-besseren-schutz-derprivatsphaere,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

Ministry of the Interior. (2014a). Schutz—Sicherheit—Vertrauen Auftrag der Politik im digitalen Zeitalter. *Ministry of the Interior*. Retrieved from http://www.

protokoll-inland.de/SharedDocs/Reden/DE/2014/06/dud.html

Ministry of the Interior. (2014b). Rede von Bundesinnenminister de Maizière anlässlich des 11. Symposiums des Bundesamtes für Verfassungsschutz am 8. Mai 2014 in Berlin. *Ministry of the Interior*. Retrieved from http://www.bmi.bund.de/SharedDocs/Reden/DE/2014/05/bfv-symposium.html

Organization for Security and Co-operation in Europe. (2016). Surveillance amendments in new law in Germany pose a threat to media freedom, OSCE Representative says, asks Bundestag to reconsider bill. *Organization for Security and Co-operation in Europe*. Retrieved from http://www.osce.org/fom/252076

Papier, H.-J. (2016). Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten. *Neue Zeitschrift für Verwaltungsrecht*, *35*(15), 1–15.

Sabatier, P. A. (1988). An advocacy coalition framework of policy change and the role of policy-oriented learning therein. *Policy Sciences*, *21*(2/3), 129–168.

Schulze, M. (2015). Patterns of surveillance legitimization. The German discourse on the NSA scandal. *Surveillance & Society*, *13*(2), 197–217.

Segal, A. M. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. New York, NY: PublicAffairs.

Smale, A. (2013, October 23). Anger growing among allies on U.S. spying. *New York Times*. Retrieved from http://www.nytimes.com/2013/10/24/world/europe/united-states-disputes-reports-of-wiretapping-in-Europe.html?_r=0

Troianovski, A., Gorman, S., & Torry, H. (2013, October 24). European leaders accuse U.S. of violating trust. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB100014240527023047994045791950188871722

United Nations. (2013). Resolution 68/167. *United Nations*. Retrieved from. http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

United Nations. (2016). *Stellungnahme*. Retrieved from https://netzpolitik.org//wp-upload/2016/09/160829_Stellungnahme_UN-Sonderbeauftragte_zur_BND-Reform.pdf

Wetzling T. (2016). Stellungnahme zum Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BND) sowie weiterer Vorlagen. *Deutscher Bundestag*. http://www.bundestag.de/blob/459622/a6a22e212bb9c777028554ed1ba4bbfc/18-4-653-c-data.pdf

Wodak, R., & Krzyzanowski, M. (Eds.). (2008). *Qualitative discourse analysis in the social sciences*. Basingstoke: Palgrave Macmillan.

Xiao Wu, A. (2012). Hail the independent thinker. The emergence of public debate culture on the Chinese internet. *International Journal of Communication*, *6*, 2220–2244.

About the Authors

Stefan Steiger, MA, is a research fellow and doctoral student at the Institute of Political Science of the University of Heidelberg. His main fields of interest are cyber security, internet governance and foreign policy analysis.

Wolf J. Schünemann, Dr., is Junior Professor of Political Science at Hildesheim University. His main fields of interest are internet governance, political online communication, European integration and discourse studies.

Katharina Dimmroth, MA, is a research fellow at the Institute of Political Science of RWTH Aachen University. Her main fields of interest are US and German foreign policy, cyber security and international relations.

COGITATIO

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 17–28
DOI: 10.17645/mac.v5i1.821

Article

Intelligence Reform and the Snowden Paradox: The Case of France

Félix Tréguer

Center for International Studies and Research, Sciences Po, 75006 Paris, France; E-Mail: felix.treguer@sciencespo.fr

Submitted: 10 November 2016 | Accepted: 26 January 2017 | Published: 22 March 2017

Abstract
Taking France as a case study, this article reflects on the ongoing legalisation strategies pursued by liberal states as they seek to secure and expand the Internet surveillance programs of their domestic and foreign intelligence agencies. Following the path to legalisation prior and after the Snowden disclosures of 2013, the article shows how post-Snowden controversies helped mobilise advocacy groups against the extra judicial surveillance of Internet communications, a policy area which had hitherto been overlooked by French human rights groups. It also points to the dilemma that post-Snowden contention created for governments. On the one hand, the disclosures helped document the growing gap between the existing legal framework and actual surveillance practices, exposing them to litigation and thereby reinforcing the rationale for legalisation. On the other hand, they made such a legislative reform politically risky and unpredictable. In France, policy-makers navigated these constraints through a cautious mix of silence, denials, and securitisation. After the Paris attacks of January 2015 and a hasty deliberation in Parliament, the Intelligence Act was passed, making it the most extensive piece of legislation ever adopted in France to regulate secret state surveillance. The article concludes by pointing to the paradoxical effect of post-Snowden contention: French law now provides for clear rules authorising large-scale surveillance, to a degree of detail that was hard to imagine just a few years ago.

Keywords
contentious politics; intelligence; internet; securitisation; Snowden; surveillance

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).

1. Introduction

In January 2008, a meeting took place in the office of then President of France, Nicolas Sarkozy, at the Élysée Palace. In front of him sat Prime Minister François Fillon and the Director of the *Direction Générale de la Sécurité Extérieure* (DGSE, France’s foreign intelligence agency) Pierre Brochand, as well as a few of their staff.

Brochand had come with a plea. France, he explained, was on the verge of losing the Internet surveillance arms race. From the 1980’s on, French intelligence services had managed to develop top notch communications intelligence (COMINT) capabilities, thanks to a network of intercept stations located across metropolitan France and overseas territories, sometimes in partnership with the German *Bundesnachrichtendienst*, or BND. But as almost all of the world’s communications were now travelling on IP based networks, the DGSE was losing ground on its main partners and competitors—in particular the National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ)

France had some serious catching up to do, but it also had important assets. First, its geographic location, with almost two dozen submarine cables landing on its shores, both in Brittany, Normandy and the Marseilles area. Second, its engineering elite state schools and high tech firms—not least of which submarine cable operators Alcatel and Orange as well as surveillance technology provider Qosmos—, which could provide the technical know-how necessary to carry on this ambitious project.

Sarkozy was hesitant at first. The plan was very costly and its legality more than dubious. The French legal basis for communications surveillance dated back to 1991. Another issue was that of cost. At the time, the 2008 financial crisis had yet to unleash, but the government was already facing recurring deficits and it needed to contain public spending.

But Pierre Brochand and its supporters in the President's staff turned out to be convincing. Sarkozy eventually agreed to move forward with the proposed plan: Over the course of the next five years, the DGSE would get the €700 million it needed to upgrade its surveillance capabilities and hire over 600 staff to work in its Technical Directorate (the number of DGSE employees was then 4,440). Only six months later, near Marseilles, the first of the new intercept stations was up and running, doubling up the traffic coming from international cables, filtering it and transmitting it to the DGSE's headquarters in Paris.

How do we even know about this meeting? We owe this account to journalist Vincent Jauvert, who revealed its existence in a French weekly magazine on July 1st 2015, at the very end of the parliamentary debate on the 2015 Intelligence Bill (Jauvert, 2015). According to former high ranking officials quoted by Jauvert, these efforts paid off: "When we turned on the faucet, it was a shock! All this information, it was unbelievable!" All of sudden, France was back in the game. To such an extent that, a few months later, in 2009, the NSA even offered to make the DGSE a member of the exclusive Five Eyes club.

Apparently, the "Sixth Eye" deal failed over the Central Intelligence Agency's (CIA) refusal to conclude a no-spy agreement with France, and in 2011, a more modest cooperation was eventually signed between the NSA and the DGSE under the form of a memorandum—most likely the so-called LUSTRE agreement revealed in 2013 by NSA whistleblower Edward Snowden (Follorou, 2013). Another agreement was struck in November 2010 with the British GCHQ.

Jauvert's report connected many pieces of information of what was—and still remains—a puzzle. By then, a few public statements by intelligence officials had already hinted at the formidable growth of the DGSE's Internet surveillance capabilities. The Snowden documents and a handful of investigative reports had also given evidence of France's rank in the world of COMINT. However, for the first time, we were able to get a sense of some of the political intricacies and secret negotiations that presided over the rise of the most significant Internet surveillance program developed by French agencies, as well as their geopolitical outcomes.

But his report also raised questions: If the plan agreed upon at the Élysée Palace in January 2008 was so successful, why did the new French administration wait until the Spring of 2015 to "go public" by presenting the Intelligence Bill aimed at legalising this large-scale surveillance program?

The goal of this paper—adapted from a longer research report (Tréguer, 2016a)—is to study the process of legalisation of Internet surveillance capabilities, taking France as a case study to analyse the impact of post-Snowden contention on the techno-legal apparatus of surveillance, one that has become deeply embedded in the daily routine of security professionals in domestic and transnational security fields.

To provide an empirical analysis of this process of legalisation, the article uses the methodological toolbox of contentious politics, a sub-field of political sociology (Tilly & Tarrow, 2015). It first looks at historical antecedents of legalisation and contention around communications surveillance in France. By providing a content analysis of recent investigative reports and policy documents to shed light on a policy domain veiled in secrecy, the paper points to the growing gap between secret surveillance practices and the law prior to the Snowden disclosures of 2013. It then turns to the impact of these leaks and the resulting episodes of contention for the strengthening of privacy advocacy in France, its chilling effect on legalisation, as well as the role of the terrorist threat and associated processes of securitisation in the adoption of the Intelligence Act of 2015.

While calling for cross-country comparisons of intelligence reforms passed by liberal regimes since 2013, this case study concludes by suggesting that, rather than helping restore the rule of law, post-Snowden contention might paradoxically contribute to reinforcing illiberal trends towards the circumvention of procedural and substantive human rights safeguards, while strengthening the executive power's ability to "rule by law" (Tarrow, 2015, p. 162).

2. Before Snowden, Legalisation Was Underway

As many of its counterparts, France has a record of surveillance scandals. In 1974, a project by the Interior Ministry—aimed at building a huge database gathering as much information as possible on its citizens—sparked a huge outcry, after an unidentified engineer working on the project blew the whistle by speaking to the press (Joinet, 2013). The "SAFARI affair", named after the codename of the project, played an important role in the adoption of the French personal data protection framework in 1978 (Fuster, 2014).

2.1. The Wiretapping Act of 1991: An Antecedent of Legalisation

In 1991, following two condemnations by the European Court of Human Rights (ECHR) pointing to the lack of detailed provision surrounding both judicial and administrative wiretaps, the government rushed to Parliament to pass the Wiretapping Act, which provided the first comprehensive legal framework regulating the surveillance of telephone communications (Errera, 2003).

In the early 1990's, the prospect of Internet surveillance was of course still very distant, and the law was drafted with landline and wireless (satellite in particular) telephone communications in mind. So when tapping into Internet traffic became an operational necessity for intelligence agencies at the end of the 1990's, its legal basis was progressively hinged on secret and extensive interpretations of existing provisions (one notable exception was a 2006 statute which authorised administrative access to metadata records for the sole purpose of anti-terrorism) (Tréguer, 2016b). Such was the case of the DGSE's large-scale Internet surveillance programme launched in 2008, and apparently backed by a provision of the 1991 Wiretapping Act that gave a blank check to the DGSE to conduct bulk interceptions of so-called "Hertzian transmissions" without any oversight.

French officials looking back at these developments have often resorted to euphemisms, talking about a zone of "a-legality" to describe this secret creep in surveillance capabilities (e.g. Follorou & Johannès, 2013). Although "a-legality" may be used to characterise the legal grey areas in which citizens operate to exert and claim new rights that have yet to be sanctioned by either the parliament or the courts—for instance the disclosure of huge swathes of digital documents (Tréguer, 2015)—it cannot adequately qualify these instances of legal tinkering by secret bureaucracies that seek to escape the safeguards associated with the rule of law. Indeed, when the state interferes with civil rights like privacy and freedom of communication, a detailed, public and proportionate legal basis authorising them to do so is required by supranational courts like the ECHR. Otherwise, such interferences are, quite plainly, illegal.

2.2. Legal Insecurity as a Driver for Legalisation

Secret legal interpretations are, of course, a common feature in the field of surveillance (Rubinstein, Nojeim, & Lee, 2014), and the extralegal regulation of Internet communications has become increasingly common among liberal regimes (Benkler, 2011; Tréguer, 2015). In France, as we will see, they could prosper all the more easily given the shortcomings of human rights advocacy against Internet surveillance. But even so, French national security policy-makers began to worry that the existing framework failed to comply with the standards of the ECHR.

In July 2008, six months after the launch of the DGSE's large-scale Internet surveillance program, the government released the *White Paper of Defence and National Security*—a major effort of strategic planning conducted under Sarkozy's presidency. This official policy document claimed, for what appears to be the first time, that intelligence legislation would soon be presented to Parliament:

> Intelligence activities do not have the benefit of a clear and sufficient legal framework. This shortcoming must be corrected. A new legal architecture will define the duties of intelligence agencies, safeguards for both their personnel and human sources, as well as overarching rules for the protection of classified information. Legislative amendments will be provided, while respecting the balance between the protection of civil rights, the effectiveness of judicial proceedings and the protection of secrecy. (French Government, 2008, p. 142)

The document added that "the consultation of metadata and administrative databases…will be enlarged".

But the following September, a major scandal erupted around the adoption of a decree authorising a very broad intelligence database—named EDVIGE—for domestic surveillance purposes. Within a few weeks, a widespread civil society mobilisation against the decree led the government to backtrack (Marzouki, 2009). It marked one of the biggest episodes of human rights contention under Sarkozy's presidency and was apparently enough to put the government's broader plans for modernising intelligence law to rest until the end of its mandate.

What a conservative, "tough-on-security" government could not achieve would eventually be pursued and carried out by a left-of-center, supposedly pro civil rights party. By the time the Socialist Party returned to power in 2012, its officials in charge of security affairs were the ones pushing for a sweeping reform that would legally secure the work of people in the intelligence community and, incidentally, put France in line with democratic standards (which require a public and detailed legal basis for the surveillance activities of intelligence agencies).

One man played an important role in this process: Jean-Jacques Urvoas, a long-time proponent of intelligence reform in the Socialist Party, who became Minister of Justice in early 2016. After the 2012 elections, Urvoas was re-elected to the National Assembly and awarded with the prestigious position of President of the Committee on Legal Affairs. This also made him a de facto member of the Parliament's Committee on Intelligence, sealing his membership to the small circle of intelligence policy-makers. Mid-May 2013—just two weeks before the first Guardian article based on the Snowden files—, Urvoas presented a 200-page-long bipartisan report on the "evolution of the legal framework of intelligence services" (Urvoas & Verchère, 2013). In one section entitled "Tomorrow, a Condemnation by the ECHR?", the report provided an overview of the court's case law and insisted that:

> In France, for lack of legislation adapted to certain aspects of their activities, intelligence services are forced to act outside of any legal framework…. The interception of communication, the listening of places and the tapping of images violate the right to private life, as do the geo-localisation of a phone or of a vehicle…. Concretely, France is risking a condemnation by the European Court of Human Rights for violating the European Convention on Human Rights. For the time being, no legal challenge has been introduced against intelligence-related activities, but there is a constant risk of condemnation. (p. 31)

Recalling the ECHR 1990 rulings against France, the section ended with an invitation to engage in an intelligence reform based on a careful analysis of the ECHR case law in the field of secret surveillance. But despite this acknowledgement that intelligence agencies had been engaging in illegal surveillance, there was no reaction from human rights groups.

3. After Snowden, Legalisation Sparked Contention

While the global anti-surveillance contention unleashed by Snowden reinforced intelligence policy-makers' rationale for legalisation by documenting surveillance practices to litigation, it also made such reform more exposed to public scrutiny and therefore politically riskier. However, probably comforted by the fact that French privacy advocates had traditionally overlooked the issue of Internet surveillance, policy-makers nevertheless gave it a try. In late 2013, a first attempt at partial legalisation was introduced, eventually giving rise to new alliances among advocacy groups.

3.1. Initial (Lack of) Contention

Initially, the reaction of the French civil society to the Snowden disclosures—the first of which appeared in a Guardian article on June 5th 2013—was relatively mild.

Like in the US, the UK, Germany, and other countries, there was of course widespread media coverage of the Snowden affair in June, July and August of that year (see Figure 1).

Many French Non Governmental Organisations (NGOs) active in the field of human rights joined the media frenzy. Some international organisations with presence in France, like Amnesty or Human Rights Watch, were able to get traction from the initiatives launched elsewhere, occupying the French public sphere by translating press releases targeting the US and the UK agencies. Digital rights organisations working on the overhaul of the EU framework for data protection, like *La Quadrature du Net* (LQDN), mentioned Snowden in passing in their public communications on the matter, but because they were busy working on the proposed EU regulation on data protection, they targeted the data collection practices of Internet firms rather than state surveillance (LQDN, 2013). The only notable exception to this relative apathy was the *Fédération Internationale des Droits de l'Homme* (FIDH), the worldwide movement for human rights founded in 1922, which filed a criminal complaint against NSA's PRISM program and appealed to the UN Special Rapporteur for Freedom of Expression, calling for an investigation into the facts revealed by Snowden (FIDH, 2013).

However, despite the recent Urvoas report hinting at the discrepancy between surveillance practices of French agencies and the law, none of these groups sought to turn the Snowden scandal into an opportunity to call, say, for an independent review of the DGSE's capabilities, or bring new privacy safeguards to a legal framework that was visibly outdated. How can we explain such lack of substantive contention?

3.2. Denials as Legitimisation Strategies

For one, even in activist circles, there was a feeling that the whole affair was mostly related to the NSA and the GCHQ, not to French agencies. In this regard, the legitimation strategies of policy-makers, which denied that French agencies were engaging in the same practices as their Five Eyes counterparts—a strategy also observed in Germany (Schulze, 2015)—, were successful. But even more than denials, it was a no-comment policy that dominated the French government's response to the unfolding scandal.

One notable exception to this wall of communication was Urvoas. On June 12th, in *Le Monde*, the then-member of Parliament refuted that French agencies were conducting large-scale surveillance of Internet communications, claiming:

> I have never heard of tools that could be associated to what the Americans use, and every time I asked intelligence officials, I got a negative answer. (Chapuis, 2013)

But two weeks later, on July 4th, Le Monde ran a piece by reporter Jacques Follorou on the "French Big Brother", claiming that France was "doing the same thing" as the NSA:

> *Le Monde* is able to reveal the General Directorate for External Security (DGSE, special services) systematically collects electromagnetic signals coming from computers or telephones in France, as well as traffic between French and foreigners: the totality of our communications is being spied upon. All emails, SMS, telephone records, connections to Facebook, Twitter, are then stored for years. (Follorou & Johannès, 2013)

The report also quoted a high-ranking intelligence official arguing that these practices were "alegal" (i.e. in a legal

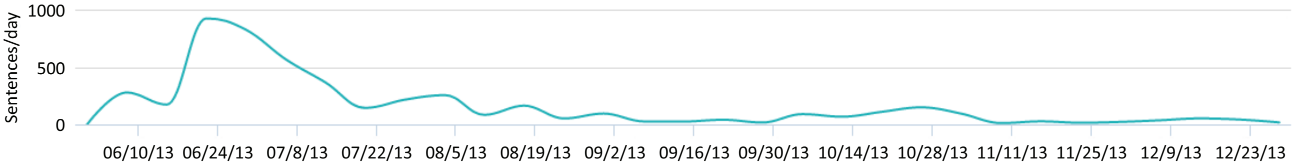


Figure 1. Number of sentences per day mentioning the term "Snowden" in national online news sources in France (based on 129 media sources) from June 2013 to January 2014. Source: MediaMeter.

grey area) rather than illegal (for lack of any public and detailed legal basis).

Considering what we now know about the DGSE's Internet surveillance programs and given also the provision of the 1991 Wiretapping Act allowing bulk collection of wireless communications, the article could have triggered a new scandal, directly aimed at French agencies. But because its sensationalist tone and several inaccuracies—most importantly the fact that it was technically infeasible for the DGSE to collect the "totality" of French communications—, it appeared overblown and was easily dismissed.

Once again, Urvoas was one of the only officials to comment. He immediately published a blog post refuting these allegations, using what would become a favoured metaphor in intelligence circles to distinguish French agencies from the NSA:

> In comparison to the NSA, a technical agency dedicated only to interceptions, the DGSE is a non-specialised agency collecting intelligence for the sole purpose of complying with its regulatory duties. We could thus say that, against the 'fishing trawls' that the NSA seems to be operating, the DGSE is conducting "harpoon fishing" as part of its prerogatives. (Urvoas, 2013a)

But the dismissal of *Le Monde*'s account did not only come from policy-makers. Jean Marc Manach, a journalist, surveillance expert and privacy advocate, also bemoaned the paranoid tone of *Le Monde*'s journalists (Manach, 2013). He also stressed that many of *Le Monde*'s claims, which quoted some of his own reports on the DGSE's so-called "Frenchelon" program, were in fact not new and had been documented before.

Manach was right. By then, officials from the DGSE had already hinted at the formidable growth of the agency's Internet surveillance capabilities. In 2010, its Chief Technology Officer, Bernard Barbier, who was then supervising the plan agreed upon in Sarkozy's office two years earlier, boasted during a public talk before the Cryptographers' Reserve that France was in the "first division" of communications intelligence. He also revealed that the Internet was now the DGSE's "main target" (Manach, 2010). Then, in March 2013, just a few weeks before the beginning of the Snowden disclosures, the head of the DGSE was even less equivocal, admitting before the National Assembly that, since 2008, "we have been able to develop a significant plan for the surveillance of Internet traffic" (French National Assembly, 2013).

3.3. Advocacy Failure

This, in turn begs the question of why, in the immediate aftermath of the Snowden disclosures and even prior to that, it took so long for human rights groups in France to pick up on the pieces of information already available and go after these illegal surveillance operations, both in courts and in policy-making arenas.

The question is a complex one, and cannot be fully addressed here. But two aspects deserve to be mentioned. First, regarding strategic litigation, it is worth noting that in the French civil law system, legal opportunities have traditionally been lacking (Meili, 1998), especially in a field such as state surveillance covered by state secrets. Statements by officials are not enough to initiate legal action. In other countries like the US, they might help trigger successful "FOIA requests" (named after the 1966 Freedom of Information Act) (Schulhofer, 2015). In France however, the national "freedom of information" law adopted in 1978 has extremely broad national security exemptions and is generally much weaker (for instance, the request must specify the exact name of the documents sought after, which represents a formidable hurdle in policy areas covered by state secrets) (Chevallier, 1992).

Second, and more importantly, the lack of mobilisation prior and in the immediate aftermath of the first Snowden disclosures speaks about the structural weaknesses of online privacy advocacy in France, at least until late 2013. Even when in October 2013, thanks to the Snowden trove, *Le Monde* revealed the existence of the so-called LUSTRE data-sharing agreement between the NSA and the DGSE, showing that the latter sent millions of metadata records daily to the US agency (Follorou, 2013), human rights advocacy groups did not pick up on the issue.

A few hypotheses, based on observant-participation conducted in this advocacy field, can be offered to explain these structural weaknesses. Though there have been recent and successful episodes of contention against offline surveillance and intelligence files, Internet surveillance has mostly remained out of the focus of large human rights organisations and smaller digital rights groups in the past decade, which may be due to the particular interests of their staff and subsequent prioritisation in handling their limited resources. Also, a general knowledge of the field in the US, the UK or Germany suggests that historical factors, more recent legalisation processes and leaks regarding Internet surveillance programs likely played an important role in helping civil society groups in these countries maintain stronger networks and expertise.

One major moment of the transnational post-Snowden contention, for instance, was the release of the "International Principles on the Application of Human Rights to Communications Surveillance" in May 2014 (EFF, 2014). Although framed as a key response of the global civil society to the Snowden controversies, the work on this text started as early as 2012 and, as noted in the document, "more than 40 privacy and security experts participated in the drafting process". However, according to one interview conducted for this article with a lawyer who played a major role in the drafting of this document, there wasn't any French national among them. This tends to confirm that, until recently, French NGOs had remained outside of these transnational networks working on state surveillance.

3.4. Legalisation of Metadata Access Sparks Contention

These structural weaknesses of anti-surveillance advocacy in France help explain why intelligence policymakers would try to legalise very intrusive metadata access powers as early as October 2013, in the midst of the Snowden scandal.

In 2006, a law had been adopted to give intelligence agencies access to metadata records held by access providers and hosting providers, but only for fighting terrorism. What is more, from 2009 on, intelligence agencies had apparently experimented with traffic-scanning devices provided by Qosmos and installed on the infrastructure of the few major telecom operators to monitor metadata in real-time (Hourdeaux, 2016; Reflets.info, 2016).

Already in late-2012, it was becoming clear to intelligence policy experts that—in line with what had already been alluded to in the 2008 White Paper of Defence—these crucial capabilities for expanded and real-time access to metadata needed to be secured. Despite public discussions on the matter in Parliament at the time, nobody in the advocacy sphere apparently took notice.

In August 2013, Prime Minister Manuel Valls presented the 2014–2019 Military Planning Bill (*Loi de Programmation Militaire*, or LPM). Over the course of the parliamentary debate, and in particular when the Senate adopted amendments to the Bill in first reading in October 2013, the law became the vehicle for a partial legalisation of the new capabilities. We were just four months after the first Snowden disclosures, and again no human rights organisation reacted. Six weeks later however, an industry group representing online social services including Google France, AOL, eBay, Facebook, Microsoft, Skype and French companies like Deezer or Dailymotion published an article against the reform (*Association des Services Internet Communautaires*, 2013). It was only then that human rights groups understood the importance of this provision and mounted a last-minute effort to get the provision out of the bill.

Coming at a very late stage of the legislative procedure, the effort eventually failed to strike out the provision. But despite this failure and a somewhat exaggerated denunciation of "generalised surveillance," this first episode of post-Snowden contention had at last led to the mobilisation of civil society groups around Internet surveillance issues, one which benefited from widespread media coverage. Frustrated by their failure to react in time (*before* rather than *after* industry groups) and also finally realising the need to build and share expertise around Internet surveillance and digital rights in general, human rights groups created a new umbrella organisation. Announced on the international "data protection day" in January 2014, it was called the *Observatoire des Libertés et du Numérique* (OLN).

OLN's initial members included organisations that often worked together on non-Internet issues—including the Human Rights League, a lawyers' union (*Syndicat des Avocats de France*) and a judges' union (*Syndicat de la Magistrature*). They were joined by two smaller research organisations devoted to the interplay of the digital technologies and privacy (CECIL and CREIS-Terminal). A few days later, LQDN—with its already established expertise on digital rights, its singular Internet-inspired political culture as well as its own international networks (Breindl, 2011)—, asked to join the coalition.

This brokerage of new connections between French human rights NGOs would play a key role against the Intelligence Bill. But in the meantime, the government apparently slowed the path to legalisation set forth by Urvoas in its recent reports. Post-Snowden contention was finally under way in France, and it was likely perceived to make any significant intelligence reform much more politically risky. At least in the short term.

4. A Long-Awaited Legalisation: Passing the 2015 Intelligence Act

Soon, with the spectacular rise of the threat posed by the Islamic State (Giroux, 2014) and the Paris attacks of January 2015, "securitisation" discourses helped create the adequate political conditions for the passage of the Intelligence Act—the most extensive piece of legislation ever adopted in France to regulate the work of intelligence agencies.

Securitisation is understood in critical security studies as "speech acts through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat" (Buzan & Wæver, 2003, p. 491). In the field of terrorism, these are of course not new. And by the time the Intelligence Bill was introduced, anti-terrorism was already back on the top of the political agenda in France, with the looming threat coming from the Islamic State in Syria and Iraq.

In July 2014, just as the government was introducing a new anti-terrorism bill before the Parliament, President François Hollande convened a National Intelligence Council at the Élysée Palace. In the laconic press-release issued on that day, the Council claimed to have "determined the strategic priorities of [intelligence] services and approved the legal, technical and human resources necessary to carry on these priorities" (French Presidency, 2014). The debate on the anti-terrorism bill, finally adopted on November 2014, also gave an opportunity to OLN members to engage in their first coordinated action against the law's new restrictions on freedom of expression online.

But on January 25th 2015, then Prime Minister Manuel Valls turned the long-awaited intelligence reform into an essential part of the government's political response to the Paris attacks carried on earlier that month. With the country under shock, Valls presented yet another package of "exceptional measures" that formed part of the government's proclaimed "general mobilisation against terrorism". (French Government, 2015). He announced his government would soon present a new bill, which he said was "necessary to strengthen the legal capacity of intelligence agencies to act," alluding to "Djihadist Internet communications".

The Paris attacks only reinforced the ongoing trend toward securitisation, helping to locate the fight against terrorism—and the instrumental role of communications surveillance in that respect—beyond the domain of normal, democratic politics. Securitisation would for instance justify the government's choice to present the bill to Parliament using a fast-track procedure, allowing only one ruling in each of the Parliament's chambers. In sum securitisation was effectively added to denials as rhetorical strategies aimed at dealing with post-Snowden contention, and finally pass a legal basis for what were until then illegal security practices.

4.1. The Intelligence Act's Main Provisions on Internet Surveillance

During the expeditious parliamentary debate that ensued (April–June 2015), the bill's proponents never missed an opportunity to stress, as Valls did while presenting the text to the National Assembly, that the new law had "nothing to do with the practices revealed by Edward Snowden". Distinction strategies notwithstanding, the Act's provisions actually demonstrate how important the sort of practices revealed by Snowden have become for the geopolitical "arms race" in communications intelligence.

The Intelligence Act creates whole new sections in the Code of Internal Security. It starts off by widening the scope of public-interest motives for which surveillance can be authorised. Besides terrorism, economic intelligence, organised crime and counter-espionage, it now includes vague notions such as the promotion of "major interests in foreign policy" or the prevention of "collective violence likely to cause serious harm to public peace". As for the number of agencies allowed to use this new legal basis for extra-judicial surveillance, it comprises the "second circle" of law enforcement agencies that are not part of the official "intelligence community" and whose combined staff is well over 45,000.

In terms of technical capabilities, the Act seeks to harmonise the range of tools that intelligence agencies can use on the regime applicable to judicial investigations. These include targeted telephone and Internet wiretaps, access to metadata and geotagging records as well as computer intrusion and exploitation (i.e. "hacking"). But the Act also authorises techniques that directly echo the large-scale surveillance practices at the heart of post-Snowden controversies. Such is the case of the so-called "black boxes", these scanning devices that will use Big Data techniques to sort through Internet traffic in order to detect "weak signals" of terrorism (intelligence officials have given the example of encryption as the sort of things these black boxes would be looking for).

Another provision limited to anti-terrorism allows for the real-time collection of metadata. Initially, the provision targeted only individuals "identified as a [terrorist] threat". After the 2016 Nice attack, it was extended to cover individuals "likely related to a threat" or who simply belong to "the entourage" of individuals "likely related to a threat". In theory, tens of thousands of people could fall under this definition, and have their metadata collected in real-time during a renewable period of four months.

Similarly, there is a whole chapter on "international surveillance", which legalises the massive programme deployed by the DGSE since 2008 to tap into international cables. Like in other countries, the underlying logic of this article breaches the universality of human rights: communications crossing French borders can be intercepted and analysed "in bulk" with lesser safeguards than those applicable to domestic surveillance. However, the transnational nature of the Internet makes it very likely that the communications of French citizens and residents massively end up in the DGSE's nets, despite a pledge for procedures of so-called "technical minimisation" aimed at protecting communications related to "French technical identifiers" (e.g. French IP addresses).

The Act also grants blanket immunity to intelligence officers who carry on computer crimes into computer systems located abroad, which again will directly affect many French Internet users. The provision may contravene Article 32(b) of the Budapest Convention on Cybercrime on the trans-border access to computer data (Cybercrime Convention Committee, 2014). This provision speaks to the fact that, with encryption on the rise since 2013, the capability to massively penetrate endpoints through hacking is becoming a focus point for intelligence agencies (e.g. UK Home Office, 2016).

As for oversight, as it has been the case since the 1991 Wiretapping Act, all national surveillance activities are authorised by the Prime Minister. A revamped oversight commission (the CNCTR) composed of judges and members of Parliament has 24 hours to issue nonbinding opinions on authorisation requests. The main innovation of the Intelligence Act is the creation of a new redress mechanism before the *Conseil d'Etat* (France's Supreme Court for administrative law), but the procedure is veiled in secrecy and fails to respect defence rights, which again echoes the law of the US and the UK (Bigo, Carrera, Hernanz, & Scherrer, 2014). International surveillance will remain completely outside of this redress procedure.

Among other notable provisions, one forbids the oversight body from reviewing communications data obtained from foreign agencies. The law also fails to provide any framework to regulate (and limit) access to the collected intelligence once it is stored by intelligence and law enforcement agencies, thereby running counter to recent rulings by the Court of Justice of the European Union (CJEU) (Woods, 2016).

4.2. Mobilisation Against the Controversial French Intelligence Bill

By the time the Intelligence Bill was debated in Parliament, in April 2015, human rights organisations partnering in OLN had built the kind of networking and expertise that made them more suited to campaign against national security legislation.

They led the contention during the three-month-long parliamentary debate on the Bill, acting as the core of a network of actors typical of post-Snowden contention (see Figure 2), including international partners in the NGO world, groups of scientists, engineers and hacker groups, French independent companies from the digital sector, and even a few security experts (including former intelligence analysts or a former anti-terrorist judge). These actors also received backing from leading national and international human rights organisations (data protection agency, Council of Europe, UN special rapporteurs, etc.).

Interestingly, to the contrary of the full-fledged contention waged in the US or the UK, large US technology firms like Google or Microsoft declined to engage in the French debate, perhaps out of fear for being cornered for their double-speak on privacy and antagonising French officials, who regularly accused them of engaging in intrusive forms of commercial surveillance. As for their French competitors, like telecommunications companies Orange, SFR and others, their even greater dependence on and proximity with the state political elite probably explain why they chose to remain neutral bystanders.

Overall, contention played an important role in barring amendments that would have given intelligence agencies even more leeway than originally afforded by the bill. Whereas the government hoped for a union sacrée, contention also managed to fracture the initial display of unanimity. MPs from across the political spectrum (including several within both socialist and conservative ranks) fought against the bill, pushing its proponents to amend the text in order to bring significant safeguards compared to the government's proposal. However, the general philosophy of the text remained intact. In June 2015, the bill was eventually adopted with 438 votes in favour, 86 against and 42 abstentions at the National Assembly and 252 for, 67 against and 26 abstentions at the Senate.

The implementation decrees were adopted by the government between October 2015 and February 2016, giving civil society opponents a two-month window to introduce several important legal challenges before the Council of State which are, at the time of writing, still pending. Other legal challenges have been introduced before the ECHR.

5. Conclusion: Facing the Snowden Paradox

The first Snowden disclosures and the global scandal that followed held the promise of an upcoming rollback of the techno-legal apparatus developed by the NSA, the GCHQ and their counterparts to intercept and analyse large portions of the world's Internet traffic. State secrets and the "plausible deniability" doctrine often used by these secretive organisations could no longer stand in the face of such overwhelming documentation. Intelligence reform, one could then hope, would soon be put on the agenda to relocate these surveillance programmes within the boundaries of the rule of law.

Almost four years later, however, what were then reasonable expectations have likely been crushed. Intel-

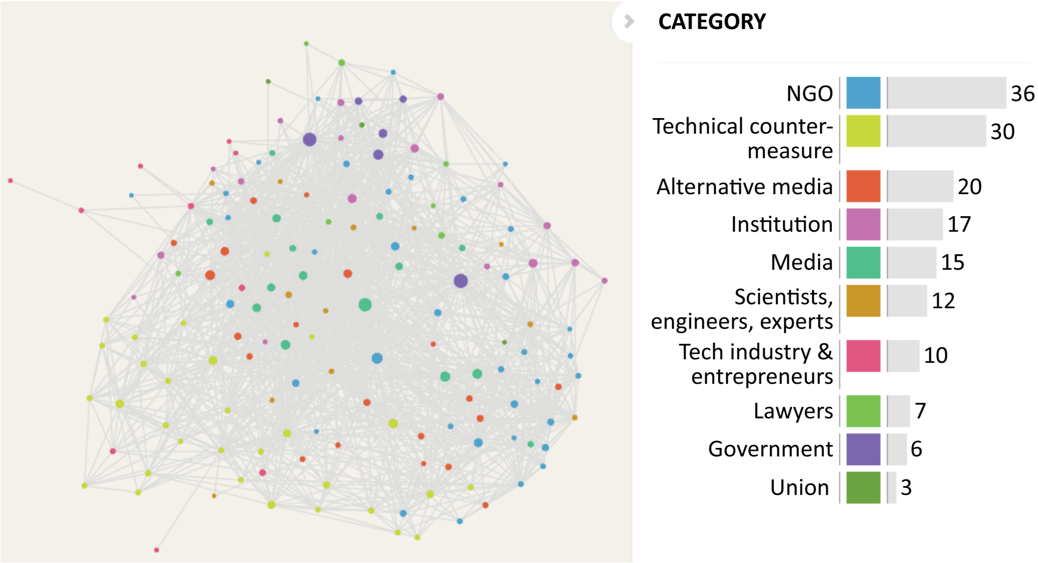


Figure 2. Web cartography of actors mobilised against the French Intelligence Bill. Explore the network online at the following address: https://is.gd/cLkzqh

ligence reform is being passed, but mainly to secure the legal basis for large-scale surveillance to a degree of detail that was hard to imagine just a few years ago. Despite unprecedented mobilisations against surveillance practices developed in the shadows of the "deep state", the latter are progressively being legalised. Hence the Snowden paradox.

France was the first liberal regime to engage in a sweeping, post-Snowden intelligence reform. There, even prior to 2013, the legal pressure exerted by human rights standards, and their application by supranational courts like the ECHR, had already triggered a slow process of legalisation. Post-Snowden contention only made that pressure stronger, pushing intelligence policymakers to secure and expand the surveillance capabilities of their agencies through intelligence reform, as soon as the political conditions seemed ripe.

While it would be tempting to see the Intelligence Act of 2015 as part of a certain French tradition when it comes to regulating the Internet (Mailland, 2001; Meyer & Audenhove, 2012; Tréguer, 2015), the situation in other countries suggests that the French case is part of a wider trend. In the Fall of 2016, the British Parliament passed the much-criticised Investigatory Powers Bill (Hintz & Dencik, 2016). Simultaneously in Germany, amendments to the so-called "G-10 law" were adopted to validate the large-scale surveillance powers of the country's foreign intelligence agency, the BND—also embroiled in the NSA scandal (Wetzling, 2016). In the Netherlands, an ongoing intelligence reform is raising similar concerns, while the reform of the US PATRIOT Act in June 2015 was extremely modest. Detailed cross-country comparisons are of course warranted. But despite important variations between these countries—for instance regarding the initial weaknesses and strengths of privacy advocacy in these different national contexts, or the role played by large US Internet firms in policy debates—, these other instances of post-Snowden intelligence reform seem to confirm the existence of the Snowden paradox.

Fifteen years after 9/11, which brought an abrupt end to the controversy on the NSA's ECHELON program (Campbell, 2000) and paved the way for the adoption of the PATRIOT Act in the US and similar legislation elsewhere, the threat of terrorism and associated processes of securitisation are hindering the global episode of contention opened by Edward Snowden. Securitisation creates a "chilling effect" on civil society contention, making legalisation politically possible and leading to a "ratchet effect" in the development of previously illegal security practices or, more generally, of executive powers. In that regard, post-Snowden intelligence reform stands as a stark reminder of the fact that, once coupled with securitisation, "a-legality" and national security become two convenient excuses for legalisation and impunity, allowing states to navigate the legal and political constraints created by human rights organisations and institutional pluralism.

During the debate on the French Intelligence Act, Urvoas stressed that the law was neither Schmitt's nor Agamben's states of exception (Urvoas, 2013b). But because it is "legal" or includes some oversight and redress mechanisms does not mean that large-scale surveillance and secret procedures do not represent a formidable challenge to the rule of law. Rather than a state of exception, legalisation carried on under the guise of the raison d'État amounts to what Sidney Tarrow calls "rule by law". In his comparative study of the relationships between states, wars and contention, he writes of the US "war on terror":

> Is the distinction between rule of law and rule by law a distinction without difference? I think not. First, rule by law convinces both decision makers and operatives that their illegal behavior is legally protected….Second, engaging in rule by law provides a defense against the charge they are breaking the law. Over time, and repeated often enough, this can create a "new normal", or at least a new content for long-legitimated symbols of the American creed. Finally, "legalizing" illegality draws resources and energies away from other forms of contention. (2015, pp. 165–166)

The same process is happening with regards to present-day state surveillance: the suspicionless interception of communications, "big data" preventive policing and large-scale computer hacking are becoming the new normal in intelligence practices. At this point in time, it seems difficult to argue that post-Snowden contention has hindered in any significant and lasting way the formidable growth of surveillance capabilities of the world's most powerful intelligence agencies.

And yet, while the current trend of legalisation is especially worrying considering the ongoing illiberal drift in Western democracies, the jury is still out. Besides legalisation, Post-Snowden contention is having another major outcome: new coordination in civil society both nationally and globally, with the formation of a transnational movement against Internet surveillance (Tarrow, 2016). This emerging movement has been documenting Internet surveillance like never before, undermining some of the secrecy that surrounds the intelligence field and hinders its democratic accountability. It has provided fresh political and legal arguments to reclaim privacy as a "part of the common good" (Lyon, 2015, p. 9), and helped push for the proliferation of legal and policy recommendations regarding the compliance of surveillance with human rights.

Most crucially, this emerging privacy movement has led courts—in particular the ECHR and the CJEU—to consider cases of historic importance that, in the long run, could prove to be game-changers. Strategic litigation has indeed the potential of turning the Snowden paradox on its head, that is to use these new laws—and the new legal opportunities it brings to privacy advocates—to counter the surveillance practices that legalisation sought to legitimise in the first place.

Judges now appear as the last institutional resort against large-scale surveillance. If court actions fail, the only possibility left for resistance will lie in what would by then represent a most transgressive form of political action: democratising the use of strong encryption, and subverting the centralised and commodified technical architecture that made such surveillance possible in the first place.

Acknowledgements

This research was conducted for the UTIC project, supported by the French National Research Agency.

Conflict of Interests

The author declares no conflict of interests.

References

Association des Services Internet Communautaires. (2013, March 18). Surveillance de l'Internet, accès aux données d'utilisateurs: Pour un moratoire sur les régimes d'exception. *Association des Sites Internet Communautaires*. Retrieved from http://archive.is/firXs

Benkler, Y. (2011). A free irresponsible press: Wikileaks and the battle over the soul of the networked fourth estate. *Harvard Civil Rights-Civil Liberties Law Review*, *46*(2), 311–397.

Bigo, D., Carrera, S., Hernanz, N., & Scherrer, A. (2014). *National security and secret evidence in legislation and before the courts: Exploring the challenges* (Report to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs [LIBE] No. PE 509.991). Brussels: European Parliament. Retrieved from http://www.europarl.europa.eu/thinktank/fr/document.html?reference=IPOL_STU%282014%29509991

Breindl, Y. (2011). *Hacking the law: An analysis of internet-based campaigning on digital rights in the European Union*. Brussels: Free University of Brussels.

Buzan, B., & Wæver, O. (2003). *Regions and powers: The structure of international security*. Cambridge: Cambridge University Press.

Campbell, D. (2000). Inside Echelon: The history, structure, and function of the global surveillance system known as Echelon. *Telepolis*. Retrieved from https://www.heise.de/tp/features/Inside-Echelon-3447440.html

Chapuis, N. (2013, June 12). Urvoas: "Je n'ai pas rencontré de programme de surveillance similaire en France". *Le Monde*. Retrieved from http://www.lemonde.fr/politique/article/2013/06/12/urvoas-je-n-ai-pas-rencontre-de-programme-de-surveillance-similaire-en-france_3428507_823448.html

Chevallier, J. (1992). Le mythe de la transparence administrative. In *Information et transparence administrative* (pp. 239–275). Paris: Presses Universitaires de France.

Cybercrime Convention Committee. (2014). *T-CY Guidance Note #3 transborder access to data* (No. T-CY [2013]7 E). Strasbourg: Council of Europe. Retrieved from https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297REV_GN3_transborder_V11.pdf

EFF. (2014). *Necessary & proportionate: International principles on the application of Human Rights to communications surveillance*. Retrieved from https://en.necessaryandproportionate.org

Errera, R. (2003). Les origines de la loi française du 10 juillet 1991 sur les écoutes téléphoniques. *Revue Trimestrielle des Droits de l'Homme*, *55*, 851–870.

Fédération Internationale des Droits de l'Homme. (2013, July 12). Affaire Snowden: La FIDH saisit l'ONU. *FIDH*. Retrieved from https://archive.is/mSEZo

Follorou, J. (2013, October 30). Surveillance: La DGSE a transmis des données à la NSA américaine. *Le Monde*. Retrieved from http://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html

Follorou, J., & Johannès, F. (2013, July 4). La totalité de nos communications espionnées par un supercalculateur. *Le Monde*. Retrieved from http://www.lemonde.fr/ societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html

French Government. (2008). *Livre blanc sur la défense et la sécurité nationale*. Paris: French Government.

French Government. (2015, November 19). *#Antiterrorisme: Manuel Valls annonce des mesures exceptionnelles*. Paris: French Government. Retrieved from http://archive.is/x1zhB

French National Assembly. (2013). *Audition du préfet Erard Corbin de Mangoux, Directeur Général de la sécurité extérieure (DGSE) au ministère de la Défense* (Compte Rendu n° 56). Paris: French National Assembly.

French Presidency. (2014, July 9). *Compte-rendu public du Conseil national du renseignement*. Retrieved from https://archive.is/7W2jm

Fuster, G. G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Berlin: Springer Science+Business.

Giroux, H. A. (2014). ISIS and the spectacle of terrorism: Resisting mainstream workstations of fear. *Philosophers for Change*. Retrieved from https://philosophersforchange.org/2014/10/07/isis-and-the-spectacle-of-terrorism-resisting-mainstream-workstations-of-fear

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

Hourdeaux, J. (2016, June 6). Comment les services de renseignement ont mis en place une surveillance générale du Net dès 2009. *Mediapart*. Retrieved from https://www.mediapart.fr/journal/france/060616/comment-les-services-de-renseignement-ont-mis-en-place-une-surveillance-generale-du-net-des-2009

Jauvert, V. (2015, July 1). Comment la France écoute (aussi) le monde. *Le Nouvel Observateur*. Retrieved from http://tempsreel.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html

Joinet, L. (2013). *Mes raisons d'État: Mémoires d'un épris de justice*. Bayonne: La Découverte.

La Quadrature du Net. (2013, July 29). Newsletter #51. *LQDN*. Retrieved from https://www.laquadrature.net/fr/newsletter/newsletter-51

Lyon, D. (2015). *Surveillance after Snowden*. Cambridge: Polity Press.

Mailland, J. (2001). Freedom of speech, the internet, and the costs of control: The French example. *New York University Journal of International Law & Politics*, *33*.

Manach, J. M. (2010, October 2). Frenchelon: La DGSE est en "1ère division". *Le Monde*. Retrieved from http://bugbrother.blog.lemonde.fr/2010/10/02/frenchelon-la-dgse-est-en-1ere-division

Manach, J.-M. (2013, July 11). La DGSE a le "droit" d'espionner ton Wi-Fi, ton GSM et ton GPS aussi. *Le Monde*. Retrieved from http://bugbrother.blog.lemonde.fr/2013/07/11/la-dgse-a-le-droit-despionner-ton-wi-fi-ton-gsm-et-ton-gps-aussi

Marzouki, M. (2009). "Non à Edvige": Sursaut ou prise de conscience? *Plein Droit*, *80*, 21–26. Retrieved from http://www.gisti.org/spip.php?article1477

Meili, S. (1998). Cause lawyers and social movements: A comparative perspective on democratic change in Argentina and Brazil. In A. Sarat & S. Scheingold (Eds.), *Cause lawyering: Political commitments and professional responsibilities* (pp. 487–522). Oxford: Oxford University Press.

Meyer, T., & Audenhove, L. V. (2012). Surveillance and regulating code: An analysis of graduated response in France. *Surveillance & Society*, *9*(4), 365–377.

Reflects.info. (2016, June 6). Qosmos et le gouvernement Français, très à l'écoute du Net dès 2009. *Reflects.info*. Retrieved from https://reflets.info/qosmos-et-le-gouvernement-francais-tres-a-lecoute-du-net-des-2009

Rubinstein, I. S., Nojeim, G. T., & Lee, R. D. (2014). Systematic government access to personal data: A comparative analysis. *International Data Privacy Law*, *4*(2), 96–119.

Schulhofer, S. (2015). *Access to national security information under the U.S. Freedom of Information Act* (Public Law Research Paper No. 15–14). New York, NY: NYU School of Law. Retrieved from https://papers.ssrn.com/abstract=2610901

Schulze, M. (2015). Patterns of surveillance legitimization. The German discourse on the NSA scandal. *Surveillance & Society*, *13*(2), 197–217.

Tarrow, S. (2015). *War, states, and contention: A comparative historical study* (1st ed.). Ithaca and London: Cornell University Press.

Tarrow, S. (2016). *Close interaction, incompatible regimes, contentious challenges: The transnational movement to protect privacy*. Berlin: Berlin Social Science Center. Retrieved from https://www.researchgate.net/project/Transnational-Movements-and-the-Protection-of-Privacy/update/582c8dc608ae91d0fe24f203

Tilly, C., & Tarrow, S. (2015). *Contentious politics* (2nd ed.). New York, NY: Oxford University Press.

Tréguer, F. (2015). Hackers vs states: Subversion, repression and resistance in the online public sphere. *Droit et Société*, *91*(3), 639–652.

Tréguer, F. (2016a). *From deep state illegality to law of the land: The case of internet surveillance in France*. Paper presented at the 7th Biennial Surveillance & Society Conference (SSN 2016) "Power, Performance and Trust", Barcelona, Spain. Retrieved from https://halshs.archives-ouvertes.fr/halshs-01306332/document

Tréguer, F. (2016b). *French constitutional council strikes down 'Blank Check' provision in the 2015 Intelligence Act*. Retrieved from https://halshs.archives-ouvertes.fr/halshs-01399550/document

UK Home Office. (2016). *Operational case for bulk powers*. London: British Government. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf

Urvoas, J.-J. (2013a, July 4). *Big Brother à la française? Commentaires*. Retrieved from http://archive.is/7SGgk

Urvoas, J.-J. (2013a, October 30). Il faut renforcer le contrôle des services de renseignement en France. *Le Monde*. Retrieved from http://www.lemonde.fr/idees/article/2013/10/30/il-faut-renforcer-le-controle-des-services-de-renseignement-en-france_3505116_3232.html

Urvoas, J.-J., & Verchère, P. (2013). *Rapport en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement* (Commission des Lois No. 1022). Paris: National Assembly. Retrieved from http://www.assemblee-nationale.fr/14/controle/lois/renseignement.asp

Wetzling, T. (2016). *The key to intelligence reform in Germany* (Europäische Digitale Agenda). Retrieved from http://www.stiftung-nv.de/sites/default/files/snv_g10.pdf

Woods, L. (2016, December 21). Data retention and national law: The ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber). *EU Law Analysis*. Retrieved from https://eulawanalysis.blogspot.fr/2016/12/data-retention-and-national-law-ecj.html

About the Author

Félix Tréguer works on past and present contention around the protection of civil rights and communicational autonomy on the Internet. He is a junior researcher at CERI-Sciences Po, where he looks at post-Snowden controversies for the UTIC project. He is a founding member of the Paris-based digital rights advocacy group *La Quadrature du Net*.

COGITATIO

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 29–41
DOI: 10.17645/mac.v5i1.808

Article

Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy

Nathalie Maréchal

Annenberg School for Communication and Journalism, University of Southern California, Los Angeles, CA 90007, USA; E-Mail: marechal@usc.edu

Submitted: 30 October 2016 | Accepted: 6 February 2017 | Published: 22 March 2017

Abstract

In the aftermath of the 2016 U.S. election, researchers, policymakers and the general public are grappling with the notion that the 45th president of the United States may very well owe his electoral victory to a sophisticated propaganda effort masterminded by the Kremlin. This article synthesizes existing research on Russia's domestic information controls, its internet policy at the global level (notably via internet governance processes), and the country's resurgence as a major geopolitical player to argue that policymakers as well as the general public should consider these themes holistically, particularly as they formulate responses to what many see as the Russian threat to Western liberal democracy. Russia may have lost the Cold War, but it is now waging information warfare against the liberal democracies of Europe and North America in a sophisticated bid to win the next round. Russia does not view internet governance, cybersecurity, and media policy as separate domains. Rather, all the areas covered by those disciplines fall under "information security" for Russian foreign policy. The paper begins by tracing the history of information controls within what is now the Russian Federation before discussing the role of information and internet policy in Russian foreign policy, drawing connections between the Russian government's control and manipulation of information—including its internet policy—in the domestic and international arenas. Next, it discusses the spread of networked authoritarianism and suggests that a "geopolitics of information" will become increasingly necessary in the coming years. Just as networked authoritarianism establishes strategic infrastructures to control the message domestically and intervene in global media systems, liberal democracies need to rethink media and communication infrastructures to ensure they foster pluralist, rights-respecting societies that are resilient to authoritarianism and extremism. In doing so, they should resist the temptation to respond to this threat in ways that will erode democracy even further, such as expanded surveillance and limits on free expression.

Keywords

2016 election; censorship; data localization; human rights; networked authoritarianism; propaganda; Russia; surveillance

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).

1. Introduction

After a long and bitter electoral campaign, the results of the 2016 U.S. election have precipitated an ongoing constitutional crisis, and continued uncertainty about the role of Russia's government in Donald Trump's electoral victory has prompted renewed interest in Russia, a country that hadn't been at the forefront of the national agenda since the end of the Cold War. Several factors contribute to making the current situation a perfect storm of uncertainty and ambiguity, including: policymakers' and the public's comparative lack of knowledge about Russia; the difficulty of parsing out something resembling empirical truth from the jumble of official statements, leaks, speculations and claims made by the various actors involved; the tumultuous presidential transition; and the arcane nature of the empirical claims underlying the web of controversy surrounding the election and any role Russia might have had in influencing the result. It will take time and serious effort for the dust to settle; an analysis of the events leading up the 2016 election, or of the election's aftermath, would be premature. However, at this stage it is appropriate to consider what we do know about Russia's policies concerning information, the internet and international relations under Vladimir Putin.

There is a natural tendency in scholarship and policy to work within disciplinary silos, without sufficiently considering related developments that are better aligned with a different field of expertise. At a time when American interest in Russia is at perhaps its highest since the end of the Cold War, it is important to consider all of Russia's information and internet policy, both domestic and international, in order to properly situate current developments and formulate policy responses that defend and support democracy and human rights. The topic is a complex one, and it would be impossible to cover it entirely, with all its nuances and complexities, in an article-length piece. My aim here is twofold: to draw connections between the Russian government's control and manipulation of information—including its internet policy—both domestically and externally, and to theorize on the spread of networked authoritarianism and the future of the geopolitics of information.

This article was written for a thematic issue on "Internet Policy After Snowden", but it is broader than that in at least two ways. First, it goes beyond narrow definitions of internet policy to consider several aspects of Russian information and communication policy that are inextricably intertwined. And second, it has very little to say about Edward Snowden. At least in the Russian context, the 2013 Snowden revelations mainly serve as a temporal marker. They alerted global public opinion to mass surveillance and made possible a change in the Kremlin's rhetoric, but did not cause a shift in Russian policy. If there was a turning point in Russian internet policy, that moment was in 2011: the year of the Arab Spring, but also the year that Russian civil society used social media to organize protests of the legislative election, about which then-U.S. Secretary of State Hillary Clinton expressed "serious concerns" (Labott, 2011). It was also the year before Putin resumed the presidency, after swapping roles with Dmitri Medvedev for four years.

In this article, I synthesize existing research on Russia's domestic information controls policy, internet policy at the global level (notably via internet governance processes), and the country's resurgence as a major geopolitical player to argue that policymakers as well as the general public should consider these themes holistically, particularly as they formulate responses to what many see as the Russian threat to Western liberal democracy. In doing so, they should resist the temptation to respond to this threat in ways that will erode democracy even further, such as expanded surveillance and limits on free expression.

Methodologically, the article relies chiefly on secondary sources, including translations of Russian sources and sources written in English by Russian journalists, while drawing on my interactions with a variety of policy experts (both Russian and Western) in the course of other ongoing work, some of whom have asked to remain anonymous for their own safety. Throughout the article I consider information policy, media policy and internet policy holistically, as they are closely interrelated. The article begins by tracing the history of information controls (which predate the internet) within what is now the Russian Federation before discussing the role of information and internet policy in Russian foreign policy. Next, I discuss the spread of networked authoritarianism and suggest that a "geopolitics of information" will become increasingly necessary as the 21st century marches on, and theorize on what this might be, concluding with a call to defend, protect and improve Western liberal democracy.

2. Information in Russia Before the Internet

This section traces the history of the media and information controls in Russia, which is distinct from the history of the press and the media in the West. Media in Russia have always served as instruments of political propaganda, going back to the country's first newspaper. *Vedomosti* was founded in 1702 to disseminate the czar's wishes, plans, and priorities across the country, and to build popular support for the ruler (Rohlenko, 2007). Under the USSR, information was considered a dangerous commodity to be feared and controlled, rather than a right and a public good. Contrary to liberal conceptions of a free press serving as a fourth branch of governance and fostering a habermasian public sphere (Habermas, 1989), the Soviet regime saw the media as a danger to be tightly controlled, with only select elites permitted access to objective news or to foreign publications (Gorny, 2007; Soldatov & Borogan, 2015). For example, ownership and use of photocopiers were tightly restricted in an attempt to prevent the distribution of *samizdat*, photocopied pamphlets of "subversive" material (Hanson, 2008).

It is no accident of history that the collapse of the USSR coincided with the emergence of the information society in the West. Indeed, Castells and Kiselyova (1995) argue that this death grip on information was the primary reason for the USSR's implosion. The 1990s were a period of relative freedom for the press in post-Soviet Russia, albeit a short-lived one as the levers of power—recently relinquished by the Communist Party—were seized by the new oligarch class. The media were no longer beholden to a monolithic ideology, but instead answered to a variety of corporate backers whose interests didn't always align. Print media lost their state subsidies and saw their circulation and importance decline precipitously, leaving broadcast TV to take over as the country's predominant communication medium (Ognyanova, 2015).

Vladimir Vladimirovich Putin, Yeltsin's chosen successor, first assumed the presidency of the Russian Federation in 1999, and quickly restored the Kremlin's control over print and broadcast media—a move that he characterized as "liberating" news outlets from the oligarchs. For many Russia experts, understanding Putin is key to understanding Russia today. Putin served in the Soviet intelligence agency, the KGB, for 16 years, rising to the rank of colonel, and he spent much of the pivotal perestroika years outside of Russia. His views on governance, the rule of law, the role of information in society, and the Russian national interest are very much influenced by the KGB's authoritarian traditions, themselves grounded in the authoritarianism of imperial Russia. Putin switched posts with his prime minister, Dmitri Medvedev, in 2008 to circumvent constitutional term limits, and in 2012 Putin returned to the Kremlin and redoubled his efforts to control the internet (Ognyanova, 2015; Soldatov & Borogan, 2015).

The end of the Cold War, which also ended Russia's superpower status (as nominal as it might have been, particularly toward the end), was a sore spot for the Russian elite, which perceived the U.S.'s success in exporting its cultural products as a threat to national sovereignty. Elites also resented growing U.S. influence in Eastern Europe and Central Asia, which they saw as their rightful sphere of influence, and the European Union's eastward expansion. Over the course of his first presidency (2000–2008), during which time domestic internet access grew considerably, Putin came to see the information revolution as "one of the most pervasive components of U.S. expansionism in the post-Soviet sphere, most notably in Russia itself" (Nocetti, 2015, p. 129). Where others might have seen opportunities for innovation and growth, Putin saw threats to the status quo and his hold on power, thus following in the footsteps of his Soviet and pre-bolshevik predecessors alike.

3. The Russian Information Controls Regime

Ronald Deibert and his team at the University of Toronto's Citizen Lab coined the phrase "information controls" to describe the "techniques, practices, regulations or policies that strongly influence the availability of electronic information for social, political, ethical, or economic ends". These include technical means like "filtering, distributed denial of service attacks, electronic surveillance, malware, or other computer-based means of denying, shaping and monitoring information" and policies like "laws, social understandings of 'inappropriate' content, media licensing, content removal, defamation policies, slander laws, secretive sharing of data between public and private bodies, or strategic lawsuit actions" (Citizen Lab, 2015). As a field of inquiry, information controls can also include the means of circumventing or otherwise countering barriers to the free flow of information online. Importantly, the field is inherently multidisciplinary and transcends the barrier between academia and civil society, with many important advances coming from activists and nonprofits.

The Freedom on the Net Index classifies information controls under three broad categories: obstacles to access, limits to content, and violations of user rights (Karlekar & Cook, 2009). Compared to China, Russia rarely uses obstacles to access (which include infrastructural and economic barriers as well as shutdowns and application-level blocking), relying instead on censorship and intimidation. However, Russia is taking steps to create an internet "kill switch", allowing it to disconnect the RuNet from the global network "in case of crisis", without specifying what such a crisis might entail beyond vague allusions to the internet being shut off from the outside (Duffy, 2015; Nocetti, 2015). Internet shutdowns—whether of all connection to the outside world, or of specific applications and protocols like VOIP, Twitter or WhatsApp—are used by governments like Egypt, Uganda and Iran to control the flow of information around elections, protests, and other politically sensitive events (DeNardis, 2014). The advocacy organization Access Now has reported a marked increase in the number of network shutdowns worldwide in recent years (Access Now, 2016). The Russian "kill switch" system has yet to be put into effect, as of this writing.

Censorship and violations of user rights, then, have historically been the principal mechanisms for information control in Russia. Katherine Ognyanova (2015) identifies three mechanisms through which the Russian state asserts power over the media: censorship and resulting chilling effects, state control over mainstream (especially broadcast) media, and the selective application of unrelated laws (building codes, tax laws, criminal laws, and intellectual property laws have all been used for this purpose) to put pressure on media organizations as well as individual journalists, bloggers, and activists. Extrajudicial executions are not uncommon. This is in many ways a continuation of the mechanisms used by successive Russian and Soviet governments to control the traditional print and broadcast media (Ognyanova, 2015). One key difference from the Soviet era is that the domestic media has since been privatized, and foreign companies—notably internet intermediaries—now operate in Russia as well.

In Russia, as in most countries, the physical structure of the internet is built, owned and maintained by the private sector. Companies like internet companies, Internet Service Providers (ISPs), social networking sites (SNSs), search engines, blogging platforms, and more then exercise a form of de facto private governance over online activity (MacKinnon, 2012). This private rule-making can come into conflict with the law. Absent a strong rule of law, governments can use their power to constrain, influence and even coerce information and telecommunications (ICT) companies. As Laura DeNardis notes, "state control of Internet governance functions via private intermediaries has equipped states with new forms of sometimes unaccountable and nontransparent power over information flows" (DeNardis, 2014, p. 15). We now turn to an examination of how the Russian state practices censorship and surveillance with the assistance of the private sector.

4. Censorship

Media in the Russian Federation, including the internet, is regulated by a branch of the Ministry of Communications and Mass Media, the Federal Service for Supervision of Communications, Information Technology, and Mass Media, better known as Roskomnadzor. Unlike the UK's Ofcom or the U.S. Federal Communications Commission, which are independent agencies with no power of prior restraint (the main enforcement mechanism is to assess fines), Roskomnadzor can block certain types of content without a court order: calls for unsanctioned public actions (i.e. protests), so-called extremist content, materials that violate copyright, information about juvenile victims of crime, child abuse imagery, drug propaganda, and information about suicide—as can several other agencies, including the Federal Drug Control Service, the Federal Service for Surveillance on Consumer Rights and Human Wellbeing, and the Prosecutor General's Office (Freedom House, 2015). Other types of content can also be blocked, but a court order is required.

While the authority to censor rests with the state, the responsibility to implement censorship falls on the internet service providers, who are held legally responsible for any forbidden content that is accessible to their users, a legal construct known as intermediary liability (MacKinnon, Hickock, Bar, & Lim, 2014). Since 2014, the Russian media regulator Roskomnadzor has maintained a block list of websites featuring banned content, including child abuse imagery, drug-related content, and "suicide advocacy". ISPs must regularly consult this "blacklist" of verboten websites, and are incentivized to interpret blocking orders as widely as possible to avoid liability for under-censoring, which can result in heavy fines and even the loss of their state licenses. The "blacklist" itself is often vague as to which page within a website or service should be blocked, or only specifies an IP address—which can represent any number of websites. Crucially, the list itself is secret, leaving internet users in the dark as to what is actually prohibited (Freedom House, 2015, 2016).

Roskomnadzor's powers are even greater with respect to websites that are registered as mass media—a broader category than one might think, thanks to the "Bloggers' Law". As early as 2001, the then-press minister, Mikhail Lesin,[1] "called for legislation requiring the registration of Internet media outlets", which would have included any website registered with the .su or .ru top-level domain (TLD) (Ulmanu, 2001, as cited in Bowles, 2006). Lesin finally got his wish in 2014, when the so-called "Bloggers Law" was instituted, requiring all online outlets (including blogs and personal pages within social networking sites) with more than 3,000 daily page views to register with the government, while the "Law Against Retweets" punishes the dissemination or re-dissemination of "extremist content" with up to five years in prison. "Extremist content" is defined so vaguely that it can be interpreted to include many kinds of speech that would be considered innocuous in many other countries. Another 2014 law prohibits the use of public wifi without providing one's mobile phone number. Acquiring a SIM card, in turn, requires providing one's passport number, as does signing up for home internet access. It is all but impossible, then, to surf the "RuNet" (as the Russian-language internet is called) without linking one's online activity to one's identity and passport (Duffy, 2015).

Under Article 4 of the law "On Mass Media", the regulator can issue warnings to an outlet's editorial board about "abuse of freedom of mass media", a category that includes such infractions as obscene language, information about illegal drugs, extremism, incitement to terrorism, and propaganda and cruelty. Here again, the specific interpretation of these terms leads to censorship well beyond what a literal reading of the law might suggest. For example, news sites have received warnings for publishing stories about calls for greater local governance ("federalization") and for government reform, and about international news events related to freedom of expression such as the attack on the Charlie Hebdo offices in Paris in January 2015 (Freedom House, 2015).

In addition to legislative and technical controls, the flow of information on the Russian internet is limited by two "soft" factors: cultural norms and practices grounded in centuries of authoritarianism, and deliberate framing of the internet as dangerous (Ognyanova, 2015). The Russian political class and broadcast media work together to frame the internet as a dangerous place, and online content as "unreliable, biased, and dangerous" (Kratasjuk, 2006; Ognyanova, 2015). For example, the mayor of Moscow wrote that "propaganda of drugs and violence, human trafficking and child prostitution—that's the reality of today's internet", asserting that "the Internet is gradually being settled by unconcealed terrorists who turn the web, not only into their own mailbox, but into a real, underground, military infrastructure" (Ognyanova, 2015). The strategy seems to be effective. Indeed, the report "Benchmarking Public Dissent: Russia's Appetite for Internet Control" found that 49% of all Russians believe that information on the internet needs to be censored, while 42% of Russians believe foreign countries are using the internet against Russia and its interests, and 24% think the internet threatens political stability (Nisbet, 2015). Propaganda of the kind described above allows the Kremlin to present its restrictions on the free flow of information as responses to popular will.

Restrictions on free expression continue apace, as the 2016 Yarovaya laws place new restrictions on "proselytizing" (i.e. discussing one's religion with potential converts) and require anyone with knowledge that someone else is "planning" certain kinds of crimes, mainly offenses

[1] Lesin was found dead, seemingly of a blow to the head, in a Washington hotel in November 2015. See Smith and Walker (2016).

that involve expressing dissenting views, to notify the authorities (Lokshina, 2016).

5. Surveillance

Domestic surveillance in Russia predates the internet, of course. As with censorship, the current surveillance regime is historically grounded in the country's Soviet and imperial past. The KGB may have a new acronym, FSB (standing for Federal'naya sluzhba bezopasnosti, or Federal Security Service), but it casts a long shadow (Soldatov & Borogan, 2015).

The System of Operational-Investigatory Measures (SORM) was first implemented in 1995, requiring telecommunications operators to install FSB-provided hardware allowing the agency to monitor users' communications metadata and content—including phone calls, email traffic and web browsing activity, despite the low internet penetration rate at the time.

Coming in the final year of Yeltsin's presidency, the 1999 SORM-2 reform required the FSB to obtain a post-collection court warrant to access records (Bowles, 2006). This was an encouraging sign that the intelligence services of the new Russian Federation would be governed by the rule of the law. However, shortly after taking office, Putin authorized several additional agencies to access SORM's collected data, including the tax authorities, border patrol and customs agencies, and the Presidential Security Service. The warrant requirement remains in place, but is remarkably toothless: surveillance can begin before the warrant is granted (or even requested), the warrant need not be shown to anyone (whether the surveillance target or the telecom operator), and it is only required for the retrieval of collected communications content, and not for the metadata that is often just as revealing as content, if not more so. In 2012 SORM-2 was expanded to include social media platforms, though documentation of how this works in practice is scant (Paganini, 2014; Soldatov & Borogan, 2012, 2015). Nevertheless, the assumption among Russian digital rights activists is that any information shared on Russian social networks like Vkontakte or Odnoklassniki is collected by the intelligence services (author interviews, 2016).

The latest update to SORM came in 2014, when the Ministry of Communications ordered companies to install new equipment with Deep Packet Inspection (DPI) capability (Soldatov & Borogan, 2015). As DeNardis puts it, "DPI is a transformational technology that creates unprecedented regulatory possibilities for controlling the flow of content online" (2014, p. 206). Demonstrating why this is the case requires a basic understanding of the technology itself. Information (whether it's text, voice, or something else) is transmitted over the internet as packets, small bundles of data that are individually routed from the sender to the receiver, then put back together in the correct order. Packets consist of both payload (the actual content of the communication) and a header, which contains the packet's metadata: its origin, destination, and not much else. The header is analogous to an envelope, telling each piece of equipment along the way where the payload should be delivered. Until fairly recently, computing power limited the types of analyses that routers, switches and other network hardware could perform on passing traffic, but advances in this domain have made it possible for hardware to simultaneously process millions of packets, reading not just the headers but the payload as well. Unless the packet is encrypted, the only impediment to stopping a DPI-capable machine from reading the payload are social and legal norms against this type of surveillance—which are absent in Russia. From there it is possible to block or throttle back traffic based on its origin, destination, file type (text, voice, multimedia), protocol (P2P, FTP, HTML, SMTP) or the content of the message itself (DeNardis, 2014). Here again, there is little reliable, publicly available information on how SORM-3 works, as discussing the topic is against the law. The new, secret regulations came into effect in fall 2016, and apply to all ISPs in Russia. Noncompliance comes at a steep price: stern warnings from Roskomnadzor followed by revocation of the ISP's license. Extra-legal intimidation is common, and formal enforcement appears to be increasing. Indeed, investigative journalists Andrei Soldatov and Irina Borogan obtained internal Roskomnadzor statistics that showed that the number of warnings issued by the agency grew from 16 in 2010 to 30 in 2012 (Soldatov & Borogan, 2013).

Also in 2012, SORM was applied to social networking sites, a key area of concern for Russian authorities given the role of such sites in various "color revolutions" and the 2011 Arab Spring (Howard & Hussain, 2013). As Soldatov and Borogan note, the tools used to monitor social networking sites had a crucial flaw:

> These systems were developed for searching structured computer files, or databases, and only afterwards adapted, some more successfully than others, for semantic analysis of the Internet. Most of these systems were designed to work with open sources and are incapable of monitoring closed accounts such as Facebook.
>
> The FSB discovered early on that the only way to deal with the problem was to turn to SORM. The licenses require businesses that rent out site space on servers to give the security services access to these servers via SORM, without informing the site owners. With this provision, the FSB has had few problems monitoring closed groups and accounts on Russian social networks Vkontakte and Odnoklassniki. But Facebook and Twitter don't store their user data in Russia, keeping it out of SORM's reach. (Soldatov and Borogan, 2013, para. 20)

Edward Snowden's revelations about the U.S. National Security Agency's PRISM program, which tapped into American ICT companies' data centers to extract desired information, provided the perfect justification for requiring all data pertaining to Russian citizens to be stored within the Russian Federation. Brazil and several European countries have made announcements about eventual data localization requirements, as well, providing further legitimacy to the Russian plan in the eyes of public opinion. However, there is no evidence that data localization does much to protect user privacy (Sargsyan, 2016). Indeed, it is much easier (and more clearly within the bounds of U.S. law) for the U.S. intelligence apparatus to target data outside of the U.S., while locating data centers within Russia makes it easier for Russian agencies to access user content. Data localization serves to increase the Kremlin's access to citizen data under the guise of protecting the Russian public from American spies.

The 2016 Yarovaya laws further expanded the government's surveillance powers by increasing the mandatory data retention period to six months for content and three years for metadata and mandating cryptographic backdoors in all messaging applications (Lokshina, 2016).

6. Conscripting the Private Sector

Twenty-first century information controls in Russia distinguish themselves from earlier systems of repression in two key ways: the introduction of ICT technologies, and the irruption of the private sector in what was previously a totalitarian, state-controlled ecosystem. Moscow's appetite for surveillance has grown apace with the potential targets provided by widespread ICT adoption, and the FSB-oligarchic alliance that dominates both the state and the economy excels at finding ways to pressure ICT companies to provide the needed access to data flows.

A 2013 study by the now-defunct Center for the Study of Media and Society at the New Economic School in Moscow[2] sought to ascertain the policies and mechanisms used by domestic Russian ICT companies to protect the digital rights of their users. Conducted during a time of great uncertainty for the ICT sector in Russia, the study found that company representatives were hesitant to discuss issues of human rights (preferring the term "user rights"), the pressures they faced from the Kremlin, or the possibility of doing anything other than following the law. The majority of companies reported that they comply with all demands from the government, while only a few seemed to try to negotiate these demands. All of the companies surveyed reported being sensitive to government demands and having to contend with censorship issues, all the while insisting that they adhered to high standards of privacy and security (Maréchal et al., 2015; Petrova, Fossato, Indina, Dokuka, & Asmolov, 2013).

The Russian government ensures the compliance of domestic companies in particular by holding them liable for banned, copyrighted or otherwise illegal content accessible through their services or platforms. This intermediary liability strongly incentivizes ICT companies to block or remove any content that might plausibly be deemed illegal, lest they suffer grave repercussions (Petrova et al., 2013). Indeed, protection rackets and related thuggery are endemic in Russia, and business owners can find themselves targeted for prosecutions of dubious legal merit simply because they have upset the wrong oligarch or FSB operative (Pomerantsev, 2014). Legal remedies are nonexistent in these cases, leaving submission and exile as the only viable options. The current context of quick legislative reform and uneven enforcement keeps companies—and their staff—in a state of constant uncertainty about the rules and the penalties for breaking them.

Foreign companies operating in Russia typically have deeper pockets, greater technical and managerial knowhow, and reduced vulnerability to physical threats compared to their domestic counterparts. Google closed its Russian engineering offices in late 2014 (Luhn, 2014), and a number of former high-level executives have left the country (author interview, 2016). Neither Facebook nor Twitter have offices in Russia (Masnick, 2014), and without local staff who could face retaliation, the American platforms have greater leeway to push back against demands for censorship or for user information. According to Twitter's Transparency Report, the company refused to comply with any of the 233 requests for user information it received from Moscow in 2014–2015 (Twitter, 2015, 2016), and complied with only 5% of takedown requests received in the second half of 2015 (Twitter, 2016). Similarly, Google only produced user information for 5% of Russian government requests in the first half of 2015, though it complied with 62% of takedown requests during that period (Google, 2016). Facebook didn't comply with any Russian requests for user information, and restricted 56 pieces of content. The company does not disclose the number of requests for content restriction it received (Facebook, 2016).

Unlike domestic Russian companies, Google and Facebook (though not Twitter) are members of the Global Network Initiative, employ legal teams and other experts dedicated to advancing their users' digital rights, and engage in public transparency reporting about these issues. These efforts should be supported and encouraged. But if these companies comply with data localization laws, their users' data will fall into SORM's net, particularly given SORM-3's more powerful DPI capabilities. If they refuse, Roskomnadzor may very well block the sites entirely, as at least some of its officials have wanted to do for years (Masnick, 2014).

LinkedIn became the first foreign social media company to be banned from Russia, in part due to noncompliance with the data localization law. Roskomnadzor had sued the social networking site, which was ac-

[2] The Center received much of its funding from Western charitable foundations, which it is now prohibited from doing under the Russian law on "foreign agents". Unsurprisingly, the Center has not been able to identify domestic sources of funding, and much of its former staff is now living in the West (author interview, 2016).

quired by Microsoft earlier in 2016, for illegally sharing the personal data of non-users without obtaining prior consent—a claim that, if true, would indeed put LinkedIn afoul of data management best practices. The suit also argued that LinkedIn did not comply with data localization requirements. In its August 4, 2016, ruling, the court ordered Russian authorities to "take steps" to limit access to the site, though as of late October it remained accessible to most users (Rothrock, 2016). LinkedIn lost its appeal in November, and Roskomnadzor required Apple and Google to remove the LinkedIn app from the Russian versions of their respective app stores (Kang & Benner, 2017; Scott, 2016). With Roskomnadzor due to begin proactively enforcing foreign companies' compliance with data localization in 2017, the decisions of U.S. ICT companies like Google, Facebook and Twitter will be a test of the firms' commitment to user privacy and freedom of expression.

7. Russian Information and Internet Policy at the International Level

Russian internet policy—in both the domestic and foreign policy spheres—is rooted in the premise that Western countries (mainly the U.S.) use the internet to overthrow governments in "countries where the opposition is too weak to mobilize protests" (Nocetti, 2015, p. 114)—or, in other words, countries living under authoritarian regimes. Russian foreign policy hews to a strict interpretation of Westphalian nation-state sovereignty, at the core of which is the principle of non-intervention.[3] The free and open internet threatens that principle, allowing foreign and potentially subversive viewpoints to circulate across Russia. The "color revolutions" of the early 21st century and the Arab Spring have further fueled concerns that the internet represents a threat to the status quo and that it poses a threat to Russian political leaders (Nocetti, 2015). Indeed, opposition groups led by Alexei Navalny used Facebook to coordinate street protests in the aftermath of the 2011 legislative elections, and while the protests failed to coalesce into a lasting social movement, such an outcome was not completely outside the realm of possibility (Soldatov & Borogan, 2015; White & McAllister, 2014). Moreover, there is good reason to believe that Putin sees the U.S., and specifically then-Secretary of State Hillary Clinton, as directly responsible for fomenting these protests. Under this paradigm, such interference in Russia's domestic politics constitutes a violation of national sovereignty tantamount to information warfare. Likewise, U.S. policy initiatives like democracy promotion and the Internet Freedom Agenda are seen as promoting political projects that are aligned with U.S. interests, almost invariably at the expense of Russia's own interests (Nocetti, 2015).

Digital rights and the free flow of information are thus doubly threatening to the Kremlin. Not only does the internet embolden and empower the domestic opposition, it is (from Putin's perspective) closely associated with the U.S. government, which has historically played a unique role in internet governance and is a major funder of the global digital rights movement. In Russia's Westphalian view of the world, nation-states are the only actors that matter, and that should matter, and the actions of all other actors (be they individuals, civil society organizations, or corporations) can be imputed to a government motivated by the accumulation of power. That is the logic behind the 2012 law "On foreign agents", which stigmatizes internationally-funded NGOs that criticize the Kremlin by labelling them as "traitors" or "spies" (Human Rights Watch, 2017).

The Kremlin responded to what it sees as an existential threat by launching a campaign to reshape its near-abroad in its image, most dramatically in Estonia and Ukraine. The European and American response was tepid, and Putin grew bolder. Before long, the Kremlin was providing financial and ideological support to far-right parties and movement across the European Union, including Viktor Orbán in Hungary, the Brexit "Leave" campaign, and pro-Russian candidates in Bulgaria and Moldova (Eichenwald, 2017; Oliphant, 2016). A transnational, neo-fascist, authoritarian movement grounded in ethno-nationalism was taking shape. And then, of course, there is Donald Trump. Early analysis suggests that Trump was initially no more than a "useful fool" to be used to discredit Hillary Clinton and cast doubts on her legitimacy as president, but after a series of astounding events, the election, of course, went another way. The 2017 elections in France and Germany will be the next tests.

French Russia expert Julien Nocetti (2015) argues that "Moscow is crucially involved in the politicization of global cyber issues, to a large extent owing to the inextricable interweaving of the Russian Federation's domestic and external affairs" (p. 112). He stresses that:

> The slogan "content as threat" encapsulates the Russian perception that digital technologies can be used as tools *against* Russia. In Russian documentation it is expressed more fully as the "threat of the use of content for influence on the socio-humanitarian sphere". The notion of content as threat is reinforced by the projection onto foreign partners of Russia's own preconceptions of how international relations work, and by the presumption that a primary aim of western powers is to disrupt and undermine Russia. (p. 116)

For many years, Russia simultaneously sought to constrain the use of this powerful weapon (information) through international norms and treaties even as it developed its own offensive capabilities, echoing its Cold War approach to nuclear weapons. Since 1998—shortly before Putin became president—Russia has proposed

[3] A Westphalian paradigm doesn't mean that a country won't interfere in another country's affairs; it means that any such intervention is considered an act of war.

annual UN resolutions prohibiting "information aggression", which Nocetti interprets to mean the use of ideas or ideology to undermine regime stability (2015, p. 122). This is only one example of Russian attempts to regulate the use of information under international law. At the same time, Russia uses the Shanghai Coordination Organization (SCO) to provide technical assistance and knowledge transfer to other illiberal regimes eager to up their information controls game. This authoritarians' club further includes China, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan, with several other countries having observer or dialogue partner status. Russia and China use the SCO to share new advances in repression with one another, as well as with the less powerful member states whose regimes they want to bolster (Diamond, Plattner, & Walker, 2016; Nocetti, 2015).

8. Edward Snowden

More than three years after his initial revelations, Edward Snowden's continued asylum in Russia remains perplexing for many observers, some of whom speculate that the former NSA contractor must be a Russian agent, even if a reluctant one. The Snowden camp categorically denies this, and available evidence strongly suggests that Snowden's arrival in Moscow was not of his own making. Shortly after coming out to the world as the source for the Guardian and Washington Post stories about NSA surveillance, Snowden left Hong Kong for Latin America, with a layover in Moscow. He was accompanied by WikiLeaks's Sarah Harrison, who was apparently sent by Julian Assange to help escort Snowden to safety. There are only so many options for this route, and Moscow seemed to pose the fewest risks of being intercepted by U.S. officials. Unfortunately for Snowden, his passport was revoked while he was in the air, and he was stuck within the Moscow airport for 39 days while his asylum application was processed. Snowden was granted temporary asylum in Russia for a year, followed by a three-year residency permit in 2014 that was later extended to 2020 (Greenwald, 2014; Harding, 2014; Sharkov, 2016; Williams & Toropin, 2017).

As the world grappled with the unprecedented revelations of U.S. spying, and the key role played by internet platforms and telecommunications companies in collection programs like PRISM, governments explored ways to protect their citizens from the NSA's reach. Data localization schemes were proposed by countries as varied as Brazil, China, France, Germany, South Korea and Russia with the stated aim of ameliorating privacy risks from foreign surveillance. But in Russia at least, data localization laws "leveraged the public outrage and the heightened privacy concerns caused by the NSA spying to extend their control over data and their surveillance potential by data localization" (Sargsyan, 2016). The Kremlin thus seized the Snowden revelations, as well as his presence in Moscow, as an opportunity to craft a narrative that furthered its political objective: to portray the U.S. and its allies as the real adversaries of privacy and individual autonomy while continuing to intensify domestic censorship, surveillance, and the dismantling of Russian civil society. Meanwhile, Snowden has been an outspoken critic of Russian policy (Nechepurenko, 2016).

9. Analysis: Understanding Russia's Networked Authoritarianism

The key to understanding Russian internet policy is that it is part and parcel of an overall information control policy, the goal of which is the accumulation of power and wealth for Russia's kleptocratic elites. The global practice of information controls has undergone three generational shifts in rapid succession (Deibert, Palfrey, Rohozinski, & Zittrain, 2010). First generation controls prevent the population from accessing forbidden content, either through barriers to access or by blocking specific websites or pages. China's "Great Firewall" is a classic example of first generation information controls, and the Roskomnadzor blacklist is a poorly executed example of the same. The second generation involves creating legal and technical frameworks allowing public and private authorities to deny access to information on a case-by-case basis. "Just-in-time" blocking and sporadic internet shutdowns linked to specific political events exemplify this method. Third-generation controls combine legal and technical means with a proactive public relations (or propaganda) strategy: "it is less a matter of refusing access as of competing with potential threats through effective counter-information campaigns which discredit or demoralize the opponent" (Deibert et al., p. 16). The Kremlin's army of online trolls and use of broadcast and online media for domestic and external propaganda exemplify such third-generation controls. Deibert further identifies advocating for illiberal practices in internet governance arenas as a possible fourth generation of information controls (Deibert, 2016). This is already a core part of Russian foreign policy, as discussed above. The result is "networked authoritarianism" (MacKinnon, 2011), a political system that leverages ICTs and media regulation to carefully control the expression of dissent in a way that gives the impression of limited freedom of expression without allowing dissent to gain traction. Russia has long been "on the cutting edge of techniques aimed to control online speech with little or no direct filtering" (p. 43).

While historically Russia has indeed eschewed the more heavy-handed information controls in favor of second- and third-generation tactics, since Putin's 2012 return to the presidency—preceded by popular demonstrations that shared many characteristics of successful "color" revolutions (White & McAllister, 2014)—there have been increasing signs that the gloves are coming off. Google chairman Eric Schmidt worried as early as 2013 that Russia was beginning to copy China in internet censorship (Luhn, 2014), while SORM-3 and data localization requirements (including the LinkedIn ban) are further indications that the Kremlin is serious about controlling information within its borders. At the international level, Russia is normalizing and helping to spread networked authoritarianism through various strategies in internet governance fora, at the UN, and through the Shanghai Cooperation Organization "authoritarians' club" (see Pearce & Kendzior, 2012, for an examination of networked authoritarianism in Azerbaijan). At the same time, it has been waging a slow, covert campaign to dismantle the transatlantic alliance using "information weapons" honed in its near-abroad, most famously in Ukraine but also in Moldova. If information has always been political, today it is geopolitical and weaponized.

If true, the allegations of Russian interference in Western elections, including the 2016 U.S. presidential contest, would clearly constitute a pattern of "information aggression". Russia may be trying to give its adversaries a taste of as their own medicine (as the Kremlin sees it), or it may be teaching the world an object lesson on the dangers of the free flow of information. It is also possible that having failed to garner support for a norm against informational violations of state sovereignty, Russia decided to use that powerful weapon to reshape the international system to better fit its authoritarian, Westphalian worldview. Regardless of the grand strategy pursued by Putin, the tactics used insidiously turned open societies' strengths—pluralism, free expression, acceptance of diversity—against them at a time when they were especially vulnerable. Indeed, in the aftermath of the 2008 financial crisis the economic recovery has left too many behind, for which many Americans blame coastal elites and the incumbent Democrats. Populist contestations of capitalism, including the surveillance capitalism that powers the internet economy (Zuboff, 2015), open a door for competing political projects like the far-right ethno-nationalisms gaining ground across Europe and, of course, the Trump phenomenon—itself no stranger to xenophobia and white supremacist themes. Liberal democracies' policy responses must navigate between Scylla and Charibdis, facing down the threat of far-right extremism without developing our own version of networked authoritarianism.

10. Towards a Geopolitics of Information

As early as 2012, Rebecca MacKinnon predicted that "in the twenty-first century, many of the most acute political and geopolitical struggles will involve access to and control of information" (2012, p. XXV). Geopolitical debates about the flow of information typically pit champions of free expression and access to information against those who want to see state sovereignty replicated in cyberspace. There are shades of gray between those positions, of course, but it is nevertheless an ideological division that should be taken seriously. As Shawn Powers and Michael Jablonski note in their book about the Internet Freedom Agenda:

> The real cyber war is not over offensive capabilities or cybersecurity but rather about legitimizing existing institutions and norms governing Internet industries in order to assure their continued market dominance and profitability….While heavy-handed government controls over the Internet should be resisted, so should a system whereby Internet connectivity requires the systematic transfer of wealth from the developing world to the developed. (Powers & Jablonski, 2015, p. 24)

Powers and Jablonski thus identify two internet-mediated threats to human wellbeing: information controls (Crete-Nishihata, Deibert, & Senft, 2013) and surveillance capitalism (Zuboff, 2015). The former represents a threat from the state, while the latter is best understood as a threat from capitalism. This article has described a third threat: information warfare, a threat from external adversaries who strategically use information to achieve geopolitical goals—or, as defined by the former head of the Directorate for Electronic Warfare of the Russian Main Naval Staff, "securing national policy objectives both in peacetime and in wartime through means and techniques of influencing the information resources of the opposing side" (Pomerantsev, 2016, p. 181).

However, it is important not to succumb to false equivalencies that equate civic activities (like teaching people how to run elections) with the present moment—the stuff of dystopian science fiction. U.S. democracy promotion and the Internet Freedom Agenda undoubtedly support regime change in a number of countries by bolstering alternative political projects (author interview with Daniel Sepulveda, 2015), however that is far from being the only reason for supporting fair elections or the open internet. In many cases, the U.S. is less interested in supporting a specific alternative to the incumbent regime than it is in opening markets for U.S. companies, and many individual policymakers and bureaucrats genuinely embrace the ideals of access to information, free expression, and accountable democracy (Powers & Jablonski, 2015). Moreover, there is no evidence that domestic demands for free and fair elections, or a free and open internet, are anything other than genuine, including in Russia.

The past several years have seen a shift from a normative debate between the "free flow" and "online sovereignty" camps, to carefully plotted intervention. President Barack Obama noted in a 2009 speech that "the great irony of the information age" is that "those states that have most successfully adopted and exploited the opportunities afforded by the Internet are also the most vulnerable to range of threats that accompany it" (Carr, 2016, p. 2). Indeed, the Russian campaign's two greatest ostensible victories to date, the British "Brexit" vote and Donald Trump's victory, took place in deeply connected societies. If politics is war by other means, then we might call this terrorism by other means. Like terrorism, information warfare turns open societies against themselves, creating chaos and breeding suspicion. Without knowing friend from foe, or credible analysis from "fake news", societies become paralyzed, unable to coordinate against a shape-shifting enemy that many doubt is even there. For scholar Madeline Carr, "No previous technology has been regarded concurrently as a source of power and vulnerability in quite the way that the Internet has" (Carr, 2016, p. 2).

Monroe Price's (2015) examination of "the new strategic communication" provides a useful framework for understanding the new geopolitics of information. The concept almost seems tailor-made for the current crisis: strategic communication is a "consolidating relationship between information and power" that is "heavily subsidized, usually transnational, engineered and often deceptive" (p. 7), and it is "sensitive to the particular environment in which the information intervention takes place" (p. 9). This describes Russian intervention in Western elections perfectly. Price argues that the affordances of ICTs have "raised the consequences and possibilities of strategic communication to new levels" (p. 1), empowering states to "experiment with ways to 'move the needle' of public opinion among targeted populations utilizing advanced tools of communication and [to] integrate the consequences in their theories of speech and conduct" (p. 3). Having failed to secure an international agreement circumscribing transnational communication, Russia resolved to use "information weapons" first in the pursuit of its strategic objectives, with apparent success.

At least part of that success can be traced to the state of our media ecosystem. Before Facebook launched in 2005, "the often unstated assumption was that [information intermediaries like newspapers and television networks] would function (or would be obligated to function) as guardians of the public interest" (Price, 2015, p. 35). The system was far from perfect, but by and large media institutions took their gatekeeping role seriously, and followed a highly developed code of journalism ethics.

Today's intermediaries have no such ethical code, and some explicitly reject a sense of responsibility for their platforms' impact on society, as Facebook's Mark Zuckerberg did at several points during the 2016 U.S. presidential campaign (Zuckerberg, 2016). Further complicating matters, the most visible intermediaries have a global footprint: how does a profit-seeking corporation, lacking any appetite to perform journalistic functions, determine what is in the best interest of humanity?

Meanwhile, traditional media outlets have lost advertising revenues and audience shares to social media platforms, and in their weakened financial state have been absorbed by vertically integrated media conglomerates motivated by financial gain (McChesney, 2013; Pickard, 2014, 2017). The quality of discourse suffers, and the public struggles to parse truth from falsehood, opinion from fact. The "marketplace of ideas" is flooded with mediocre fare that anyone can access for free. Journalists struggle to make a living, and would-be members of the Fourth Estate flock to careers in public relations. The "quality control" on the public sphere erodes inexorably, leaving public discourse vulnerable to manipulation.

Price introduces the concept of "strategic architectures", which he defines as "large-scale efforts to fix or stabilize the relationship of states and other major players to information flows" (p. 9):

> These wholesale approaches include active rethinking of communications structures by powerful states so as to maintain control over their own narratives and affect relevant communications systems outside their borders. These are designs not only of government but of the corporate empires for whom communication is key and certainly for the media companies themselves. For those who seek to ensure a particular narrative—for example, of governmental legitimacy, religious authenticity, or the advantages of consumerism—establishing an infrastructure they can control is significant. (Price, 2015, pp. 9–10)

As John Gilmore said in 1993, the free and open global internet treats censorship as damage and routes around it, presenting a threat to networked authoritarianism. The threat would have been even greater if it had been embraced and promoted by a hegemonic power, as would doubtless have been the case under a Hillary Clinton presidency. The Kremlin saw undermining her presidency, and Americans' faith in democracy, as a geopolitical imperative, and established a strategic infrastructure to spread messages that would favor her opponent, Donald Trump, whose authoritarian predisposition, ignorance of global affairs, and business ties to Russia further increased his value as a "useful fool" (Davidson, 2016; Miller & Entous, 2017) The early days of the Trump presidency show no indication that the 45th president will respect, much less support, a free press or open internet.

11. Conclusion

The brewing conflict between Vladimir Putin's regime and the liberal democracies of Europe and North America appears to pit two conflicting paradigms about the role of information—distributed via the internet—in society (Zuboff, 2015). This article has described Russia's historical and contemporary approaches to controlling the flow of information, both domestically and at the international level, to argue that Russia does not view internet governance, cybersecurity, and media policy as separate domains. Rather, all the areas covered by those disciplines falls under "information security" for Russian foreign policy. Domestic surveillance, content censorship and illiberal internet governance reform are deeply connected to misinformation campaigns abroad, and are used strategically to achieve geopolitical goals.

Despite all its flaws, liberal democracy is still the best form of governance available if the goal is to ensure human rights and economic prosperity. Just as networked authoritarianism establishes strategic infrastructures to control the message domestically and intervene in global media systems, we need to rethink our media and communication infrastructures to ensure they foster a pluralist, rights-respecting society that is resilient to authoritarianism and extremism. Governments, corporations, civil society organizations and the public all have roles to play in this endeavor.

Moreover, the liberal democracies of Europe and North America need significant reforms to fulfill their promises to their citizens if they are to survive. In the U.S., Barack Obama's presidency was a solid, albeit imperfect, start that a majority of voters endorsed by voting for Hillary Clinton. Scholars of all disciplines should consider how their work can support the positive reforms that our democracies urgently need, counter the forces of authoritarianism, and actively participate in the shared work of governance.

Acknowledgements

The author gratefully acknowledges Griffin Boyce, Sergei Hovyadinov, Priya Kumar, Jeff Landale, Tanya Lokot, Rebecca MacKinnon, and Sarah Myers West for their comments at various stages of this manuscript, as well as the issue editors and anonymous reviewers.

Conflict of Interests

The author declares no conflict of interests.

References

Access Now. (2016). *#KeepItOn*. Retrieved from https://www.accessnow.org/keepiton

Bowles, A. (2006). The changing face of the RuNet. In H. Schmidt, K. Teubener, & N. Konradova (Eds.), *Control + shift. Public and private usages of the Russian internet* (pp. 21–33). Norderstedt: Books on Demand.

Carr, M. (2016). *US Power and the internet in international relations*. New York, NY: Palgrave Macmillan.

Castells, M., & Kiselyova, E. (1995). *The collapse of Soviet communism: A view from the information society*. Los Angeles, CA: Figueroa Press.

Citizen Lab. (2015). *Citizen Lab summer institute*. Retrieved from http://citizenlab.org/summerinstitute

Crete-Nishihata, M., Deibert, R., & Senft, A. (2013). Not by technical means alone: The multidisciplinary challenge of studying information controls. *IEEE Internet Computing*, *17*(3), 34–41. doi:10.1109/MIC.2013.29

Davidson, J. D. (2016, August 31). Russia's cyber warfare has bigger aims than electing Donald Trump. *The Federalist*. Retrieved from http://thefederalist.com/2016/08/31/russias-disinformation-operations-aim-to-undermine-american-democracy

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: MIT Press.

Deibert, R. (2016). Cyberspace under siege. In L. Diamond, M. F. Plattner, & C. Walker (Eds.), *Authoritarianism goes global: The challenge to democracy* (pp. 198–215). Baltimore, MD: Johns Hopkins University Press.

DeNardis, L. (2014). *The global war for internet governance*. New Haven, CT: Yale University Press.

Diamond, L. J., Plattner, M. F., & Walker, C. (Eds.). (2016). *Authoritarianism goes global: The challenge to democracy*. Baltimore, MD: Johns Hopkins University Press.

Duffy, N. (2015). *Internet freedom in Vladimir Putin's Russia: The noose tightens*. Washington, DC: American Enterprise Institute.

Eichenwald, K. (2017, January 10). Trump, Putin and the hidden history of how Russia interfered in the U.S. presidential election. *Newsweek*. Retrieved from http://www.newsweek.com/trump-putin-russia-interfered-presidential-election-541302

Facebook. (2016). *Global government requests report*. Retrieved from https://govtrequests.facebook.com

Freedom House. (2015). Freedom on the net. *Freedom House*. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2015

Freedom House. (2016). Freedom on the net. *Freedom House*. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2016

Google. (2016). *Transparency report*. Retrieved from https://www.google.com/transparencyreport/?authuser=1

Gorny, E. (2007). *The Russian internet: Between kitchen-table talks and the public sphere*. Boston, MA: Art Margins.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York, NY: Henry Holt and Co.

Habermas, J. (1989). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*. Cambridge, MA: MIT Press.

Hanson, E. C. (2008). *The information revolution and world politics*. Lanham, MD: Rowman & Littlefield.

Harding, L. (2014). *The Snowden files: The inside story of the world's most wanted man*. New York, NY: Vintage Books.

Howard, P. N., & Hussain, M. M. (2013). *Democracy's fourth wave? Digital media and the Arab Spring*. Oxford and New York, NY: Oxford University Press.

Human Rights Watch. (2017, January 17). Russia: Government vs. rights groups. *The Battle Chronicle*. Retrieved from https://www.hrw.org/russia-government-against-rights-groups-battle-chronicle

Kang, C., & Benner, K. (2017, January 6). Russia requires Apple and Google to remove LinkedIn from local App Stores. *The New York Times*. Retrieved from https://www.nytimes.com/2017/01/06/technology/linkedin-blocked-in-russia.html

Karlekar, K., & Cook, S. (2009). *Access and control: A growing diversity of threats to internet freedom*. Washington, DC: Freedom House.

Kratasjuk, E. (2006). Construction of "reality" in Russian mass media news on television and on the Internet. In H. Schmidt, K. Teubener, & N. Konradova (Eds.), *Control + shift. Public and private usages of the Russian internet* (pp. 34–50). Norderstedt: Books on Demand.

Labott, E. (2011, December 6). Clinton cites "serious concerns" about Russian election. *CNN*. Retrieved from http://www.cnn.com/2011/12/06/world/europe/russia-elections-clinton

Lokshina, T. (2016, July 7). Draconian law rammed through Russian parliament: Outrageous provisions to curb speech, privacy, freedom of conscience. *Human Rights Watch*. Retrieved from https://www.hrw.org/news/2016/06/23/draconian-law-rammed-through-russian-parliament

Luhn, A. (2014, December 12). Google to close engineering office in Russia as internet restrictions bite. *The Guardian*. Retrieved from http://www.theguardian.com/world/2014/dec/12/google-closes-engineering-office-russia

MacKinnon, R. (2011). China's "networked authoritarianism". *Journal of Democracy*, *22*(2), 32–46.

MacKinnon, R. (2012). *Consent of the networked: The world-wide struggle for Internet freedom*. New York, NY: Basic Books.

MacKinnon, R., Hickock, E., Bar, A., & Lim, H. (2014). *Fostering freedom online: The role of internet intermediaries*. Paris: UNESCO.

Maréchal, N., MacKinnon, R., Bar, A., Kumar, P., Mendes de Almeida Bottino, C. B., Micek, P., . . . Wanstreet, R. (2015). *Case study research: Laying the groundwork for the methodology*. Washington, DC: New America Open Technology Institute. Retrieved from https://rankingdigitalrights.org/wp-content/uploads/2015/02/RDR-Case-studies.pdf

Masnick, M. (2014, May 16). Russian official threatens to block Twitter and Facebook in Russia. *Tech Dirt*. Retrieved from https://www.techdirt.com/articles/20140516/06421727254/russian-official-threatens-to-block-twitter-facebook-russia.shtml

McChesney, R. W. (2013). *Digital disconnect: How capitalism is turning the Internet against democracy*. New York, NY: The New Press.

Miller, G., & Entous, A. (2017, January 6). Declassified report says Putin "ordered" effort to undermine faith in U.S. election and help Trump. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/intelligence-chiefs-expected-in-new-york-to-brief-trump-on-russian-hacking/2017/01/06/5f591416-d41a-11e6-9cb0-54ab630851e8_story.html?utm_term=.8ec13fc7ff94

Nechepurenko, I. (2016, June 27). Edward Snowden criticizes "Big Brother" measure in Russia. *The New York Times*. Retrieved from https://www.nytimes.com/2016/06/28/world/europe/edward-snowden-criticizes-big-brother-measure-in-russia.html

Nisbet, E. (2015). *Benchmarking public demand: Russia's appetite for Information control*. Philadelphia, PA: Center for Global Communication Studies.

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

Ognyanova, K. (2015). In Putin's Russia, information has you: Media control and internet censorship. In M. M. Merviö (Ed.), *Management and participation in the public sphere* (pp. 62–78). Hershey, PA: IGI Global.

Oliphant, R. (2016, November 14). Pro-Russian candidates win presidential votes in Bulgaria and Moldova. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/2016/11/14/pro-russian-candidates-win-presidential-votes-in-bulgaria-and-mo

Paganini, P. (2014). New powers for the Russian surveillance system SORM-2. *Security Affairs*. Retrieved from http://securityaffairs.co/wordpress/27611/digital-id/new-powers-sorm-2.html

Pearce, K. E., & Kendzior, S. (2012). Networked authoritarianism and social media in Azerbaijan. *Journal of Communication*, *62*(2), 283–298. doi:10.1111/j.1460-2466.2012.01633.x

Petrova, M., Fossato, F., Indina, T., Dokuka, S., & Asmolov, G. (2013). *Ranking digital rights report: Russia* (Unpublished Report). Moscow: Center for the Study of New Media and Society.

Pickard, V. W. (2014). *America's battle for media democracy: The triumph of corporate libertarianism and the future of media reform*. New York, NY: Cambridge University Press.

Pickard, V. W. (2017, January 30). The problem with our media is extreme commercialism. *The Nation*. Retrieved from https://www.thenation.com/article/the-problem-with-our-media-is-extreme-commercialism

Pomerantsev, P. (2014). *Nothing is true and everything is possible: The surreal heart of the new Russia* (1st ed.). New York, NY: PublicAffairs.

Pomerantsev, P. (2016). The Kremlin's information war. In L. Diamond, M. F. Plattner, & C. Walker (Eds.), *Authoritarianism goes global: The challenge to democracy* (pp. 174–186). Baltimore, MD: Johns Hopkins University Press.

Powers, S. M., & Jablonski, M. (2015). *The real cyber war: The political economy of internet freedom*. Urbana, IL: University of Illinois Press.

Price, M. E. (2015). *Free expression, globalism, and the new strategic communication*. New York, NY: Cambridge University Press.

Rohlenko, D. (2007). *The first Russian printed newspaper*. Science and Life.

Rothrock, K. (2016, October 25). Russia is reportedly banning LinkedIn. *Global Voices*. Retrieved from https://globalvoices.org/2016/10/25/russia-is-reportedly-banning-linkedin

Sargsyan, T. (2016). Data localization and the role of infrastructure for surveillance, privacy, and security. *International Journal of Communication*, *10*, 2221–2237.

Scott, M. (2016, November 10). Russia prepares to block LinkedIn after court ruling. *The New York Times*. Retrieved from https://www.nytimes.com/2016/11/11/technology/russia-linkedin-data-court-blocked.html?_r=0

Sharkov, D. (2016, April 14). Kremlin rebuffs Donald Trump's Edward Snowden "spy" claims. *Newsweek*. Retrieved from http://www.newsweek.com/kremlin-rebuffs-donald-trumps-snowden-claims-433332

Smith, D., & Walker, S. (2016, March 10). Former Putin press minister died of blow to head in Washington hotel. *The Guardian*. Retrieved from http://www.theguardian.com/world/2016/mar/10/mikhail-lesin-blunt-force-trauma-death-washington-dc-vladi mir-putin

Soldatov, A., & Borogan, I. (2012). The Kremlin's new internet surveillance plan goes live today. *Wired*. Retrieved from https://www.wired.com/2012/11/russia-surveillance

Soldatov, A., & Borogan, I. (2013). Russia's surveillance state. *World Policy Journal*. Retrieved from http://www.worldpolicy.org/journal/fall2013/Russia-surveillance

Soldatov, A., & Borogan, I. (2015). *The red web: The struggle between Russia's digital dictators and the new online revolutionaries* (1st ed.). New York, NY: PublicAffairs.

Twitter. (2015). *Transparency report*. Retrieved from https://transparency.twitter.com/en.html

Twitter. (2016). *Transparency report*. Retrieved from https://transparency.twitter.com/en.html

White, S., & McAllister, I. (2014). Did Russia (nearly) have a Facebook revolution in 2011? Social media's challenge to authoritarianism. *Politics*, *34*(1), 72–84. doi:10.1111/1467-9256.12037

Williams, J., & Toropin, K. (2017, January 18). Russia extends Edward Snowden's asylum to 2020. *CNN*. Retrieved from http://www.cnn.com/2017/01/18/europe/russia-snowden-asylum-extension

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. doi:10.1057/jit.2015.5

Zuckerberg, M. (2016, November 12). *Facebook post*. Retrieved from https://www.facebook.com/zuck/posts/10103253901916271

About the Author

Nathalie Maréchal is a doctoral candidate at the University of Southern California's Annenberg School for Communication and Journalism and Senior Research Fellow at Ranking Digital Rights. She researches the intersection of internet policy and human rights, and is writing a dissertation on the political economy of digital rights technology. Nathalie's work has been published in the *International Journal of Communication*, *Media and Communication*, the *Fibreculture Journal*, and by the Global Commission on Internet Governance. She frequently speaks at international conferences about issues related to data, society and human rights.

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 42–53
DOI: 10.17645/mac.v5i1.816

Article

Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era

Ksenia Ermoshina and Francesca Musiani *

Institute for Communication Sciences, 75013 Paris, France; E-Mails: ksenia.ermoshina@cnrs.fr (K.E.), francesca.musiani@cnrs.fr (F.M.)

* Corresponding author

Submitted: 4 November 2016 | Accepted: 23 January 2017 | Published: 22 March 2017

Abstract

In response to the growing censorship of their national Internet, Russian users, content producers and service providers have developed several resistance tactics. This paper analyzes these tactics with particular attention paid to their materiality. It first addresses the different levels of Internet "governance by infrastructure" in Russia, then focuses on the different tactics of individual and collective resistance and concludes by discussing how forms of control enacted at different levels of infrastructure are reconfiguring the geopolitics of the Russian Internet.

Keywords

digital sovereignty; Edward Snowden; Internet geopolitics; Internet governance; Internet infrastructure; resistance; Russian Internet

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).

1. Introduction

The last two decades of Russian Internet (RuNet)'s development have showed a paradoxical situation where a rapidly developing[1] Internet coexisted with a state-centered Internet governance. A "half-freedom of speech" (Gelman, 2010) was associated with the hope of a democratization of the country (Elting et al., 2010; Lonkila, 2012). However, after the defeat of the protest movement "For Fair Elections" (2011–2012), these democratic expectations were questioned. The Kremlin started seeing the Internet "as politically disruptive because it enables citizens to circumvent government-controlled 'traditional' media" (Nocetti, 2015, p. 113).

Recent developments in RuNet regulation demonstrate the government's will to establish national control of the digital sphere (Freiberg, 2014; Nocetti, 2015). The presidential administration organized an "Internet + Sovereignty" forum in May 2016 around issues of national governance of the Internet of Things (IoT) and Big Data, promoting a project of Russian standards and the possibility of building a closed national network in the field of IoT. The intention to develop a "sovereign Internet" was also proposed as a double response to the terrorist threat and the domination of American web services.

However, the laws that frame online activities of Russian users are diverse and constantly evolving as a patchwork of incomplete measures that overlap and sometimes contradict each other. Each of these measures challenges IT professionals, e.g. Internet service providers, hosting providers, developers, journalists, bloggers and NGOs. Simultaneously, a set of individual practices, know-how, or *arts de faire*, is being developed by RuNet users to bypass access restrictions or protect their communications from governmental surveillance.

[1] 75% of population are said to have Internet access in 2016.

Emerging NGOs and associations promote and institutionalize some of these hacks and launch large-scale campaigns for RuNet freedom.

In light of this context, the central research aim of this paper is to understand the connection between the "State-centered" style of Russian Internet governance and the local tactics of *détournement* and bricolage (Akrich, 1998). Our hypothesis is that in the Russian case, resistance to Internet control and surveillance happens not only and not *primarily* at the political and legal levels (e.g. lobbying or negotiations with governmental structures, class action or collective mobilizations) but at the level of everyday individual practices of usage, such as anonymization of users or migration of people and infrastructures. A specific body of research dedicated to local social movements in contemporary Russia (Erpyleva & Magun, 2014; Kharkhordin, 2011; Prozorov, 2012; Zhuravlev, Savelyeva, & Yerpylova, 2014) is helpful to analyze this style of contention: indeed, this research analyzes post-Soviet de-politicization as the consequence of an "exodus" from the public sphere to the private sphere. It shows that Russian civil society tends to mobilize around local problems, often related to the materiality of the city (Ceruzzi, 2006) rather than to support global challenges; for example, bottom-up activities of repair and maintenance of a particular district or equipment in the city will be favored over a protest against the Mayor of the same city. In this sense, and along the lines of recent scholarship such as Klyueva's (2016), the article is also an attempt to understand the specificities of the response of Russian civil society—with its mix of collective and individual tactics of resistance—to restrictive Internet policies.

The structure of the paper is as follows. First, it addresses the different levels of Internet "governance by infrastructure" (DeNardis & Musiani, 2016), in Russia—showing how the Russian State is increasingly leveraging, co-opting and on occasion "tampering with", Internet infrastructure in order to fulfill political aims that, in some instances, are sensibly different than the objectives the infrastructure was originally meant for. Then, the paper focuses on the different tactics of individual and collective resistance, and concludes with a discussion of how the forms of control enacted at different levels of RuNet infrastructure are reconfiguring its geopolitics.

The paper builds upon observations of "cryptoparties", on original interviews with Russian IT-specialists, Internet service providers (ISPs) and expatriate journalists and developers, and situates this material by means of a brief analysis of Russian Internet legislation. More specifically, the empirical part of the research combined several methods: observation of three cryptoparties in 2012, 2015 and 2016—the purpose of these observations being to analyze different tools used in order to protect anonymity and bypass censorship, as well as the discourse organizers and participants were developing about Internet regulations in Russia; interviews with 3 internet service providers, 4 expatriated developers, 1 NGO organizer and a dozen users. The interviews were semi-structured with grids adapted to providers, developers and users, and lasted between 40 minutes and 2 hours. Qualitative analyses of relevant press materials and Web ethnographies analyzing professional forums of ISPs as well as the biggest Internet resources dedicated to Internet Freedom in Russia (such as Moskovskiy Libertarium or Rublacklist) were also conducted.

2. Surveillance, Data Storage and Filtering: Levels of Infrastructure-Based Internet Control in Russia

RuNet governance has developed upon several layers, with three main types of measures adopted since 1998:

a) Surveillance measures of 'lawful interception', called System of Operative Investigative Measures (SORM), aimed at giving governmental services such as FSB (former KGB) access to private communications both by telephone and on the Internet;[2]
b) Regulation of data storage, restricting important data flows to national borders;
c) Filtering measures, restricting access to a growing list of websites (blacklist)[3] considered as extremist. These three layers are interconnected and show a global tendency towards a RuNet "balkanization"—hyper-localization and nation-state regulation of data and communication flows.

2.1. "SORMisation" of Russia: Surveillance Measures and ISP Markets

The SORM was first implemented in Russia in 1998. SORM provides an architecture by which law enforcement and intelligence agencies can obtain direct access to data on commercial networks. During the past eight years, SORM has given rise to new configurations of sociotechnical "actants" (Latour, 1988) with long-term consequences on the market of ISPs. Three generations of SORM measures have seen the light. SORM-1 allows FSB to access telephone traffic, including mobile networks. SORM-2, implemented in 2005, is responsible for inter-

[2] Apart from FSB and Roskomnadzor, MVD (Ministry of Internal Affairs), FSO (Federal Service of Security), FSKN (Federal Service for Control of Drug Traffic), FTS (Federal Customs Service) and FSIN (Federal Penitentiary Service) also participate in online surveillance in Russia. However, while MVD, FSB and FSKN both possess the equipment and have the right to use it for lawful interception, FSO and FTS depend on FSB to have an access to the equipment, while FSIN has the equipment but does not have the right to use it for investigative activities. Apart from state actors regulating online surveillance, a market of surveillance equipment has been developing in recent years (especially since the adoption of SORM-3 measures). Several private companies seem to play the most important role in this field: "Special technologies" and "MFI-Soft" (who earn 5–6 billion rubles a year on SORM equipment) and smaller manufacturers (Reanet, Norsi-Trans and TechArgos each earning 1 billion rubles a year). The most recent player on the market is the State corporation RosTech, supposed to produce the necessary equipment to implement Yarovaya law.

[3] Officially called "Unified Register of Domain Names, Internet Website Page Locators, and Network Addresses that Allow to Identify Internet Websites Containing Information Prohibited for Distribution in the Russian Federation" (or Unified Register).

cepting IP traffic, including VoIP. SORM-3, implemented in 2014, gathers information from all communication media, and offers long-term and comprehensive storage of subscriber data (Privacy International, 2016).

Compared to international Lawful Interception standards, SORM gives great autonomy to surveillance actors. In most Western countries, law enforcement agencies seek a warrant from a court and then issue an order for lawful interception to a network operator or ISP, which is obliged to intercept and deliver the requested information. The FSB does not need to contact the ISP because of the very architecture of SORM, containing two main elements: the "extractor" (the equipment—software and hardware—that performs data extraction) and the "remote control station". The control station is localized in the FSB regional office and enables remote control of the extractor without the provider's permission: the provider may not know which data, and how, is intercepted, analyzed and transferred. No court decision is necessary in order to activate the interception of the metadata. However, in order to access the actual telephone recordings, FSB has to ask for a court permission. In 2012, there were 372,144 orders distributed, according to the official data provided by the Supreme Court.[4]

The most expensive component of SORM is the circular buffer for data storage. However, each new generation of SORM measures has changed the technical requirements: while for SORM-2 providers needed to store all the traffic for 12 hours, SORM-3 obliged them to store all the metadata for three years. Thus, the providers have to change all their equipment as the implementation of SORM systems completely relies on them: "We pay for it", remarks internet provider Michael I. "If you do not put this equipment, you do not have license and you lose state clients".

When the local FSB or prosecutor's office identifies shortcomings, they send the information to Roskomnadzor (the Federal Service for Supervision of Communications, Information Technology and Mass Media).[5] The ISP is warned, first fined, then if violations persist, its license may be revoked (Borogan & Soldatov, 2013). Roskomnadzor statistics show that in 2010, there were 16 warnings, 13 in 2011, and 30 in 2012.[6]

Providers have to renew SORM equipment by themselves as no certified standards exist on the market and there is no consensus among manufacturers. As a result, providers have to adapt to the new technical demands, sometimes via DIY tinkering with old equipment: "Adapt the parts of your system, first of all…because when they will finally publish the certificates…we will have to spend tons of bucks again, and we will have to do it, because that's the Law",[7] notes user Andrei on 14 November 2015.

An inquiry led by Leonid Volkov, activist, blogger and programmer, claims that "a small provider has to give about 20%–30% of his annual income to buy SORM equipment" (Volkov, 2016). The two biggest manufacturers of SORM equipment earn 5–6 billion rubles per year on SORM, while three other small manufacturers earn about 1 billion. To reduce their costs, smaller providers buy SORM-as-a-service from their upstream providers. The implementation of SORM-1 in Russia sparked a protest campaign by IT-professionals, human rights organizations and Internet freedom defenders. The first anti-SORM movement was launched in the late 1990s in the form of a DDoS attack on FSB semantic analysis tools. Activists were adding specific keywords to every mail, such as "bomb", "explosion", "terrorist attack", triggering constant alerts to the control station and overloading it. Moscovskiy Libertarium,[8] with Russian and international partners, launched an international solidarity campaign against SORM. A public petition was sent to the Supreme Court and former Russian president Boris Yeltsin, asking him to "use his authority in order to stop the implementation of SORM", an "unprecedented example of violation of the rights to privacy and human rights convention".[9] While this campaign did not produce immediate results, fifteen years later the European Court of Human Rights has recognized that SORM was a violation to the European Convention of Human Rights, because its technical infrastructure enabled interception of communications without court permission, thus bypassing legal procedures.

The early-2000s anti-SORM campaign was mostly led by journalists, NGO activists and programmers, while providers were almost absent from the controversy, with the exception of "Bayard-Slaviya Communications". As Sergey Smirnov, activist of Pravozashitnaya Set (Human Rights Network), notes: "Internet service providers have come to the conclusion that the perspective to lose their license is much worse than the necessity to collaborate with FSB. In one of the recent publications about SORM, an FSB officer noticed that in the majority of cases providers apply all the requirements without any pressure and even demonstrate an understanding".[10] The

[4] According to the official statistics provided by the Supreme Court, in 2012, 372,144 orders were distributed, compared to 326,105 in 2011, 276,682 in 2010, 245,645 in 2009, 229,144 in 2008 and 189,591 in 2007: https://ria.ru/infografika/20130815/956535235.html

[5] Roskomnadzor is a Federal Executive Authority of the Russian Federation, performing the following functions: control and supervision of mass media (including electronic mass media), mass communications, information technology, and telecommunications; supervision and statutory compliance control of personal data processing; managing the Radio Frequency Service activities; supervision of production of copies of audiovisual works, computer software, databases and audio recordings on any media; accreditation of experts and expert organizations for content evaluation in order to ensure child information security. It is affiliated to the Ministry of Communications and Mass Media of the Russian Federation. The role of Roskomnadzor has recently expanded. The list of all its functions may be found on its official website: http://eng.rkn.gov.ru/about

[6] Available at https://rkn.gov.ru/press/annual_reports

[7] Available at http://forum.nag.ru/forum/index.php?showtopic=47641&st=560

[8] Available at http://www.libertarium.ru, created by Anatoliy Leventchuk in 1994.

[9] Available at http://www.libertarium.ru/l_sormact_gilc

[10] Available at http://www.libertarium.ru/l_sormact_conf6aprd

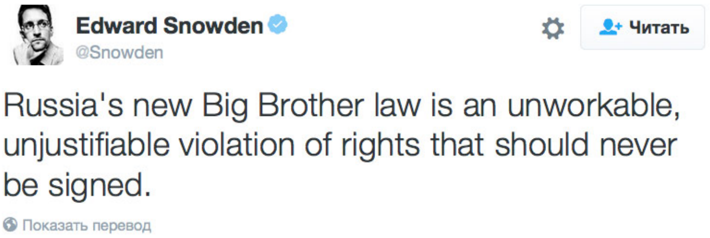
lack of providers in the anti-SORM movement made any civil disobedience movement technically impossible. In order to create a precedent, Leonid Volkov launched a campaign against SORM-3 in 2015; he started the so-called "Attack on SORM", a legal and political project of collective appeal to court by operators and providers, to demand better regulation of SORM and state-funded certified equipment.

2.1.1. Yarovaya Law: When Law (Unusually) Pre-Dates Technology

Nonetheless, the development of SORM legal and technical requirements created tensions in the ISP community. In June 2016, a new set of surveillance measures was proposed by Representative Irina Yarovaya: Russian telecom operators will have to store all traffic (including calls, letters, documents, images and video) for six months, and related metadata for three years. The importance of this case lies in its revealing a "reverse gap" between legal measures and financial and technical resources: while "governments are struggling to keep up with the pace of technological change, with technology evolving faster than law-making efforts" (Nocetti, 2015, p. 111), in the Yarovaya law case, law-making has outpaced the actual technological development of the country. Indeed, such surveillance needs a complex and multilayered technical infrastructure (including servers, the network itself, data storage systems and software), with far-reaching implications for the ways Internet and telecommunications work in Russia, including quality of connection, the speed at which and the amounts of data the network is able to transfer and the price of Internet services. Vladimir K., ISP, says: "Yarovaya law is technically absurd. Firstly, there is no necessary equipment on the market. Secondly, it is useless to store encrypted data. With the same success, we can code a random numbers generator and send this data to FSB pretending it is our users' traffic".

The problem is both technical and geopolitical, as it questions the limits of the Russian nation-state and its capabilities to implement a new infrastructure independently from the Western market. Within embargo, due to the Western sanctions imposed on Russia following the annexation of Crimea in 2014, the Russian government turns to national companies to produce the necessary equipment. The politics of "substitution of imports" coupled with the new series of surveillance laws have an important impact on the Russian IT-industry. The CEO of MGTS (Moscow State Telecom Network), Andrey Ershov, states: "Today we do not have any equipment in order to be able to put the 'Yarovaya law' into practice….So, the biggest concern that all telecom operators publicly express, is related to the cost of such solutions. [The equipment] is about tens of billion rubles". Even the emerging set of firms specialized in SORM equipment cannot satisfy Yarovaya law requirements in terms of equipment, estimated at 10.3 billion rubles (Kantyshev, 2016). Providers and telecom operators have publicly expressed their skepticism of the new surveillance law, pointing out that new solutions risk becoming obsolete within a few years and will demand further investment (Schepin, 2016). Press and specialized websites show a rise in disapproval of the Yarovaya law among IT professionals, for similar reasons. Among the actors criticizing the law are the biggest Russian IT companies, Mail.ru and Yandex, as well as professional associations Russian Association of Electronic Communications and Russian Civic Organization Center for Informational Technologies and even a pro-governmental working group "Communications and IT" ("Svyaz i IT"). The most popular professional forum of Russian providers, Nag.ru, creatively reacted to the law by developing a "Yarculator"[11], a software enabling providers to calculate the prices for the necessary equipment and the cost of Internet services for end users.

The law was largely contested by civil society. A petition on Change.org gathered 623,465 signatures as of 8 January 2017. A demonstration against the law was held in Moscow in August 2016 and gathered between 2,400 to 4,000 people (Kozlov & Filipenok, 2016). On his end, Edward Snowden publicly asked Putin not to sign the Yarovaya law, emphasizing its nefarious economic consequences and pointing out that a six-month storage of data is dangerous, unfeasible and expensive[12] (Figures 1 and 2).



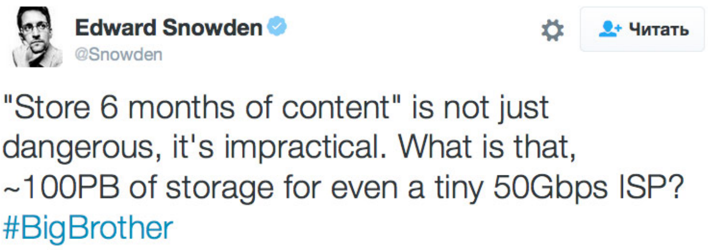
Edward Snowden
@Snowden

Russia's new Big Brother law is an unworkable, unjustifiable violation of rights that should never be signed.

Figure 1. Edward Snowden's critical tweet on the Yarovaya law.

[11] Available at http://nag.ru/articles/article/29513/-yarkulyator-kalkulyator-yarovoy.html#comments

[12] Available at http://www.macdigger.ru/iphone-ipod/snouden-raskritikoval-zakon-yarovoj-on-otnimet-u-rossiyan-dengi-i-svobodu.html



"Store 6 months of content" is not just dangerous, it's impractical. What is that, ~100PB of storage for even a tiny 50Gbps ISP? #BigBrother

Figure 2. Edward Snowden's critical tweet on the duration of data storage outlined in the Yarovaya law.

While SORM and Yarovaya law give FSB access to data stored on Russian servers without informing site owners or providers, it is more difficult to get access to foreign services, e.g. Facebook and Twitter. Thus, a set of new measures has been adopted to reconfigure data storage and transfer.

2.2. "Snowden Effect" on RuNet: Migrations of Personal Data

Snowden's revelations had a considerable effect on IT markets. The leaks "changed the way people perceive their personal data, and will cost internet corporations, especially American ones, millions of dollars" (Filonov, 2014). Indeed, in January 2014, Canadian provider Peer1 showed that 75 British and Canadian companies did not want to store their data in the US because of the fear of being tracked down by the surveillance services.[13] Internet companies started creating servers outside US territory.

Russian Internet users—particularly specific groups including developers and activists—were seemingly not caught unprepared by Snowden's revelations. SORM being well-known since the late 1990s to all active Internet users, it was not news for Russians that governments could track their communications without a court order. Maxim I., hosting provider with Komtet, notes: "His revelations were not a surprise for specialists….In Russia, and I am sure, in any country, it is possible to get whatever information about a user or his websites. Some RuNet users even joked about the role Snowden played in RuNet regulation: 'Why have they kept Snowden here?' Very simple. They just asked him about the downsides of the American system of surveillance and made a better one".[14]

Snowden's revelations attracted attention to existing surveillance practices and made it possible to compare SORM with the US system. However, the revelations' most important impact concerned the role of US cloud services and internet corporations. In response, the Russian government modified the "Law on storage and protection of personal data" and reconsidered data geopolitics to allegedly guarantee the "protection of Russian citizens' data from US government surveillance". Researcher-journalists Andrei Soldatov and Irina Borogan insist on the role that Snowden played in this: "Right on time, Edward Snowden appeared on the world stage. The NSA scandal made a perfect excuse for Russian authorities to launch a campaign to bring global web platforms such as Gmail and Facebook under Russian law—either requiring them to be accessible in Russia by the domain extension .ru, or obliging them to be hosted on Russian territory" (Borogan & Soldatov, 2013).

The law #242-FZ was adopted on 1 September 2014. It obliges providers to "store personal data of Russian citizens, used by internet services, on the territory of the Russian Federation". Providers must guarantee recording, systematization, accumulation, storage, updates, modifications and extraction of personal data using databases located on Russian territory.[15] Noncompliance with this new law may result in total blockage of the service. Thus, for example, in November 2016 LinkedIn was blocked in Russia (including mobile apps) for the violation of the new data storage policies. Web services are also required to build backdoors for Russian secret services to access stored data. Another way to put pressure on western companies is to block entire web services because they store "forbidden information". Thus, YouTube was blocked in Russia for hosting a video judged as extremist. Facebook removed a page called Club Suicide rather than seeing its entire network blacklisted. The repatriation of data illustrates the tendency of Russian internet governance towards "digital sovereignty" (Nocetti, 2015, p. 112).

Several resistance tactics have developed in response to these balkanization measures. A petition addressed to Google, Facebook and Twitter asks them not to oblige: "We don't trust the domestic security services that are in charge of data security once the data is in Russia. We're asking internet companies to withstand this pressure using all possible legal means and we are ready to support them".[16] Developers were immediately concerned, as the law attacked the instruments they were constantly using, such as GitHub, as well as their data storage practices. Another tactic deployed was a reorientation towards new products that would avoid storage of personal

[13] Available at http://go.peer1.com/rs/peer1/images/Peer1-Report-NSA-Survey-NA.pdf

[14] Available at http://www.yaplakal.com/forum1/st/75/topic1086610.html

[15] Available at http://www.garant.ru/news/648095/#ixzz4LqmT7iT8

[16] Available at https://www.change.org/p/facebook-google-twitter-don-t-move-personal-data-to-russia

data: "We try to make services that do not store user data, so that we do not have to store it on our servers", remarks Alexey P., developer, CTO of Progress Engine; "We have some apps that we make for TV, or for electronic wallets, where the data is stored on the servers of our clients". These are specific resistance tactics which we could call tactics of "evasion". In fact, instead of contesting the law #242-FZ by communicating directly with the Russian government, citizens either try to communicate with western IT companies (addressing petitions to Google and Facebook), or modify their own practices and professional activities in order to find legal gaps or grey zones (e.g. using APIs for authorization or third parties for user data storage, or repositioning their product in order to use no personal data at all).

Another step towards digital sovereignty was made in spring 2016 with an ambitious project of "state-in-the-middle": during the forum "IT + Sovereignty", the intended creation of state-owned SSL-certification was announced. Forum member Natalya Kasperskaya explains: "Roskomnadzor and FSB are lobbying the delegation of SSL certificates to governmental organizations….Now we have a piece of the Internet that is completely out of control by our own country, and it is not good. Because the data is being gathered globally, by someone who is beyond the borders of our state, and it is totally wrong".[17] According to our interviewees, this project is actually a response to the inefficient Yarovaya law and the growing popularity of encryption among RuNet users. Alexey P. emphasizes: "They understood that storing gigabytes of data will give no results, especially because it is encrypted….So the project to build a Man-in-the-middle attack on the governmental level is scary".

2.3. Error 451: Filtering Websites, Restricting Access to the Content

```
HTTP/1.1 451 Unavailable For Legal Reasons

      <h1>Unavailable For Legal Reasons</h1>
  <p>This request may not be serviced in the
Roman Province of Judea due to the Lex Julia
       Majestatis, which disallows access to
     resources hosted on servers deemed to be
operated by the People's Front of Judea.</p>
                                     </body>
                                     </html>
```
[18]

A third set of measures, based on filtering, seeks to control user access to the content of websites judged as extremist or criminal. Since 2007, regional prosecutors have implemented court decisions requiring ISPs to block access to banned sites accused of extremism, but this has not been done systematically. In order to centralize these different materials, a "Single register of Internet resources containing information whose distribution is forbidden in Russia" was created in 2012: any websites that enter this blacklist have to be blocked and three governmental agencies participate in the constitution of this blacklist. Since the adoption of the "Lugovoy law" on 1 February 2014, the list includes websites that "appeal to extremism", e.g. mass disorders, religious or interethnic discord, participation in terrorist attacks or some types of public mass events.

On 13 March 2014, Roskomnadzor blocked access to four webpages: Grani.ru (a liberal online media platform), Kasparov.ru (the website of Garry Kasparov, chess-player and a leader of the liberal opposition), Ezhednevniy Zhurnal (liberal media platform) and the blog of Alexey Navalny (anti-Putin movement leader in 2011–2012 and reputable blogger). Roskomnadzor stated that "these websites contain appeals to illegal activities and participation in mass demonstrations that violate the law".[19]

The list of forbidden webpages is accessible online.[20] As of 30 September 2016, 41,064 pages—mostly concerning prostitution, gambling, black markets, gaming and torrents—are blocked. However, NGO websites are also present, such as the site of Mirotvorets,[21] a pro-Ukrainian organization that informs about the conflict in Ukraine, in particular on the location of Russian troops.

The blocking happens in three ways: by DNS, by IP address or by URL, using Deep Packet Inspection. Administratively, hosting providers are responsible for keeping the blacklist up-to-date and communicating with the owners of forbidden sites and end-users. Maxim I. notes that "The blocking is very easy. We receive and update regularly the black list, twice in a day, and we block those of our clients who are not lucky….We inform our client that his site has been added to the blacklist. Then we listen to everything that the client wants to say about Roskomnadzor but we can't help them or ignore the demand of Roskomnadzor because in this case they can block the IP address of the server, or even an address pool. I am not even speaking about administrative consequences for the company".

While providers have very little possibility to resist the blocking of the blacklisted resources, they choose other forms of action to express their critique of Internet censorship. Vladimir K., director of the ISP CLN, says: "When users try to access to a blocked page, we show them the error message that starts with a phrase: "The struggle against evil is almost never a struggle for good". Thus, the error message itself becomes a space of expression where providers can symbolically communicate with their users by showing their attitude towards the Lugovoy law.

However, Russian filtering and blocking systems are applied unevenly from one region to another, from one

[17] Available at https://rublacklist.net/21509

[18] Available at https://tools.ietf.org/html/rfc7725

[19] Available at http://www.newsru.com/russia/13mar2014/block.html

[20] Available at https://reestr.rublacklist.net

[21] Available at www.myrotvorets.center

provider to another. For example, several employees of ISPs of big companies/monopolists, such as Russian Railways, confirm that they have not been blocked, as Dmitry M. in 2014: "We have this provider in our company, and all the blacklisted websites can be opened. However this seems quite logical, because Roskomnadzor can't give any orders to Russian Railways, who own this provider" (Nossik, 2014). Also, filtering works only partially, depending on the region, the provider and its position on the market, its connections with western providers (e.g. providers who had a peering agreement with Stockholm could access blacklisted websites).

The paradox of filtering consists in the double digital divide that it creates. The more "politicized" users, familiar with the forbidden online resources, will keep on accessing them, using specific tools to bypass censorship. However, the majority of the population will be unable to access this content, lacking the necessary knowledge, resources and technologies to do so. Search engines are also impacted by filtering, so reinforcing the divide: before the blockage, users could accidentally discover some websites (e.g. Navalny's blog) through search engines, but after the blockage these sites "disappeared" (were dereferenced) from the search results. This consequently reduces considerably any potential audience and reinforces the echo-chamber effect by regrouping users who already agree, as mentioned by user popados: "These blockages are not for those who read and will bypass no matter how. It is for random visitors that come from the search or other casual channels that actually constitute the majority. They will just go to another website. In this sense, the blockage is rather efficient" (Nossik, 2014). The same phenomenon touches blacklisted torrent websites, such as Rutracker, that demonstrate a significant decrease in traffic: "the majority of users are just lazy, they are finding new open sources of content. So the goal of the filtering is not to close for everyone, but for an important part", says Maxim I.

Still, access restrictions are not especially difficult to bypass. The IETF notes that "in many cases clients can still access the denied resource by using technical countermeasures such as a VPN or the Tor network" (RFC 7725). Indeed, users deploy manifold technical practices, bricolages and *arts de faire*.

3. Elusive Users: Countermeasures for Bypass and Anonymity

> "Long ago, when GSM connection was not very high quality, there was a trick: you just need to say 'bomb, president, terrorism' and the connection would become much better" Fedor, ISP

Users recently gathered in associations to denounce RuNet censorship and surveillance and promote countermeasures: these include but are not limited to the Russian Pirate Party, *Roskomsvoboda* (Association for the Freedom of Communications), a website for monitoring and analytics of the blockages (Rublacklist), and the project Openrunet promoting countermeasures. While some of these are focused on political campaigning against access restrictions, others concentrate on promoting countermeasures and do not focus on the government but on RuNet users.

Different resistance tactics circulate on forums, blogging platforms and social networks, in the form of comments, posts or specific tutorials. Dedicated "offline" workshops, called "cryptoparties", are organized to present privacy-enhancing tools, and draw from an international cryptoparty movement launched in 2012. Pre-Snowden, in 2012, we participated in such workshops in Saint-Petersburg. They were aimed at left activists (anarchists and antifascists). After 2013, seminars were aimed at a wider audience including NGO workers, journalists, rights defenders and RuNet users seeking to adapt their habits to new realities. The event name was also adapted, the marked word "cryptoparty" being replaced by "seminars on information security".

A wide range of bypass and anonymization tactics and tools exist, circulating both on the Web and during thematic seminars. The organizers themselves attempt to classify existing tools and practices, to build tutorials and construct a coherent presentation, for which several strategies have been observed. Classification occurred, for example, based on the question "Who is your enemy?" Thus Igor, moderator of a cryptoparty for an audience of NGO workers in April 2016, Saint-Petersburg, constructed his presentation around two "big enemies": the state and corporations. He presented the tools that can help bypass state censorship and some devices that would help resist targeted advertising and data tracking. A different format was observed in the *Roskomsvoboda* tutorials, which organize materials according to the tasks users want to perform: "access to a blocked website", "communicate in privacy", "protect your metadata while surfing the web".

On our end, we distinguish such practices here according to the laws they intend to challenge, whether it is SORM or filtering practices and access to blacklisted content. Some of the tools are used in both cases.

As SORM is aimed at intercepting communications, bypassing techniques consist in encrypting them. Encryption tools are used at both the application and network layers. At the application layer, cryptography has been promoted since the first campaigns against SORM launched in 1998 by Moscovskiy Libertarium.[22] Back then, activists were promoting PGP or GnuPG over a mail client, all the while understanding the limits of cryptography: "These countermeasures can't *exclude* the possibility to intercept your communications, but our goal is to make this access extremely hard and *expensive*" (Otstavnov, 1998, our emphasis). Moskovskiy Libertarium was promoting massive usage of these tools

[22] Available at http://www.libertarium.ru/sorm_crypto_esc

as collective action to make surveillance hard and economically disadvantageous for the state: "If the Internet community used these technical means at least in half of the cases, it would become almost immunized against all these dirty tricks such as SORM. However, even occasional usage of strong crypto (especially for fun) will make our opponents' work very hard" (Otstavnov, 1998).

Nowadays, usage of PGP has increased, while remaining far from the ambitious goal of 50% or 100% of users; however, mobile apps for encrypted messaging are gaining popularity. The market for encrypted messaging and mailing clients being in expansion (Ermoshina, Musiani, & Halpin, 2016), cryptoparty organizers and specialized NGOs (e.g. Roskomsvoboda) elaborate several sets of criteria to rate and compare the apps. For example, Igor, the moderator mentioned above, presented a set of criteria including open source, end-to-end, group chat and calls, synchronization between devices, self-destroying messages, notifications about logins from different devices, logging history and multi-layered authentication.

For the time being, alongside WhatsApp,[23] Telegram remains the most popular secure messaging app among Russian users. The usage of Telegram varies according to users' goals and threat models. Several functionalities of the app make it convenient for different user groups: chats, secret chats, group chats, bots and channel broadcasting. Users faced with a low level of threat, not associated with any political activities, tend to adopt Telegram as an alternative to WhatsApp and SMS for everyday conversations with their peer groups. Many activists and privacy-concerned users are aware of the absence of "privacy by default" in Telegram chats (client-to-server encryption) and opt for a "secret chat" option that offers end-to-end encryption. This user group also adopts two-step authentication and self-destruct timer options. Functions such as "Group chat" are used for group conversations between up to 200 users and are popular among activists, journalists or researchers for organizational purposes, as an alternative to Google Groups or mailing lists. For example, one of our use-cases, a group of researchers working in Eastern Ukraine, use Telegram on a daily basis to coordinate research activities, discuss fieldwork, materials and other organizational information. However, they do not rely on Telegram for very sensitive discussions and prefer face-to-face offline meetings.

The popularity of Telegram in Russia can be partly explained by the reputation of its founders, Nicolai and Pavel Durov, Russian-born developers and entrepreneurs. Pavel Durov, the founder of Vkontakte, the most famous Russian social network, is colloquially referred to as the "Russian Zuckerberg" and became *persona non grata* in Russia after his refusal to collaborate with the FSB.[24] Telegram's quick rise on the market of messaging apps is of particular interest as it tells us a lot about the socio-economic factors that influence the success of an innovation in the field: it was when Facebook bought WhatsApp (followed by a several hours blackout for the latter), that the Telegram download rate exploded. As opposed to WhatsApp, Telegram can publicly underline its non-for-profit character and lack of ties with any commercial or governmental services.

While the Russian version of Telegram was released in 2012, before the Snowden revelations, Durov claims that the international version of his tool was inspired by the whistleblower: "In 2012 my brother and I built an encrypted messaging app for our personal use—we wanted to be able to securely pass on information to each other, in an environment where WhatsApp and other tools were easily monitored by the authorities. After Edward Snowden's revelations in 2013 we understood the problem was not unique to our situation and existed in other countries. So we released the encrypted messaging app for the general public".[25]

As Telegram servers are located in five different countries around the world, outside Russia, its broadcasting function is used by censored media as a way to bypass the blockage, and by bloggers as an alternative to Facebook and traditional blogging platforms (for example, Alexey Navalny's popular bot on Telegram and the Grani.ru channel and bot, amongst others). However, unlike private communications on Telegram, public channels may be read and blocked by ISPs and by the Telegram technical team. As of January 2016, 660 channels attributed to ISIS were blocked.

While the "broadcasting channel" function made Telegram an alternative to other news sources and social networks, political activists prefer either the "secret chat" function, or Signal. The Signal application, which Snowden recommended, is used for a specific and limited set of functions—SMS and phonecalls. However, at recent cryptoparties Signal has been criticized for the absence of functions such as automatic synchronization among different devices, time-settings and search.

The technologies used to bypass the Lugovoy law and access censored websites mostly employ the practice of IP address-switching. Therefore one of the most popular and easy-to-use tools is an online proxy server,such as hideme.ru or cameleo.ru. However, this system was criticized by our IT-security activist interviewees for its lack of traffic encryption: a proxy is only useful for by-

[23] We do not examine WhatsApp here, as it was not initially designed as a secure messaging app with end-to-end encryption. Our research and interviews with developers of secure messaging apps (especially with Peter Sunde from Heml.is, who had been contacted by WhatsApp before they decided to purchase the Signal protocol) also show that WhatsApp's motivation to adopt encryption was a market-driven choice, not an ideological decision. Even though the consequences of WhatsApp's decision are very important for the overall "passive" adoption of encryption in Russia, what interests us in this paper is the deliberate and intentional choice of a secure tool. We also do not have data measuring the explicit adoption of WhatsApp consequent of its turn to end-to-end encryption.

[24] Available at http://www.reuters.com/article/idUS74722569420130830

[25] http://www.dazeddigital.com/artsandculture/article/24279/1/pavel-durov

passing the blockage to access content from a blacklisted website, but it does not hide the content that a user is reading. Users are also creatively adapting existing tools to achieve the bypassing goal. For instance, Russians actively use Net archives (archives.org, archive.is or cached versions of websites stored by Google), or activate the "turbo" mode in Opera or Yandex browsers, enabling a very high speed of data transfer. However, once again these tools merely give access to the blocked page, but do not guarantee any anonymity. Moreover, in November 2016, Roskomnadzor started negotiations with Opera representatives about the possibility of blocking access to forbidden content even in "turbo" mode. As of January 2017 no agreement has yet been reached, due to Opera having recently been sold to Golden Brick Capital, a Chinese investment consortium.

As users can be tracked and eventually persecuted for their search of forbidden materials, a set of anonymizing network-layer tools is promoted through cryptoparties and online tutorials, starting with Tor. However, this popular tool is increasingly criticized. Snowden's revelations proved the importance of metadata protection and exposed the vulnerability of Tor. While seminars on informational security observed before 2013 in Saint-Petersburg were promoting widespread use of Tor with almost no attendant criticisms, more recent observations (2015 and 2016) show a growing skepticism and loss of trust. Igor explained the vulnerability of Tor at a workshop organized by Teplitsa Sotsialnih Technologiy: "First of all, your internet service provider will see that you use Tor. That gives him, and the people behind him, a reason to be attentive to you: who is this person who is constantly using Tor? Snowden said that the NSA is tracking everybody who uses Tor, automatically. There are only 7,000 exit nodes in the Tor network, it is not that complicated to track them all".

Another type of network layer tools is a Virtual Private Network (VPN), which adds a supplementary layer of traffic protection. Some of our interviewees pointed out that VPN usage "has become a norm" for them after the GitHub blocking incident in Russia. Among the trusted VPN plugins, activists prefer "zenmate"[26] and "tunnelbear",[27] as they do not need to access user data, while other apps demand the right to access the memory card, photos and contacts. Another popular VPN is offered by Riseup.net,[28] which has a good reputation among politically engaged users ("done by activists for activists"). However, along the lines of Ethan Zuckerman's "cute cat theory of digital activism" (2008), users point out that activist-oriented tools are more vulnerable to targeted attacks than are general public-oriented tools.

Snowden's revelations had a pedagogical effect on Russian activist communities: during observed cryptoparties they were repeatedly heard to emphasize the global character of the surveillance phenomenon. Information security advocates insisted on the necessity for users to change their whole "lifestyle", including interaction with different devices and publishing on social networks. Igor remarks: "You can encrypt your traffic as you wish, you can hide, but if you go to Vkontakte and publish your photo, or talk about revolution, you must understand that it is extremely easy to de-anonymize you and track your network of friends. So start by using your brains, before using Tor and VPN". Thus, after Snowden revealed the interests of big corporations in collecting user-generated data, cryptoparties began to focus not only on activist use cases but on everyday life habits, "unboxing" mobile devices and laptops to demonstrate customization of privacy settings.

On their end, activists are learning how to program message self-destruction or deactivate the tracking of search history and location. Encryption of mobile devices and usage of pass-paragraphs and double or triple authentication methods (combining fingerprints, password and a figure) are becoming popular alongside the use of anonymous search engines such as StartPage or DuckDuckGo, adblocking plugins and cookie controls. Activists advocate multilayered protection and encryption by combining virtual machines, VPN, TOR and encrypted mail and messaging clients.

Finally, Snowden's revelations on NSA surveillance enabled a comparison of the Russian SORM and US intelligence strategies, showing common points and important differences between the two surveillance systems. Activists describe the Russian system as less efficient than its US counterpart, pointing to the geopolitical reasons behind this gap. Not only is Russian surveillance less effective, but the diplomatic context and IT-market configuration also make it harder for Russian surveillance services to be as omnipresent as US ones. Yuriy, an activist, developer and participant in the April 2016 workshop, notes: "As we now know from Edward Snowden's leaks, Americans have their own kind of SORM deployed by the NSA. But it is much more expanded than SORM, it has lots of subdivisions, some of them really crack servers, some others do cryptoanalytics. Snowden claims American services have managed to somehow survey even the Tor traffic, by taking control over the exit nodes. But well…I am really not sure whether it is possible for Russian services to control exit nodes, because sometimes they are located, I don't know, in Panama. And the NSA has much more power to control exit nodes in different countries than Russia. No one likes Russia, and Russia likes no one. It is much more complicated for the FSB to negotiate the access". Therefore it is the controversial position of Russia within the international political arena that makes it harder to negotiate with Western companies to control the traffic of Russian citizens who use anonymizers and Tor.

[26] Available at https://zenmate.com

[27] Available at https://www.tunnelbear.com

[28] Available at https://riseup.net/en/vpn

4. Migrating Servers (and People): A Geopolitical Countermeasure

Due to this geopolitical aspect of RuNet governance, another effective protection tactic is the physical migration of servers and people. Indeed, the legal and technical constraints of RuNet result not only in individual strategies for bypassing and collective action and campaigning, but also in a significant exodus of Web professionals, especially journalists of online media.

The emigration of Russian journalists is not new. In the USSR a significant number of journalists left the country as a result of political persecution (De Tinguy, 2004). However, in the 2010s these exiles are paradoxical, because even if they leave the country they remain connected to Russian cyberspace and actively contribute to its development (Bronnikova, 2016).

Media websites Grani.ru and Meduza were shut down by Roskomnadzor in 2014, making it extremely hard for their editors and owners to survive economically. Despite bypassing tools, their audience decreased. This resulted in the migration of infrastructure and of some journalists out of the Russian Federation. Yuliya Berezovskaya, from Grani.ru, left for France, while Meduza was dislocated to Riga. The cases of Grani.ru and Meduza are interesting for reconsidering the notion of "brain drain". Indeed, the Internet connects migrant and non-migrant populations in their transnational online engagement (Diminescu, 2008; Nedelcu, 2010): online journalists and bloggers expatriated in the European Union, the US or Israel are not excluded from Russian political life but remain important actors in the RuNet freedom quest. For example, Meduza actively informs its readers about recent updates in Russian Internet governance.

Such expatriation also takes shape in a diaspora of infrastructures. In particular, what are called "mirrors" of forbidden websites are created, using platforms such as Amazon.[29] An increasing number of NGOs and other associations opt to transfer their hosting to outside of Russia. As Maxim I., a hosting provider, observes: "Such websites as Children 404[30] or oppositional websites are progressively transferred to foreign servers and start using non-Russian gTLDs (generic top-level domains, such as .ORG). The reason for this is simple: without any court decision your page or the entire website can be blocked, sometimes even by mistake, as it happened with Google or GitHub. I remember also a mass exodus of clients in Belarus, after they have been obliged to work only in Byelorussian data-centers". The tactic of domain zone migration was also adopted by Grani.ru which moved to the .org domain zone on 27 May 2016, two years after its chief editor physically left Russia. Another tactic of "exodus" concerns the kinds of platforms used to disseminate content: more and more of Russia's liberal online media are abandoning the traditional format of websites or blogs in favor of social media pages or Telegram broadcasting channels.

Interestingly, this exodus had begun even before the "Law on Personal Data Storage": Alexey Sidorenko, director of the NGO *Teplitsa Sotsialnih Technologiy*,[31] dates the first wave of infrastructure migration back to 2010. The second wave of digital migration can be attributed to the "Foreign Agent" law: Teplitsa itself had to move from Moscow to Warsaw after the clampdown on foreign aid agencies. IT specialists have seldom been using Russian data-centers because of their technical drawbacks: "People have been actively using western platforms, just because it is more useful and efficient", says Russian-born, Turkey-adopted developer Timofey. However, recent regulation of the Internet has modified the practices of developers and reconfigured the markets. Alexey, CTO of Progress Engine, concludes: "If GitHub is closed, this will enforce brain-drain. And it has already started, several of my colleagues have left to Germany. Folks prefer to work with foreign markets and foreign services. First of all, it's the quality of technological solutions. And also, when you work with a western client, there's a possibility to move. If there's more control from the government, you have a chance to leave".

5. Conclusions

As Edward Snowden is currently on (temporary) asylum in Russia, numerous scholars and journalists insist on the geopolitical significance of this act and emphasize its importance within the global context of a "Cold War 2.0". Yet, far from supporting Snowden's fight for transparency of government data and Internet users' freedom, the Russian government is gradually centralizing its surveillance over the RuNet. However, the direct and indirect influence of the Snowden revelations is making itself visible in a number of other ways, by exposing censorship and surveillance at an unprecedented scale and encouraging creative responses to it. This article has explored how, in response to growing censorship, a variety of tactics are being developed and deployed by Russian users and content producers, ranging from infrastructure-based countermeasures and *détournements* to geopolitical reconfigurations involving the migration of hardware and people.

Although it is not within the scope of this paper to estimate the long-term impact of recent mobilizations (as we do not have enough data to measure this), we can conclude that Russian civic mobilization may be analyzed at two levels. The first is public and collective, for example the "anti-SORM" movement or petitions against Yarovaya law. Such movements appear to have limited impact beyond encouraging visibility and draw-

[29] *Reporters without Borders*, having experimented this technique with Chinese bloggers, helped Russian blacklisted media to put it in practice. Thus, mobilizations for RuNet freedom are integrated in transnational campaigns.

[30] NGO defending the rights of LGBTQI-children.

[31] Teplitsa Sotsialnih Technologiy is an NGO specialized in IT-education of social workers and activists and in development of collaboration between Russian non-profit organizations and IT-specialists. Available at https://te-st.ru

ing public attention to the problem, and even so they remain limited to a small section of the population (with only around 600,000 signatures on Change.org and 2,000 people in attendance at the anti-Yarovaya law meeting), namely IT professionals, journalists, bloggers and Internet freedom activists. However, at the second level, that of so-called "evasion" tactics, mobilisation is far more successful: far from being a contentious means to criticize government or affect changes in legislation and Internet policy, these invisible or elusive techniques have a direct and immediate impact on the everyday practices of users and IT professionals. Evasion techniques are based on an ingenious and constantly changing set of tools and *arts de faire*, and can help to access or broadcast forbidden content as well as to continue IT-related business.

This article shows that Russian Internet governance increasingly takes shape as an "infrastructural battle", a dialectic between the government, who use and co-opt infrastructure, and users, developers and providers who hijack and reconfigure it, in a constant co-shaping of law and technology. This speaks to the "turn to infrastructure" we have recently explored as an increasing tendency in Internet governance (Musiani, Cogburn, DeNardis, & Levinson, 2016). If the Snowden revelations have constituted the 'perfect excuse' for the Russian government to try to enforce a radical approach of "digital sovereignty" (Nocetti, 2015), they have also become on the one hand a catalyst of freedom activists' mobilization, not only for "power users" but for the everyday situated practices of lambda users, and on the other hand an opportunity for Russian businesses working with Western companies to fight both from within and from outside the country. Moreover, the specific geopolitical and economic conditions of embargo can be understood as an important obstacle for Roskomnadzor. It is not civil society but rather Russia's lack of resources, infrastructure, expertise and technologies that make it impossible, at least for now, to apply this law in practice. Despite the current escalation of surveillance, could Russia's controversial position on the international chessboard turn into a paradoxical opportunity for the RuNet?

Acknowledgements

This work is supported by the European Union's Horizon 2020 Framework Programme for Research and Innovation (H2020-ICT-2015, ICT-10-2015) under grant agreement nº 688722—NEXTLEAP.

Conflict of Interests

The authors declare no conflict of interests.

References

Akrich, M. (1998). Les utilisateurs, acteurs de l'innovation, *Education Permanente*, *134*, 78–89.

Borogan, I., & Soldatov, A. (2013). Russian surveillance state. *World Policy*. Retrieved from http://www.worldpolicy.org/journal/fall2013/Russia-surveillance

Bronnikova, O. (2016). Publikovat dlya Rossii iz-za granitsi. Internet—prostranstvo bez granits? [Publishing for Russia from abroad. Is internet a borderless space?]. In F. Daucé, B., Ostromooukhova, O., Bronnikova, & A. Zaytseva (Eds.), *Nezavisimye ot kogo? Alternativnye SMI, malye izdatelstva i bloggery v sovremennoy Rossii [Independent from whom? Alternative mass-media, small editors and bloggers in contemporary Russia]*. Moscow: NLO. Book in preparation.

Ceruzzi, P. (2006). The materiality of the Internet. *IEEE Annals of the History of Computing*, *28*(3), 96–97.

De Tinguy, A. (2004). *La Russie et les Russes depuis l'ouverture du rideau de fer*. Paris: Plon.

DeNardis, L., & Musiani, F. (2016). Governance by infrastructure. In F. Musiani, D. Cogburn, L. DeNardis, & N. Levinson (Eds.), *The turn to infrastructure in Internet governance* (pp. 3–21) New York, NY: Palgrave-Macmillan.

Diminescu, D. (2008). The connected migrant: An epistemological manifesto. *Social Science Information*, *47*(4), 565–579.

Elting, B., Alexanyan, K., Kelly, J., Faris, R., Palfrey, J., & Gasser, U. (2010). *Public discourse in the Russian blogosphere: Mapping RuNet politics and mobilization* (Report no. 2010–11, October 19, 2010). Cambridge, MA: Berkman Center for Internet and Society.

Ermoshina, K., Musiani, F., & Halpin, H. (2016). End-to-end encrypted messaging protocols: An overview. *Proceedings of Internet Science Conference 2016* (pp. 244–254). Florence, Italy: University of Florence.

Erpyleva, S., & Magun, A. (Eds.). (2014). *Politika Apolitchnyh: Grazhdanskie Dvizheniya V Rossii 2011–2013 Godov. [Politics of apolitical: Civic movements in Russia in 2011–2013]*. Moscow: Novoe Literaturnoye Obozrenie.

Filonov, D. (2014, August 12). Otlozhennyi effekt. Kak Snowden zastavil Acronis potratitsya na servery [Postponed effect. How Snowden made Acronis spend money for the servers]. *Forbes.ru*. Retrieved from http://www.forbes.ru/tekhnologii/tekhnika-i-biznes/265017-otlozhennyi-effekt-kak-snouden-zastavil-acronis-potratitsya-na

Freiberg, P. (2014). *Putin's Russia—On a path to cyber sovereignty?* Retrieved from http://www.academia.edu/10762446/Future_of_Internet_Freedom_in_Russia

Gelman, V. (2010, March 9). Lovushka polusvobody: The trap of a half-freedom. *Slon.ru*. Retrieved from http://slon.ru/russia/lovushka_polusvobody-310531.xhtml

Kantyshev, P. (2016, September 4). Rostehu Nuzhno 10,3 Milliarda Rubley na Razrabotky Paketa Yarovoj [Rostech needs 10.3 mlrds of Rubles to develop Yarovaya Law]. *Vedemosti*. Retrieved from http://www.

vedomosti.ru/technology/articles/2016/09/05/655653-rostehu-zakona-yarovoi

Kharkhordin, O. (2011). *Ot obshchestvennogo k publichnomu: kollektivnaia monografiia [From social to public: Collective monograph]*. Berlin: EUSP Press.

Klyueva, A. (2016). Taming online political engagement in Russia: Disempowered publics, empowered state and challenges of the fully functioning society. *International Journal of Communication*, *10*, 4661–4680.

Kozlov, V., & Filipenok, A. (2016, August 9). Miting protiv zakona Yarovoy v Moskve sobral neskolko tysyach chelovek [Meeting against Yarovaya law gathered several thousand people]. *RBC*. Retrieved from http://www.rbc.ru/politics/09/08/2016/57aa0a259a79470ed51332fd

Latour, B. (1988). *The pasteurization of France*. Cambridge, MA: Harvard University Press.

Lonkila, M. (2012). *Russian protest on- and offline. The role of social media in the Moscow opposition demonstrations in December 2011* (FIIA Briefing Paper 98). Helsinki: The Finnish Institute of International Affairs.

Musiani, F., Cogburn, D., DeNardis, L., & Levinson, N. (Eds.). (2016). *The turn to infrastructure in internet governance*. New York, NY: Palgrave-Macmillan.

Nedelcu, M. (2009). Du brain drain à l'e-diaspora: Vers une nouvelle culture du lien à l'ère du numérique? *TIC et Sociétés*, *3*(1). Retrieved from http://ticetsociete.revues.org/675

Nocetti, J. (2015). Russia's "dictatorship-of-the-law" approach to internet policy. *Internet Policy Review*, *4*(4). doi:10.14763/2015.4.380

Nossik, A. (2014, March 19). *Dyryavoe sito censury [Leaky strainer of censorship]*. Retrieved from http://dolboeb.livejournal.com/2652283.html

Otstavnov, M. (1998, June 26). *Chifrovaniye I SORM—Tchastnoye mnenie [Encryption and SORM"—A personal opinion]*. Retrieved from http://www.libertarium.ru/l_sorm_cryptsorm

Prozorov, S. (2012). Vtoroj konec istorii: Politika bezdejatelnosti ot perestrojki do Putina [The second end of History: The politics of inactivity from Perestroika to Putin]. *Neprikosnovennyj zapas*, *2*(82), 169–191.

Schepin, A. (2016, August 1). Irkutskie Operatory Svyazi O Nedostatkah Paketa Yarovoy [ISPs from Irkutsk: On the drawbacks of Yarovaya Package]. *IRK*. Retrieved from https://www.irk.ru/news/articles/20160801/package

Volkov, L. (2016, March 24). *Pedofil Na Slujbe FSB: Kto Sledit Za Nami v Internete? [A pedophile that serves FSB: Who is surveilling us in the internet?"]*. Retrieved from https://www.leonidvolkov.ru/p/119

Zhuravlev, O., Savelyeva, N., & Yerpylova, S. (2014). Individualizm I solidarnost v Novyh Rossijskyh Grazhdanskih Dvizheniyah [Individualism and solidarity in new Russian civic movements]. *Journal of Social Policy Studies*, *12*(2), 185–200.

Zuckerman, E. (2008, March 8). *The cute cat theory talk at ETech*. Retrieved from http://www.ethanzuckerman.com/blog/2008/03/08/the-cute-cat-theory-talk-at-etech

About the Authors

Ksenia Ermoshina (PhD, MINES ParisTech, 2016) is a postdoctoral researcher at the French National Centre for Scientific Research (CNRS), Institute for Communication Sciences (ISCC-CNRS/Paris-Sorbonne/UPMC). Ksenia is working with the European H2020 project NEXTLEAP (2016–2018, Next-Generation Techno-Social and Legal Encryption, Access and Privacy). She is also co-chair of Emerging Scholars Network of the International Association of Media and Communication Research.

Francesca Musiani (PhD, MINES ParisTech, 2012) is Associate Research Professor (*chargée de recherche*), French National Centre for Scientific Research (CNRS), Institute for Communication Sciences (ISCC-CNRS/Paris-Sorbonne/UPMC), associated researcher with the Centre for the Sociology of Innovation of MINES ParisTech-PSL, and academic editor for the *Internet Policy Review*. She is currently one of the Principal Investigators for the European H2020 project NEXTLEAP (2016–2018, Next-Generation Techno-Social and Legal Encryption, Access and Privacy).

COGITATIO

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 54–62
DOI: 10.17645/mac.v5i1.805

Article

Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016

Matthias Schulze

International Relations Department, Friedrich-Schiller University Jena, 07743 Jena, Germany;
E-Mail: matthias.schulze@mailbox.org

Submitted: 31 October 2016 | Accepted: 18 January 2017 | Published: 22 March 2017

Abstract

This article analyzes two cryptography discourses dealing with the question of whether governments should be able to monitor secure and encrypted communication, for example via security vulnerabilities in cryptographic systems. The Clipper chip debate of 1993 and the FBI vs. Apple case of 2016 are analyzed to infer whether these discourses show similarities in their arguments and to draw lessons from them. The study is based on the securitization framework and analyzes the social construction of security threats in political discourses. The findings are that the arguments made by the proponents of exceptional access show major continuities between the two cases. In contrast, the arguments of the critics are more diverse. The critical arguments for stronger encryption remain highly relevant, especially in the context of the Snowden revelations. The article concludes that we need to adopt a more general cyber security perspective, considering the threat of cyber crime and state hacking, when debating whether the government should be able to weaken encryption.

Keywords

Apple; cryptowar; discourse analysis; encryption; FBI

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).

1. Introduction

One effect of the leaks by former National Security Agency (NSA) contractor Edward Snowden in 2013 was that both Apple and Google introduced encryption to their smartphones. Law enforcement and intelligence agencies protested that widespread, unbreakable encryption would make it harder to retrieve evidence from these phones in criminal investigations (Kehl, Wilson, & Bankston, 2015, p. 1). In early 2016, the Federal Bureau of Investigation (FBI) issued a court order to compel Apple to unlock an encrypted iPhone 5C that was used by the San Bernardino attacker in December 2015. The FBI wanted Apple to rewrite its iOS software, to disable encryption security features that would allow the enforcement agency to guess the correct passcodes in a trial and error fashion. Apple resisted and ignited a wider debate within the context of the presidential elections. For some observers, the Apple/FBI debate resembled another instance of the so-called crypto-wars, defined as technological debates about whether the government should have access to encrypted communication. The crypto-wars between national security actors, technology firms and Internet users emerged during the early days of the World Wide Web in late 1992 with the debate about the Clipper chip (Kehl et al., 2015). The aim of this contribution is to analyze whether these two crypto-war discourses are in fact similar. Are there any lessons that can be drawn for the current debate?

This paper builds broadly on the Copenhagen School (Buzan, Waever, & Wilde, 1997) in International Relations and the concept of securitization of technology (Barnard-Wills & Ashenden, 2012; Deibert & Rohozinski, 2010; Hansen & Nissenbaum, 2009), which provides a link to Science and Technology Studies. Securitization is understood as the social construction of security/insecurity, for example in the digital realm (cyber security). Actors compete in the discourse over the meaning of security, i.e. what counts as a threat and how these threats should be dealt with (Dunn Cavelty, 2013). Threat constructions are used for the legitimization of extraordinary security measures that would not be approved by a democratic audience in the absence of a threat. These measures include electronic surveillance, Internet censorship (Deibert, 2015), offensive computer-network-attack capabilities (Lawson, 2012) and exceptional access or state-regulation of encrypted communication, called crypto-politics (Moore & Rid, 2016).

Interestingly, the securitization framework has been rarely adopted to study cryptography discourses. Studies on the crypto-wars debate tend to be either technical (see Abelson et al., 2015; Dam & Lin, 1996) or historical (Kehl et al., 2015). Empirical securitization studies, which focus on digital technologies, tend to ignore the potential material impact of discourses, as Dunn Cavelty argues (Dunn Cavelty, 2015). The securitization of cryptography could have severe implications for cyber security but also for human rights in the digital age. Governmental access to otherwise secure cryptography could, in the worst case, substantially weaken these systems and thus threaten the safety of digital technologies like smartphones, which billions of people use.

The next section offers a short introduction to cryptography debates and outlines the two cases. These are then compared in a qualitative fashion, focusing on what the dominant arguments and actors are. I will concentrate on similarities first and then discuss the differences between the discourses. The final section offers a critical discussion of the arguments.

2. A Short History of the Crypto-Wars

Encryption is a century-old technique to scramble readable text, via mathematical algorithms, into unreadable cypher-text. Sender and recipient require a correct key or password to make the encrypted text intelligible again. The purpose of encryption is to avoid eavesdropping from third parties. Since 1976, a method called public-key encryption (Diffie & Hellman, 1976) promised easy-to-use, widespread encryption of electronic communication. The NSA recognized the potential danger to its global signals intelligence (interception of communication data) effort, if encrypted communication became a mainstream technology. Director of the NSA, Bobby Inman, warned that "unrestrained public discussion of cryptologic matters will seriously damage the ability of this government to conduct signals intelligence" (Inman, 1979, p. 130). Coinciding with the beginning of the personal computer revolution, the NSA argued that an important data source would be "going dark" if every new PC user were to use encrypted, digital communications. Thus, the entire sphere of digital communication could be metaphorically shrouded in darkness, unreadable to the NSA. The dilemma of how to resolve this issue was born.

In 1992, American Telephone and Telegraph (AT&T) began with the development of a consumer-market telephone that could encrypt voice communication between two parties. The NSA recognized that with the looming digital age, traditional, interceptable audio communication could be replaced by encrypted digital communication (Kaplan, 2016, p. 21). This led NSA Director Michael McConnell to rush into the development of the Clipper technology, which would set a standard for the emerging market. The proposal theoretically allowed user-friendly encryption based on a hardware chip called Clipper, which would be attached to devices like phones or computers. In contrast to other products on the market, it had a built-in security weakness: a copy of the encryption key would be stored in government databases. This key-escrow method gave law enforcement "exceptional access" to an otherwise secure technology. The NSA and FBI could thus eavesdrop on any Clipper-based phone call with a warrant because they could access a copy of the key. In February 1993, the newly elected Clinton–Gore Administration adopted the idea (Levy, 1994). On April 16th, 1993, the White House announced the launch of the voluntary Clipper initiative (White House, 1993). A strong public reaction across the political spectrum followed. Most computer experts, technology companies and a social movement of digital natives opposed it (Rid, 2016, pp. 333–337). A series of hearings were held to evaluate the technology. In early 1994, the Clipper program officially started, yet it never saw any widespread adoption. According to the National Research Council, only 10,000 to 15,000 Clipper-enabled phones have ever been sold, mostly to the government (Dam & Lin, 1996, p. 174). A CNN survey in 1994 found that roughly 80% of Americans opposed the initiative (US Senate, 1994). The death blow came when a cryptography expert discovered a security flaw within Clipper's algorithm, although the NSA and its supporters claimed the system was superior and more secure than anything else on the market (Brickel, Denning, Kent, Maher, & Tuchman, 1993). During the mid-1990s, the proposal was silently dropped. According to General Michael Hayden, the NSA "lost" this crypto-war: "We didn't get the Clipper Chip, we didn't get the back door" (Hayden, 2016a).

An outcome of the Clipper debate was that the US government relaxed its strict opposition to the widespread use of encryption. Laws like the Communications Assistance for Law Enforcement Act (CALEA) were adopted to prohibit the government from forcing companies to build government backdoors in their technology (Crawford, 2016). Over time, the US government relaxed its very strict export-regime that treated cryptographic products as dual-use goods. By the end of the 1990s, a widespread consensus (Kehl et al., 2015, p. 19) had been reached that "the advantages of more widespread use of cryptography outweigh the disadvantages" (Dam & Lin, 1996, p. 6). Scientists made the convincing case that key-escrow systems "enabling exceptional access to keys would be inherently less secure, more expensive, and much more complex than those without" (Abelson et al., 2015, p. 7).

The debate about governmental “exceptional access” reemerged in the summer of 2014, after Apple had decided to turn device encryption of its iPhones on by default. On October 10th, FBI Director James B. Comey warned that encryption was hindering evidence retrieval for law enforcement. Comey urged the government to adopt a legislative fix and companies to find a solution (Comey, 2014). In fall 2015, the Washington Post published internal communication from within the intelligence community complaining about a hostile legislative environment on the encryption matter “that could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement” (Nakashima & Peterson, 2015). This was a reference to President Obama who had indicated that his government would not pursue legislation on the matter. The debate resurfaced on February 16th, 2016, when an US Magistrate ruled—ex parte—that Apple must provide “reasonable technical assistance” to FBI investigators to unlock an iPhone 5C that belonged to the San Bernardino shooter of December 2015 (Volz & Menn, 2016). The judge issued the warrant based on the All Writs Act (AWA) from 1789, which becomes active only if there is no other governing law, thus bypassing CALEA (Tangri, Lemley, Feldman, & Landers, 2016). Apple indeed helped the FBI with this iPhone, but mistakes were made and normal unlocking procedures did not work. Apple CEO Tim Cook, the main protagonist of the counter-discourse, contested that the court order was “unreasonably burdensome” (Cook, 2016a). Because of the ongoing election campaign, multiple high profile politicians, intelligence professionals, media and tech companies began to publicly take side with or against Apple. According to a Pew survey, the public sided with the FBI initially, with around 51% arguing that Apple should help the FBI. However, later polls with diverse methodologies showed that the public sided with Apple (Elmer-Dewitt, 2016). The fierce discourse about encryption lasted until March, when a Brooklyn court ruled in Apple’s favor that AWA did not govern the unlocking of an iPhone in a similar case (Lichtblau & Goldstein, 2016). The whole debate suddenly disappeared in March, when it became public that a third party could unlock the iPhone without Apple’s help (Benner & Apuzzo, 2016). Two weeks later it was revealed that the phone did not include any valuable information (McGoogan, 2016) and the Department of Justice issued a filing that it would no longer need Apple’s assistance (Novet, 2016).

3. Methodology

The paper analyses the Clipper discourse between 1993–1994 and the Apple/FBI case between 2014 and 2016, with a focus on the peak of the debate in February/March 2016. Using the snowball technique, a literature corpus (Apple/FBI N = 42, Clipper N = 22) was assembled that contains official statements, newspaper or internet coverage, congressional hearings and some scientific literature of the respective debates. Documents repeatedly mentioned in the corpus were analyzed more deeply using content analysis techniques (Mayring, 2000). The first step was to identify the different discursive positions (opponents, proponents and middle ground). Then the arguments of the respective positions were inductively identified and coded throughout the corpus in an iterative fashion (Keller, 2007). Some codes were deduced from the securitization framework, namely *threats*, *threatened referent* objects and *extraordinary measures* that are demanded to remedy the threat and that go beyond established social norms and procedures (Buzan et al., 1997, pp. 23–24). Another aim was to find out which characteristics, whether negative or positive, were being attributed to encryption. Finally, the frequencies of individual codes were counted and collected in a table to provide some (limited) quantitative insights and to assess what the most dominant arguments were in each debate. Of course, these findings are not generalizable and serve more as an ideal type (Weber, 1973) to gauge the general content of other potential cryptography discourses in the future.

During the Clipper discourse in 1993, only 27% of Americans owned a computer and 2% used the Internet (World Bank, 2016). The Apple/FBI discourse on the other hand happened at a time when 87% of Americans used the Internet (World Bank, 2016), 73% had a computer and 68% a smartphone (Anderson, 2015). In contrast to 1993, cyber security issues like hacking, data theft and state-sponsored cyber attacks were ubiquitous in 2016, with encryption being one line of defense against these issues. This means that in 2016, potentially more customers were affected by the encryption debate. Additionally, the Apple/FBI case stands in the context of the Snowden leaks of 2013 which uncovered the extensive Internet surveillance capacities of the NSA and its targeted operations against encryption systems. NSA programs like Bullrun allegedly implanted software backdoors in HTTPS encryption used for secure web-browsing and also utilized hardware backdoors for exceptional access to Internet routers (Ball, Borger, & Greenwald, 2013). Other Snowden leaks indicate intense NSA efforts to gain access to encrypted Virtual Private Network connections, often used by large corporations to offer secure access to files from afar (Goodin, 2015), or even the Onion Router or TOR network, that utilizes multiple layers of encryption and thus is highly resistant to eavesdropping (Sayer, 2014). Thus, the Snowden leaks increased public awareness of data security, encryption and concerns about government surveillance programs (Rainie & Maniam, 2016).

4. Comparing Two Crypto-War Discourses

4.1. Similarities between Clipper and Apple vs. FBI

The discursive positions in the two discourses are somewhat similar. Law enforcement (FBI), intelligence actors

(NSA) and politicians (predominantly, but not exclusively conservatives) argue for governmental regulation of encryption and providing exceptional access for legitimate law enforcement inquiries. In both discourses, this group produces a relatively homogenous set of arguments. Technology companies, cryptography experts, scientists and a mix of civil-libertarians and tech enthusiasts argue for widespread, public use of encryption. This group is more heterogeneous and uses a huge variety of arguments. In both instances, there is a middle ground, recognizing the needs of both groups and arguing for a compromise (which is technologically difficult to achieve).

When comparing the two discourses, it becomes immediately obvious that the law enforcement perspective is very similar in both cases. The general argument is that "encryption threatens to significantly curtail, and in many instances, preclude, effective law enforcement" (Sessions, 1993), which resembles the NSA's warning from 1979. This is the main argument (uttered 27x) within the debate and a center-piece of the "going dark" metaphor. It is supported by and often combined with a legalistic justification that with a court order or a warrant, the government should have access to encrypted communication (39x). This is the extraordinary measure demanded. It is extraordinary in the sense, that the government wants access to communication intended for no-one else except the communicating parties and demands from companies to change their technology to meet wiretapping needs, effectively influencing hard and software development (Lessig, 2006, p. 66). In other words, the crypto-war discourse is about establishing/contesting the norm of government control over cryptography vs. the right of every user to communicate privately (Levy, 1994).

How are these extraordinary capabilities and powers legitimized? Proponents argue that "criminals" (27x) and "terrorists" (31x) cannot be caught if they use encryption. Interestingly, the Clipper discourses highlights "drug-traffickers", whereas the Apple/FBI discourse is more about "terrorists" and "child molesters". These are framed by law enforcement as the main threats. Closely connected to the argument is the frame that "law enforcement must keep pace" (9x) with malign actors. It creates the impression that the highly trained and equipped, multi-million dollar law enforcement apparatus is falling behind. The referent objects that need to be protected from these threats are mentioned in statements like the following: "Successful conduct of electronic surveillance is crucial to effective law enforcement, to the preservation of the public safety, and to the maintenance of the national security" (15x) (Sessions, 1993). This clearly indicates a national-security perspective. Widespread encryption itself is presented as a threat or at least as a problem to national security (7x). The key description here is that encryption is presented (10x) as a "dual-edge sword: encryption helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists" (White House, 1993). The dilemma is that in both cases, the government recognizes the positive effects of encryption for privacy and the protection of intellectual property (12x). Therefore, the key metaphor is the demand for the rightful balance between privacy and (national) security (11x). In sum, the negative effects of encryption and threats to national security outweigh the benefits. The argument can be found in its entirety in the press release following the official announcement of the Clipper initiative in 1994: "if encryption technology is made freely available worldwide, it would no doubt be used extensively by terrorists, drug dealers, and other criminals to harm Americans both in the US and abroad. For this reason, the Administration will continue to restrict export of the most sophisticated encryption devices, both to preserve our own foreign intelligence gathering capability and because of the concerns of our allies who fear that strong encryption technology would inhibit their law enforcement capabilities" (White House, 1994).

Whereas the government predominantly uses national security-related arguments, the counter-discourse is more heterogeneous. There are three types of argument. Technical arguments state that government access makes encryption systems less secure and are mostly put forward by the technology and science community. Economic arguments argue against government interference in the market and the costs of the proposal. Finally, there are civil liberty arguments that revolve around privacy and mistrust of the expansion of state power and are uttered by libertarians. There are also several other arguments that overlap or do not necessarily fall into either group. Their common denominator is that the government wants to interfere with the products of private companies (24x) in terms of hardware with Clipper and software with Apple. The metaphor of choice is that the government wants to create a "backdoor" (25x) in an otherwise secure system. Libertarians see this as an expansion of government authority, or with the words of Apple CEO Tim Cook as "government overreach" (20x) and thus as a potential threat (Cook, 2016a). Business actors are more afraid of the potential future effects of the government regulating encryption, which might result in the widespread use of inferior technology (15x).

These diverse groups share a relatively similar perspective on encryption. Cryptography is a privacy-enhancing technology (19x) and seen in an exclusively positive way (13x). This explains why any government interference is seen as problematic. The referent objects in this discourse are privacy and civil liberties in particular (24x) and, more implicitly, American identity and values, which are prominently present in the Apple/FBI discourse. The argument in both cases is that control of encryption technology is a norm of authoritarian regimes and police states and therefore inappropriate in democracies (14x). The technological principles of encryption must be understood to make sense of this frame. The fewer parties have access to a system, the more secure it gets. Ideally, public key encryption only has two parties, the sender and receiver. With key-escrow, a third party (the government) is introduced, which creates security risks. The threat in both cases is that the method for exceptional access could fall into the wrong hands (21x) and thus could potentially be misused. In the case of Clipper, the key-escrow database could be stolen, and with the Apple/FBI case, the source code for bypassing iOS security could be hacked, for example by foreign states.

However, there is also a general critique against the government mandating which encryption products to use. In both discourses, technical experts point to the fact that those with malign interest will find a way around government mandated encryption (17x). The key question that comes up in congressional hearings is: Which bad actor would use a technology that he/she knows the government is using to listen in (12x)? Ultimately, law-abiding citizens would be forced to use an inferior technology, while bad actors could use encryption without US backdoors from the international market. This argument is particularly brought forward by critics in the Apple/FBI case (11x), but also existed in a slightly different form in 1993. The reference to foreign crypto-products or the "off-shoring" of cryptography, as former Director of NSA Michael Hayden calls it, is a compelling argument in both cases (Hayden, 2016b). It creates the overall risk that cryptography evolves outside the US market where the government has even less control. This would create a competitive disadvantage for American tech firms. The economic damage of regulating cryptography to American business is a key argument in the Clipper discourse (21x), but not so much in the Apple/FBI case (1x).

The general argument put forward by critics in both cases is that the government should look at the bigger picture (33x), recognizing the general interest of the people and corporations that need encryption, both for privacy reasons but also for business interests and data security. Cryptography is no longer a state monopoly but a matter for citizens (5x) and therefore the government should not prioritize the particular interests of the NSA and FBI. In other words, the general positive effects outweigh the negative effects for a greater audience. This ultimately reflects the legal and discursive consensus that was reached during the mid-1990s.

4.2. Differences

Clipper and the Apple vs. FBI cases differ in some aspects. The Clipper initiative is a government attempt at standard-setting using a NSA-developed chip. It is also a voluntary technology initiative and not a law per se. This means that the government utilizes a range of arguments to "sell" their product to the skeptical audience by arguing Clipper is far superior to anything else on the market (22x), that Clipper does not weaken, but enhances, privacy (9x) and generally that Clipper strikes the right balance between security and privacy (6x). These arguments are particularly highlighted in White House briefing documents from the FBI/NSA and indicate that the Clinton–Gore Administration must have been aware of a potential backlash (Sessions, 1993). Another indicator for this anticipation is the fact that this initiative is not a law, but described as a "voluntary" tech initiative (7x).

Critics contest these arguments. The tech community argues that the NSA developed Clipper (7x) and its encryption algorithm in secrecy (11x), which goes against industry best practices of public code evaluation and the law because the National Institute for Standards would be legally in charge (9x). Others criticize the enormous cost of several million dollars annually that it would take just to maintain the key-escrow infrastructure and the cost of the Clipper chip itself, which would increase hardware prices (8x). Because of these technical facts, the initiative is described as premature, rushed and not thought through (9x). A CNN poll of the time indicates that a majority of 80% is not convinced of the government's arguments (US Senate, 1994). The fact that almost all technology companies and experts are against the Clipper initiative is an important point (17x). To understand this, one must consider the strong skepticism vis a vis government interference in the market (12x).

This is different in the counter-terrorism and post-Snowden context of 2016. The first theme of the Apple vs. FBI discourse is that encryption and its potential weakening is not about the singular San Bernardino case but a *general matter*. Apple systematically argues that government mandated exceptional access is a "threat to millions of customers worldwide" and not just in the US (30x). For Apple, the debate is not about one particular iPhone, but a general case that affects potentially every phone today and in the future (40x). The FBI wants to interfere with Apple's hard/software design (24x) to mandate the construction of a backdoor (25x). Apple calls it the "software equivalent of cancer" (Cook, 2016b). If the courts allowed this, it would create a dangerous legal precedent (26x), which the FBI repeatedly denies (although Comey testifies that the FBI has around 600 other iPhones to be unlocked) (C-Span, 2016). Apple repeatedly argues that in the encryption debate we need to look at the bigger picture, beyond law enforcement interests (33x). The bigger picture includes the cyber security landscapes and new threats: from cyber attacks (20x), data-theft (14x) and hackers (15x). Backdoors resemble weaker encryption which itself is represented as a threat (19x). Backdoors would introduce vulnerabilities to all iPhones, which would represent an enormous public safety risk (16x) because iPhones are used in areas like government agencies and critical infrastructures. These areas would become vulnerable to hacking. Weak encryption would make the entire digital infrastructure less secure (10x). Apple also fears a potential future spillover: weakening encryption now will harm the US digital infrastructure in the future (9x), because exploits could be stolen, and thus fall into the wrong hands (15x). The powerful technical argument that there is no backdoor that could be exploited just by the good guys is put forward (11x). Moreover, other agencies might dig up cases to mandate companies to build in backdoors for more trivial reasons than fighting terrorism, a phenomenon called function creep (10x).

The second discursive feature is an identity or moral narrative. Apple argues that the referent objects are not just millions of customers or privacy and civil liberties but American identity in general (23). "This is not who we are", says Tim Cook (Cook, 2016b). If Western Democracies follow authoritarian regimes in their control of private communication (via government access), it would create a soft-power precedent (10x). Dictatorships would feel legitimized in their surveillance of citizens. Likewise, the FBI uses moralizing statements like "It is about the victims and justice. Fourteen people were slaughtered and many more had their lives and bodies ruined….We can't look the survivors in the eye, or ourselves in the mirror, if we don't follow this lead" (Comey, 2016b). However, most of the FBI's argument is rather legalistic, focusing on the argument that there should be no "warrant-proof" spaces (Comey, 2016a).

In sum, the FBI and Apple recognize each other's good intentions and need for cooperation to resolve this problem. Both parties argue that there needs to be a broad public discussion about this difficult issue (22x). Policymakers in general favor strong encryption with exceptional, warrant-based access while the tech community replies that the mathematics either support secure encryption without government backdoors or exceptional access with significantly less security. The combination of both secure cryptography and governmental access represents wishful thinking or the search for a magic pony solution (Abelson et al., 2015).

5. Discussion

Whereas the Clipper discourse is focused mostly on the privacy/security dichotomy, the Apple/FBI case shows that in times of cyber crime and hacking, this dichotomy needs to be rethought. Traditionally, the two have been framed as an antagonism or a zero-sum game: more security means less privacy/liberty. This is not necessarily true anymore because encryption enhances both privacy and security, both individually but also collectively or globally. In an interconnected world, a vulnerability in one iPhone is a threat for every user, as the recent Pegasus spyware, which affected all 1 billion active iOS devices, shows. Encryption is crucial for the security of digital infrastructures (i.e. cyber security). The question we need to address is "whose security are we talking about"? The debate shows that there are two paradigms of security at work: a national security perspective with traditional, physical threats such as terrorism and a cyber security perspective, which considers the vulnerabilities of software and hardware in terms of hacking, cyber crime and state-sponsored cyber war. Former NSA Director Michael Hayden belongs to the latter and argues that considering the cyber threat, "America is simply more secure with unbreakable end-to-end encryption" (Hayden, 2016a).

The second element we need to discuss critically is the "going dark" metaphor, which creates a false dualism of light and shadow and thus another artificial zero-sum game. The metaphor ignores the fact that there are multiple sources of light. Wiretapping of conversations is just one stream of data among an increasing number of law enforcement tools like automated biometric recognition, DNA sampling, geo-location tracking or contact-chaining with social network analysis. Our "digital exhaust" as Michael Hayden calls it, the often unencrypted metadata we generate using smartphones and online services such as Facebook or Google, is in fact growing (Hayden, 2016b). Never before has there been so much private information about us in the open. The government has access to most of these new sources of data. The amount of data traversing global networks in 2016 makes the year 1993 appear like the dark ages of data and law enforcement. Arguing that we are currently "in the light" and the future will be dark is somewhat misleading. Just because content data is increasingly more encrypted and one channel of data collection might be "going dark", it does not mean that all other channels are going dark as well. The opposite is probably true.

The "going dark" metaphor creates a false technological-deterministic assumption that widespread cryptography will *automatically* lead to only one single outcome: a future of uninterceptable information. This scenario is unlikely. There is no such thing as unbreakable encryption. It might get more complicated but it is unlikely that it will ever be impossible to break. Even today, strong cryptography is circumvented by exploiting other weaknesses in the system, which probably is the reason why the FBI got into the San Bernardino iPhone without Apple's help (Benner & Apuzzo, 2016). Even if encryption was unbreakable, it would not be guaranteed that it would ever reach 100% user adoption. The technological barriers for users are still high and market mechanisms like ad-based, big-data business models stand in the way of widespread adoption. Practical reasons prohibit the adoption of encryption, which is the same reason why we do not whisper all the time to avoid eavesdropping. It is often too impractical and inconvenient. Even if everyone used encryption, people often make mistakes with the implementation which makes their systems vulnerable to attack (Gasser et al., 2016, p. 3).

Determinism overstates the effects of technology and ignores human response strategies. It is too easy to blame technologies when old strategies fail. To blame technology would be akin to the French blaming the invention of the tank for their inferior defense strategy against the German Blitzkrieg tactics in World War 2. There are always two components: technology and human agency. If encryption is indeed a problem, then law enforcement and intelligence agencies simply must adapt and change their operating strategies (Landau, 2016). For example, if electronic surveillance of a drug dealer is not feasible anymore because he/she uses encrypted phone calls, one way to resolve the problem would be to use human intelligence like surveillance personnel on the ground or even traditional acoustic surveillance bugs implanted in a car or house. Particularly the "Internet of Things (IoT)" with microphones in Smart TVs and loudspeakers and the trend of cloud-computing will offer new, unique capabilities that could be used in the traditional warrant process (Gasser et al., 2016, p. 10). At the same time, in the context of the growing vulnerabilities of a digitalized IoT infrastructure, safe systems and strong encryption are imperative. The old Clipper consensus that the widespread use of cryptography is the greater good is still valid, even though it is understandably harder to see in the current context of global terrorism.

As threatening as terrorism may be, cyber attacks from nation-states, cyber crime and digital espionage are growing rapidly and are costing millions of dollars annually. Richard C. Clarke, the senior counter-terrorism official during the Bush administration argued: "my point is encryption and privacy are larger issues than fighting terrorism" (Clarke, 2016). The ongoing securitization of cryptography in liberal democracies sets a normative precedent. Directly after the Apple/FBI debate, countries like Russia began to demand backdoors in cryptographic messengers like WhatsApp and Telegram by law and referred to the practices of Western democracies for justification (Howell O'Neill, 2016). Currently, France, Great Britain, Germany and others are pursuing similar legislation. Interestingly, the discourses in liberal and authoritarian countries rely on similar rhetorical figures, threat descriptions and referent objects identified in this article. To qualify this, further comparative research would be required. Authoritarian regimes will probably use exceptional access not to prosecute terrorists, but the political opposition or human rights NGOs. Besides this normative argument there is also a technical one: the more governments replicate this practice of actively punching holes in cryptography without disclosing them publicly, the less secure the worldwide IT-infrastructure gets.

Acknowledgements

Thanks to the anonymous reviewers for their positive and constructive feedback.

Conflict of Interests

The author declares no conflict of interests.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benalo, J., Blaze, M., Diffie, W., . . . Weitzner, D. J. (2015). *Keys under doormats: Mandating insecurity by requiring government access to all data and communications* (Computer Science and Artificial Intelligence Laboratory Technical Report, MIT-CSAIL-TR-2015-026). Cambridge, MA: Massachusetts Institute of Technology.

Anderson, M. (2015). Technology device ownership: 2015. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015

Ball, J., Borger, J., & Greenwald, G. (2013). Revealed: How US and UK spy agencies defeat internet privacy and security. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture*, *15*(2), 110–123.

Benner, K., & Apuzzo, M. (2016). US says it may not need Apple's help to unlock iPhone. *The New York Times*. Retrieved from http://nyti.ms/1UzGJTS

Brickel, E. F., Denning, D. E., Kent, S. T., Maher, D. P., & Tuchman, W. (1993). *Skipjack review: Interim report* (The SKIPJACK Algoritm). Retrieved from https://epic.org/crypto/clipper/skipjack_interim_review.html

Buzan, B., Waever, O., & Wilde, J. D. (1997). *Security: A new framework for analysis*. London: Lynne Rienner Publishers Inc.

C-Span. (2016). Apple iPhone encryption hearing. *C-Span*. Retrieved from https://www.c-span.org/video/?405442-1/hearing-encryption-federal-investigations

Clarke, R. (2016). Encryption, privacy are larger issues than fighting terrorism, Clarke says. *NPR.prg*. Retrieved from http://www.npr.org/2016/03/14/470347719/encryption-and-privacy-are-larger-issues-than-fighting-terrorism-clarke-says

Comey, J. (2014). Going dark: Are technology, privacy, and public safety on a collision course? *US Department of Justice*. Retrieved from https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

Comey, J. (2016a). Encryption tightrope: Balancing Americans' security and privacy. *US Department of Justice*. Retrieved from https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy

Comey, J. (2016b). FBI director comments on San Bernadino matter. *US Department of Justice*. Retrieved from https://www.fbi.gov/news/pressrel/press-releases/fbi-director-comments-on-san-bernardino-matter

Cook, T. (2016a). *A message to our customers*. Retrieved from http://www.apple.com/customer-letter

Cook, T. (2016b). Apple CEO Tim Cook sits down with David Muir. *ABC News*. Retrieved from http://abcnews.go.com/WNT/video/exclusive-apple-ceo-tim-cook-sits-david-muir-37174976

Crawford, S. (2016). The law is clear: The FBI cannot make Apple rewrite its OS. *Backchannel*. Retrieved from https://backchannel.com/the-law-is-clear-the-fbi-cannot-make-apple-rewrite-its-os-9ae60c3bbc7b#.sa125j16z

Dam, K. W., & Lin, H. S. (1996). *Cryptography's role in securing the information society*. Washington, DC: National Research Council.

Deibert, R. J. (2015). Cyberspace under siege. *Journal of Democracy*, *26*(3), 64–78.

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, *4*(1), 15–32.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122.

Dunn Cavelty, M. (2015). Die materiellen Ursachen des Cyberkriegs Cybersicherheitspolitik jenseits diskursiver Erklärungen. *Journal of Self-Regulation and Regulation*, *1*, 167–184.

Elmer-Dewitt, P. (2016). Apple vs. FBI: What the polls are saying. *Fortune*. Retrieved from http://fortune.com/2016/02/23/apple-fbi-poll-pew

Gasser, U., Gertner, N., Goldsmith, J., Landau, S., Nye, J., O'Brien, D. R., . . . Zittrain, J. (2016). *Don't panic. Making progress on the "Going Dark" debate*. Cambridge, MA: Berkman Klein Center.

Goodin, D. (2015). How the NSA can break trillions of encrypted Web and VPN connections. Researchers show how mass decryption is well within the NSA's $11 billion budget. *Ars Technica*. Retrieved from http://arstechnica.com/security/2015/10/how-the-nsa-can-break-trillions-of-encrypted-web-and-vpn-connections

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, *53*, 1155–1175.

Hayden, M. V. (2016a). Hayden: The pros and cons of access to encrypted files. *Youtube*. Retrieved from https://www.youtube.com/watch?v=6HNnVcp6NYA

Hayden, M. V. (2016b). General Michael Hayden on the Apple FBI and data encryption. *AEIdeas*. Retrieved from https://www.aei.org/publication/gen-michael-hayden-on-apple-the-fbi-and-data-encryption

Howell O'Neill, P. (2016). Russia lawmakers pass sweeping spying law that requires encryption backdoors, call surveillance. *The Daily Dot*. Retrieved from http://www.dailydot.com/layer8/encryption-backdoor-russia-fsb-bill-passes

Inman, B. R. (1979). The NSA perspective on telecommunications protection in the nongovernmental sector. *Cryptologia*, *3*, 129–135.

Kaplan, F. (2016). *Dark territory: The secret history of cyber war*. New York, NY: Simon & Schuster.

Kehl, D., Wilson, A., & Bankston, K. S. (2015, June). *Doomed to repeat history? Lessons from the crypto wars of the 1990s* (Report from the New America Foundation). Washington, DC: New America.

Keller, R. (2007). *Diskursforschung*. Berlin: Springer.

Landau, S. (2016). The real security issues of the iPhone case. Law enforcement needs 21st-century investigative savvy. *Sciencemag*, *352*(6292), 1398–1399.

Lawson, S. (2012). Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday*, *17*(7). doi:10.5210/fm.v17i7.3848

Lessig, L. (2006). *Code: And other laws of cyberspace, version 2.0*. New York, NY: Basic Books.

Levy, S. (1994). Battle of the Clipper chip. *The New York Times*. Retrieved from http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html

Lichtblau, E., & Goldstein, J. (2016). Justice Dept. appeals ruling in Apple iPhone case in Brooklyn. *The New York Times*. Retrieved from https://www.nytimes.com/2016/03/08/technology/justice-dept-appeals-ruling-in-apple-iphone-case-in-brooklyn.html

Mayring, P. (2000). Qualitative content analysis. *Forum: Qualitative Sozialforschung*, *1*(2). Retrieved from http://www.qualitative-research.net/index.php/fqs/article/view/1089

McGoogan, C. (2016). Terrorist's iPhone didn't turn up any useful information, FBI admits. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/technology/2016/04/15/terrorists-iphone-didnt-turn-up-any-useful-information-fbi-admit

Moore, D., & Rid, T. (2016). Cryptopolitik and the darknet. *Survival*, *58*(1), 7–38.

Nakashima, E., & Peterson, A. (2015). Obama faces growing momentum to support widespread encryption. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/tech-trade-agencies-push-to-disavow-law-requiring-decryption-of-phones/2015/09/16/1fca5f72-5adf-11e5-b38e-06883aacba64_story.html

Novet, J. (2016). Apple vs. FBI: A timeline of the iPhone encryption case. *VB*. Retrieved from http://venturebeat.com/2016/02/19/apple-fbi-timeline

Rainie, L., & Maniam, S. (2016). Americans feel the tensions between privacy and security concerns. *Pew Research Center*. Retrieved from http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns

Rid, T. (2016). *Maschinendämmerung: Eine kurze Geschichte der Kybernetik*. Berlin: Propyläen Verlag.

Sayer, P. (2014). Snowden docs show Tor, TrueCrypt, Tails topped NSA's 'most wanted' list in '12. *Computerworld*. Retrieved from http://www.computerworld.com/article/2863937/snowden-docs-show-tor-truecrypt-tails-topped-nsas-most-wanted-list-in-12.html

US Senate. (1994). *The administration's clipper chip key escrow encryption program: Hearing before the Subcommittee on Technology and the Law of the Committee on the Judiciary United States Senate*, Washington, DC: US Senate.

Sessions, W. S. (1993). *Leaked letter briefing document "Encryption: The threat, applications, and potential solutions"*. Retrieved from https://epic.org/crypto/clipper/foia/crypto_threat_2_19_93.html

Tangri, D., Lemley, M. A., Feldman, M. A., & Landers, A. L. (2016). Amicus Curiae Brief of law professors in support of Apple Inc. *Apple*. Retrieved from http://www.apple.com/pr/library/2016/03/03 Amicus-Briefs-in-Support-of-Apple.html

Volz, D., & Menn, J. (2016). Apple ordered to help FBI unlock data from San Bernadino shooter's iPhone. *Reuters*. Retrieved from http:// www.reuters.com/ article/california-shooting-timcook-idUSKCN0VQ0YG

Weber, M. (1973). Die "Objektivität" sozialwissenschaftlicher und sozialpolitischer Erkenntnis. In J. Winckelmann (Ed.), *Gesammelte Aufsätze zur Wissenschaftslehre* (pp. 146–214). Tübingen: Mohr.

White House. (1993). *Statement by the press Secretary*. Retrieved from https://epic.org/crypto/clipper/ white_house_statement_4_93.html

White House. (1994). *Statement by the press Secretary*. Retrieved from https://epic.org/crypto/clipper/ white_house_statement_2_94.html

WorldBank. (2016). Internet users (per 100 people). *World Bank*. Retrieved from http://data.worldbank. org/indicator/IT.NET.USER.P2

About the Author

Matthias Schulze, MA, is a political scientist working on issues such as surveillance (data retention) and cyber security (encryption) and cyber war in both democratic and authoritarian states. In his PhD thesis, he analyzes normative change in the behavior of democratic states towards the Internet, represented by increased surveillance and cyber war practices and discourses.

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 63–75
DOI: 10.17645/mac.v5i1.813

Article

Corporate Privacy Policy Changes during PRISM and the Rise of Surveillance Capitalism

Priya Kumar

College of Information Studies, University of Maryland, College Park, MD 20742, USA; E-Mail: pkumar12@umd.edu

Submitted: 25 October 2016 | Accepted: 28 November 2016 | Published: 22 March 2017

Abstract

Disclosure of the NSA's PRISM program demonstrated that Internet companies have become prime targets of government surveillance. But what role do companies themselves play in putting users' privacy at risk? By comparing the changes in the privacy policies of ten companies—the nine in PRISM plus Twitter—I seek to understand how users' privacy shifted. Specifically, I study how company practices surrounding the life cycle of user information (e.g. collection, use, sharing, and retention) shifted between the times when companies joined PRISM and when PRISM news broke. A qualitative analysis of the changes in the privacy policies suggests that company disclosure of tracking for advertising purposes increased. I draw on business scholar Shoshana Zuboff's conceptualization of "surveillance capitalism" and legal scholar Joel Reidenberg's "transparent citizen" to explain the implications such changes hold for users' privacy. These findings underscore why public debates about post-Snowden privacy rights cannot ignore the role that companies play in legitimizing surveillance activities under the auspices of creating market value.

Keywords

Internet companies; PRISM; privacy policies; surveillance capitalism; targeted advertising; transparent citizen

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).

1. Introduction: The Relationship between Government and Corporate Surveillance

In August 2016, New Zealander Tony Fullman became "the first person in the world to be publicly identified as a confirmed" target of the NSA's PRISM surveillance program (Gallagher & Hager, 2016). Intelligence officials in New Zealand believed Fullman and others were concocting a plot to violently overthrow Fiji's authoritarian leader. According to documents that Edward Snowden provided to The Intercept, an investigative news outlet, the U.S. National Security Agency (NSA) used PRISM to access Fullman's Gmail and Facebook accounts and turned over more than 190 pages of his communication and private information, such as bank statements, to New Zealand authorities. The information revealed no evidence of a plot, and ultimately, the government never brought charges against Fullman or others it investigated (Gallagher & Hager, 2016).

While governments are certainly justified in investigating credible threats of violence, The Intercept's investigation suggests that even before New Zealand's authorities received Fullman's communications from the NSA, they had scant evidence that the plot to assassinate Fiji's leader was, in fact, credible. Fullman exemplifies the "transparent citizen" (Reidenberg, 2015). By using networked digital technologies now common in everyday life, he becomes increasingly visible to institutional actors like governments and companies, yet those institutions' use of his personal information remains obscure. The rise of a transparent citizenry threatens privacy, undermines trust in rule of law, and challenges international norms and data flows (Reidenberg, 2015). PRISM targets non-U.S. persons located outside of the U.S., but a report from the U.S. Privacy and Civil Liberties Oversight Board ([PCLOB], 2014) found that aspects of the program also present privacy concerns for U.S. persons.

PRISM is a top-secret intelligence program in which the NSA can compel U.S.-based companies to provide information associated with certain "selectors", such as an email address or phone number. Selectors cannot include individual names or other key words (PCLOB, 2014). The Snowden disclosures name nine U.S.-based company partners: Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, Skype, AOL, and Apple (Gellman & Poitras, 2013). The program stems from legal authority Congress granted to the U.S. government under Section 702 of the Foreign Intelligence Surveillance Act Amendments Act of 2008. The PCLOB reviewed PRISM and other surveillance programs operating under the aegis of Section 702 and concluded, "PRISM collection is clearly authorized by the statute" (PCLOB, 2014, p. 9). Nevertheless, privacy and surveillance lawyers argue that Section 702's overbroad scope and insufficient protections, combined with the government's lack of transparency regarding the operations of surveillance programs authorized under Section 702, threaten the privacy and civil liberties of those within and beyond the U.S. (Butler & Granick, 2016). In 2015, the Court of Justice of the European Union invalidated the Safe Harbor agreement that permitted U.S. companies to transfer the personal data of E.U. citizens into the U.S. The court cited concerns with the U.S. surveillance programs described in Snowden's disclosures, including PRISM (Ni Loideain, 2016).

The Snowden disclosures re-ignited a public conversation about the extent to which governments should access data that people generate in the course of their daily lives. The act of governments obtaining data from third parties such as companies is nothing new. However, the rise of cloud computing and pervasive computing coupled with inexpensive data storage has enabled companies to store and retain increasing amounts of data, giving governments more data to pursue (Bellia, 2008). Indeed, "government and nongovernment surveillance support each other in a complex manner that is often impossible to disentangle" (Richards, 2013, p. 1940). Of course, companies do not collect and store user information with the goal of sharing it with the government. Rather, the allure of big data entices companies to collect and retain as much data as they can. Analyzing that data enables companies to predict and modify human behavior while also generating revenue and market control. Such is the logic of surveillance capitalism, "a new social relations and politics that have not yet been well delineated or theorized" (Zuboff, 2015, p. 76).

In the wake of Snowden's disclosures, several companies denied giving the U.S. government "direct access" to their servers, as PRISM was mistakenly first reported to entail (Blodget, 2013). However, companies are legally required to respond to national security demands, such as those the government makes under PRISM, and in some cases, companies facilitated this process (Miller, 2013). Important debate continues about the legality of Section 702, which authorizes PRISM and other surveillance programs (Butler & Granick, 2016). I argue that, in addition to interrogating the legality of surveillance frameworks, conversations regarding post-Snowden Internet policy must also examine the degree to which companies' own business practices can legitimate surveillance of Internet users around the world.

Why study these companies? The nine U.S. companies named in Snowden's PRISM disclosures are by no means the only ones who engage in and benefit from surveillance capitalism. And while disclosure of PRISM certainly spotlighted these companies, several companies had already attracted significant public and regulatory attention due to privacy concerns before the news broke. Nevertheless, the U.S. government's decision to explicitly include them in a secret surveillance program suggests that their data holds particular value and that their business practices related to that data deserve closer examination. These companies collectively serve billions of Internet users around the world, meaning they hold the power to respect or imperil the privacy rights of many (MacKinnon, 2012).

In this vein, I analyze the changes in company privacy policies over two time frames to understand how users' privacy rights shifted since companies entered PRISM. I focus on one aspect of privacy—the flow of user information across the "the informational life cycle", (Schwartz & Solove, 2014, p. 892), which includes the collection, use, sharing, and retention of user information (Kumar, 2016). This translates to the following research question:

> How did company practices surrounding the life cycle of user information (its collection, use, sharing, and retention) change in the time period spanning companies' entrance into PRISM and the program's disclosure to the public?

I don't contend that PRISM caused the companies to change their privacy policies. I suggest that while they were part of PRISM, companies undermined their users' privacy rights by expanding their use of targeted advertising, which is tantamount to tracking their users. This offers evidence of the rise of surveillance capitalism, where companies have business incentives to aggregate more and more user information, and governments gain an attractive trove of data to access for surveillance purposes. The next section of this paper describes the various stakeholders that influence company actions and outlines this paper's conception of users' privacy rights online. Section 3 explains the methods I used to locate and analyze company privacy policies. Section 4 reviews privacy policy changes related to the life cycle of user information, and sections 5 and 6 examine what this analysis contributes to debates about privacy rights in a post-Snowden world.

2. The Role of Companies in Respecting Users' Online Privacy Rights

Encouraging companies to act in ways that respect their users' privacy is a complex endeavor. Companies are accountable to several stakeholders: investors expect maximized returns and minimized risk; regulators expect adherence to law; consumers expect valuable, trustworthy products and services; civil society expects support for the public interest. Evaluating companies according to certain standards and comparing their performance can incentivize competition among companies. It can also provide valuable information to various stakeholders, who can likewise pressure companies to perform better. The Ranking Digital Rights project (RDR) developed criteria to evaluate companies in the information and communications technology (ICT) sector on their respect for free expression and privacy rights[1] (Maréchal, 2015).

RDR's criteria, which stem from nearly four years of consultation and testing, build on several existing human rights frameworks and principles and translate them into concrete, measurable indicators. While imperfect, this approach provides a mechanism to evaluate and compare companies (Maréchal, 2015). RDR's privacy indicators draw from the Fair Information Practice Principles, OECD Privacy Guidelines, European Union regulations, and other frameworks (Ranking Digital Rights, 2016a). The indicators related to company data practices focus on company disclosure related to the collection, sharing, use, and retention of user information as well as users' ability to access and control their own information (Ranking Digital Rights, 2016b). Often, company disclosure about these practices appears in a privacy policy.

Policy documents alone cannot reveal whether companies respect privacy rights, but they do represent company practice. Privacy policies notify the public, and regulators in particular, about a company's privacy practices. As such, they serve as an important source of information to understand how users' privacy rights fare online. Scholars, journalists, and those in civil society have studied privacy policies for this purpose, and some privacy policy research has taken a longitudinal approach (Jeong, 2016; Milne, Culnan, & Greene, 2006; Opsahl, 2010). In this paper, I draw on my experience studying privacy policies for RDR to evaluate how changes in the PRISM company privacy policies suggest shifts in users' privacy rights. I particularly focus on changes related to the life cycle of user information.

3. Locating and Analyzing Company Privacy Policies

This study compares versions of ten privacy policies in effect before and after two points in time:

1. The date the company entered PRISM, according to documents from Snowden (Gellman & Poitras, 2013). These dates range from September 2007 to October 2012.
2. June 6, 2013, the day the Washington Post published its story on PRISM, alerting the public to the program's existence (Gellman & Poitras, 2013).[2]

It includes the nine companies implicated in PRISM as well as Twitter, which attracted media attention for its absence from the list of PRISM companies (Martin, 2013). Since Twitter was not publicly named as a PRISM company, I only analyzed it for the second time frame.

Google and Twitter provide archives of their privacy policies. For the remaining companies, I used the Internet Archive's Wayback Machine to find previous versions of their privacy policies. Murphy, Hashim and O'Connor (2007) suggest the Wayback Machine is a valid source when examining website content and age. To check the Wayback Machine's validity for this study, I compared versions of Google and Twitter's policies from their company archives and the Wayback Machine. The text was identical in both versions, except the Wayback Machine version of one policy lacked a reference to Google's archive. This suggests the Wayback Machine provides adequate representations of previous versions of privacy policies.

Table 1 lists the policies used for each company. All companies except Paltalk included the date the policy was last updated or the date the policy went into effect, which made it easy to determine when the policies changed. The first time frame includes three policies for Paltalk because the first updated policy only contained a change in the company's mailing address. Paltalk's second updated version included one substantive change. Corporate oversight structures also influenced which policies were reviewed. Google has owned YouTube since 2006. During the first time frame, YouTube maintained a separate privacy policy, so changes in its policies are included in this analysis. By the second time frame, Google's privacy policy covered all of its services, including YouTube, so that period does not include an analysis of separate YouTube policies. Conversely, Microsoft bought Skype in 2011, but Skype maintained a separate privacy policy during both time frames and is included in both.

I used a difference-checking tool to identify the changes in each company's "before" and "after" policies. I logged each change in a spreadsheet. The addition or removal of an entire sentence represented one change. If one sentence included several distinct edits, I logged them separately. I looked at the original policies to determine whether the change was substantive, using an inductive approach to develop codes related to the substance of changes (Thomas, 2006). In the first pass, I developed the codes and assigned them to each change. I took a second pass through the entire dataset and checked for consistency. Table 2 contains examples of each code. These codes were mutually exclusive.

Overall, the policies included 814 changes, with Facebook accounting for 651, or 80 percent. Facebook overhauled its policy during the first time frame and made significant changes during the second time frame, far outpacing the number of changes from other companies. In

[1] Until August 2016, I was a research analyst with the RDR project.

[2] The Washington Post first reported the story on June 6, 2013 and updated its story on June 7, 2013 (Blodget, 2013).

Table 1. Privacy policies analyzed across two time frames.

Company	Date of Policy	Timeframe 1: Entered PRISM	Date of Policy	Date of Policy	Timeframe 2: PRISM News	Date of Policy
Microsoft	Jan. 2006	Sept. 11, 2007	Oct. 2007	April 2012	June 6, 2013	Aug. 2013
Yahoo	Nov. 22, 2006	Mar. 12, 2008	Oct. 28, 2008	May 31, 2013		Sept. 25, 2014
Google	Aug. 7, 2008	Jan. 14, 2009	Jan. 27, 2009	July 27, 2012		June 24, 2013
Facebook	Nov. 26, 2008	June 3, 2009	Nov. 19, 2009	Dec. 11, 2012		Nov. 15, 2013
Paltalk	Oct. 7, 2009 (crawled)	Dec. 7, 2009	Feb. 7, 2010; Dec. 4, 2010 (crawled)	May 19, 2013		No change
YouTube	Mar. 11, 2009	Sept. 24, 2010	Dec. 8, 2010	See Google		See Google
Skype	Nov. 2010	Feb. 6, 2011	June 2011	Dec. 2012		Aug. 2013
AOL	Feb. 14, 2011	Mar. 31, 2011	Mar. 30, 2012	May 14, 2013		June 28, 2013
Apple	May 21, 2012	Oct. 2012	No change	No change		Aug. 1, 2013
Twitter	N/A	N/A	N/A	May 17, 2012		July 3, 2013

Table 2. Examples of substantive and non-substantive changes in privacy policies.

Substantive Changes	Explanation or Example
Addition of information	Added sentence: "When we display personalized ads, we take a number of steps designed to protect your privacy."
Removal of information	Removed sentence: "You will only receive special offers via email from Paltalk if you have indicated in your account preferences, or at some other time, that you would like to receive them."
More precise information	Added the bold phrase: "If we learn that we have collected the personal information of a child under 13 **without first receiving verifiable parental consent** we will take steps to delete the information as soon as possible."
Less precise information	Changed the bolded phrase from: "If you are under 13, please do not attempt to register for Facebook or **send any information about yourself to us, including your name, address, telephone number, or email address**" to "If you are under age 13, please do not attempt to register for Facebook or **provide any personal information about yourself to us.**"
Non-Substantive Changes	
Simple fact change	Changed the "Last updated" date in a policy.
Position change	Moved a sentence from one paragraph in the policy to another.
Style change	Changed phrase from: "**NOTICE: Click here for practical tips from the federal government and the technology industry** to help you guard against Internet fraud, secure your computer and protect your personal information" to "**The federal government and technology industry have developed practical tips** to help you guard against Internet fraud, secure your computer and protect your personal information" [Hyperlink present in both sentences].
Fixing typos	Changed phrase from: "To protect your privacy and **security, may** use passwords to help verify your identity before granting access or making corrections to your AOL information" to "To protect your privacy and **security, we may** use passwords to help verify your identity before granting access or making corrections to your AOL information."

total, the policies showed 424 substantive changes, with Facebook accounting for 347, or 82 percent. This analysis focuses on the substantive changes. To answer the question of what these policy changes suggest with regard to the life cycle of user information, I again used an inductive approach to develop codes related to digital rights, as framed by RDR's indicators (Ranking Digital Rights, 2016b; Thomas, 2006). In a first pass, I developed and assigned the codes to each substantive change and in a second pass, I checked for consistency. This yielded 11 codes across four themes. These codes were not mutually exclusive, and 30 changes received two codes (25 of those changes applied to Facebook). Table 3 shows the themes and the codes present in each. It also states how many changes related to each theme appeared in Facebook's policies compared to other companies.

Table 3. Digital rights themes and codes.

Digital Rights Theme	Codes Included in Theme	Number of Changes (Not Mutually Exclusive)
Management of user information	Data collection, Use of data, Retention, Security	146 (Facebook: 133)
Data sharing and tracking	Third party, Data sharing, Tracking	149 (Facebook: 115)
User action	More information, Choice	115 (Facebook: 89)
Corporate governance	Accountability, Remedy	44 (Facebook: 35)

4. Policy Changes Related to the Life Cycle of User Information

Two of the four digital rights themes focused on the life cycle of user information: management of user information and data sharing and tracking. Together, these themes encompassed 70 percent of the substantive changes. The following analysis describes what the changes suggest for users' privacy.

4.1. Management of User Information

Over both time frames, Facebook's policies in particular included many changes related to the company's collection and use of information. Positively, changes during the first time frame clarified what information the company requires when new users join, and what additional information users can provide. The revised policy contained clear examples of what Facebook considers user content; the previous version of the policy told users to check the company's Terms of Use for a definition. However, the policy changes also disclose Facebook collecting more user information over both timeframes (see Annex Table A.1., rows 1–2, changes in bold).

Microsoft and Facebook included changes related to retention. In the first time frame, Microsoft positively added a sentence stating that it stores information about a user's behavior (e.g. page views, clicks, and search terms) separately from information that identifies the user (e.g., name, e-mail address) (see Table A.1., row 3). Somewhat positively, Facebook added a sentence describing a time frame in which it anonymizes data it receives from advertisers, but it applies only to information the company doesn't already have (see Table A.1., row 4). This suggests that some advertising-related user information is not subject to anonymization. In the second time frame, Facebook stated that apps connected to Facebook might retain user information after users delete the app (see Table A.1., row 5). Facebook also added a sentence saying users could contact the app directly and request deletion of their data.

Overall, changes across both timeframes suggest companies, primarily Facebook, provided additional detail regarding what they collect and how they manage it. In some cases, this can help users better understand company practices, for example what information they must provide and what is optional.

4.2. Data Sharing and Tracking

Yahoo and Facebook included changes related to sharing user information with governments, though the changes do not appear to be linked to PRISM (see Annex Table A.2., rows 1–2). Yahoo stated that it responds to law enforcement requests; PRISM requests fall under national security. Facebook added a sentence stating that it may disclose user information in response to requests from foreign jurisdictions; PRISM requests come from the U.S. government.

Several companies added information to policies related to their use of targeted advertising: Microsoft and YouTube in the first time frame; Skype, Yahoo, and Twitter in the second time frame; and Facebook across both timeframes. Changes in Facebook's policies appeared to give the company wider latitude in sharing user information, particularly with advertisers.

In the first time frame, Microsoft added more companies as advertising partners. It also listed the types of data it uses to target advertising (see Table A.2., row 3). Microsoft added that advertising networks compile information "over time" about where users click or see advertisements and may "associate this information with your subsequent visit, purchase or other activity on participating advertisers' websites in order to determine the effectiveness of the advertisements". Finally, Microsoft removed a sentence from its policy, raising questions about its access to advertising networks' cookies (see Table A.2., row 4). Changes in YouTube's policies state that it shows users advertising even when they are logged out, that advertisers can serve ads based on demographic categories inferred from users' behavior, and that they can serve ads based on user information obtained from other companies (see Table A.2., rows 5–7).

In the second time frame, Yahoo added two sentences to its policy that explain how it uses device identifiers to target advertising, framed in the parlance of personalization (see Table A.2., row 8). Twitter added two sentences about user information it may receive from advertising partners (see Table A.2., row 9). Skype added language suggesting that third-party advertisements would appear on its various sites and that Skype and its advertising partners would receive information (changes in bold) "about your relationship with **and use of** Skype's websites, software, and products…".

Changes in Facebook's policies over both time frames appeared to give the company wider latitude to share information, particularly with advertisers. In the first time frame, Facebook removed the phrase stating that it shares information with third parties "only in limited circumstances". The policy gained two sentences explaining what types of information Facebook uses when targeting advertising and how advertisers may interact with users. Facebook stated it only uses non-personally identifiable attributes but then stated that it may use sensitive, personal information to target advertising, and that advertisers may be able to discern that information (see Table A.2., row 10). In the second time frame, Facebook revised the following sentence about how it shares information with advertisers (changes in bold):

> 2012: We only provide data to our advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it is no longer **associated** with you.
>
> 2013: We only provide data to our advertising partners or customers after we have removed your name **and** any other personally identifying information from it, or have combined it with other people's data in a way that it no longer **personally identifies** you.

While the shift from "or" to "and" seems to provide greater protection to users, the shift from the higher threshold of association to the lower threshold of "personally identifiable" seems to negate that protection, because information that does not personally identify a user can still be associated with a user and thus can identify the user. Facebook also revised its policy to more clearly state that it uses all user information to target advertising (see Table A.2., row 11).

While these additions provide more detail for users to understand company practices, the practices themselves appear to subject users to greater tracking for advertising purposes. They include examples of companies tracking users in more circumstances and using more information to target those ads. The disclosures also use jargon such as "non-personally identifiable information" and "device identifiers" and they reference the data processing techniques of inference and association, the nuances of which are likely unfamiliar to average users. This can make it difficult for anyone who actually reads privacy policies to fully understand what the policies mean.

5. Privacy Policy Changes Offer Evidence of Surveillance Capitalism

Collectively, these privacy policy changes offer evidence that suggests several of the world's largest Internet companies operate according to the logic surveillance capitalism. We cannot know whether these privacy policy changes reflected actual changes in company practice or if they provided more detail about practices in which companies already engaged. But the changes suggest that between the time the companies joined PRISM and the public learned of PRISM, companies disclosed that they managed more user information and, in particular, broadened their targeted advertising.

Targeted advertising is the dominant business model that powers most Internet companies today (Richards, 2013). This entails collecting data from individuals' digital interactions, however minor: "Facebook 'likes', Google searches, emails, texts, photos, songs, and videos, location, communication patterns, networks, purchases, movements, every click, misspelled word, page view, and more" (Zuboff, 2015, p. 79). Companies then employ advanced data analysis techniques to determine how to use such data to extract revenue from advertisers, transforming the data into what Zuboff calls "surveillance assets" (2015, p. 80).

As a condition for using such services, people must agree to terms such as those in privacy policies, whose narrow definitions and vague language prevent people from understanding how their data flows through the life cycle of user information (Kumar, 2016). This model, which puts the onus on users to manage their own privacy and hinges on whether they "consent" to such practices, does not meaningfully protect users' privacy (Solove, 2013).

Beyond disclosing their practices in policies, companies justify their big data activities by arguing that users gain something in return, for example, free services or personalized experiences. People pay for these benefits by foregoing their right to decide whether to disclose a given facto or keep it to themselves. As such, surveillance does not erode privacy rights; it redistributes them, enabling companies or governments to know information about people without their ever having a choice (Reidenberg, 2015; Zuboff, 2015).

PRISM is one example of "the blurring of public and private boundaries in surveillance activities...between state security authorities and high tech firms" (Zuboff, 2015, p. 86). Companies collect and retain massive amounts of data about their users—itself an act of surveillance (Richards, 2013)—and the NSA can compel companies to turn over that data for targeted surveillance. The PCLOB report (2014) reviewed the checks and balances under which the government's PRISM program operates. However, the surveillance activities of companies in PRISM do not operate with as much oversight. Debates about privacy rights in a post-Snowden world cannot ignore the fact that companies have business incentives to collect and retain the data that governments can obtain through surveillance activities.

6. Conclusion: Government Surveillance as a Symptom of Surveillance Capitalism

PRISM did not cause surveillance capitalism, but this analysis suggests that PRISM companies further enmeshed themselves in it over the past decade. They did so while belonging to a secret surveillance program in which the U.S. government could compel them to turn over all the information they had associated with a given user's email address or telephone number. The PRISM companies serve billions of users worldwide. They have the power to adopt business practices that significantly enhance the privacy of everyday users. This analysis of privacy policy changes that companies made between joining PRISM and PRISM's disclosure to the public suggests that companies went in the other direction by expanding their use of targeted advertising. It illustrates that public debates about people's privacy rights in the wake of the Snowden disclosures must not ignore the role that companies themselves play in legitimizing surveillance activities under the auspices of creating market value.

Acknowledgements

I thank Nathalie Maréchal, Katie Shilton, Karen Boyd, and Jessica Vitak for their input. I also thank the editors and three anonymous reviewers, whose feedback significantly strengthened this work.

Conflict of Interests

The author declares no conflict of interests.

References

Bellia, P. L. (2008). The memory gap in surveillance law. *University of Chicago Law Review*, *75*, 137–179.

Blodget, H. (2013, June 7). The Washington Post has now hedged its stunning claim about Google, Facebook, etc, giving the government direct access to their servers. *Business Insider*. Retrieved from http://www.businessinsider.com/washington-post-updates-spying-story-2013-6

Butler, J., & Granick, J. S. (2016). Correcting the record on section 702: A prerequisite for meaningful surveillance reform. *Just Security*. Retrieved from https://www.justsecurity.org/wp-content/uploads/2016/09/Butler-Granick-Correcting-the-Record-Scope-of-702.pdf

Gallagher, R., & Hager, N. (2016, August 14). In bungled spying operation, NSA targeted pro-democracy campaigner. *The Intercept*. Retrieved from https://theintercept.com/2016/08/14/nsa-gcsb-prism-surveillance-fullman-fiji

Gellman, B., & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. Retrieved from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Jeong, S. (2016, January 14). The history of Twitter's rules. *Vice Motherboard*. Retrieved from http://motherboard.vice.com/read/the-history-of-twitters-rules

Kumar, P. (2016). Privacy policies and their lack of clear disclosure regarding the life cycle of user information. *2016 AAAI Fall Symposium Series*. Retrieved from http://aaai.org/ocs/index.php/FSS/FSS16/paper/view/14089

MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for Internet freedom*. New York, NY: Basic Books.

Maréchal, N. (2015). Ranking digital rights: Human rights, the Internet and the fifth estate. *International Journal of Communication*, *9*, 3440–3449.

Martin, S. (2013, June 7). Twitter notably absent from NSA PRISM list. *USA Today*. Retrieved from http://www.usatoday.com/story/tech/2013/06/07/nsa-prism-twitter/2401605

Miller, C. C. (2013, June 7). Tech companies concede to surveillance program. *The New York Times*. Retrieved from http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html

Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*, *25*(2), 238–249. doi:10.1509/jppm.25.2.238

Murphy, J., Hashim, N. H., & O'Connor, P. (2007). Take me back: Validating the Wayback Machine. *Journal of Computer-Mediated Communication*, *13*(1), 60–75. doi:10.1111/j.1083-6101.2007.00386.x

Ni Loideain, N. (2016). The end of safe harbor: Implications for EU digital privacy and data protection law. *Journal of Internet Law*, *19*(8), 7–14.

Opsahl, K. (2010, April 28). Facebook's eroding privacy policy: A timeline. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2010/04/facebook-timeline

Privacy and Civil Liberties Oversight Board. (2014). *Report on the surveillance program operated pursuant to section 702 of the Foreign Intelligence Surveillance Act*. Washington, DC: Privacy and Civil Liberties Oversight Board.

Ranking Digital Rights. (2016a, September 14). *Methodology development*. Retrieved from https://rankingdigitalrights.org/methodology-development

Ranking Digital Rights. (2016b, September). *2017 corporate accountability index research indicators*. Retrieved from https://rankingdigitalrights.org/wp-content/uploads/2016/09/2017Indexmethodology.pdf

Reidenberg, J. R. (2015). The transparent citizen. *Loyola University Chicago Law Journal*, *47*, 437–463.

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review*, *126*, 1934–1965.

Schwartz, P. M., & Solove, D. J. (2014). Reconciling personal information in the United States and European Union. *California Law Review*, *877*, 877–916.

Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*, 1880–1903.

Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation*, *27*(2), 237–246. doi:10.1177/1098214005283748

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*, 75–89. doi:10.1057/jit.2015.5

About the Author

Priya Kumar is a doctoral student at the University of Maryland College of Information Studies. She studies privacy from various perspectives, including corporate accountability and computer-mediated communication. Priya holds an MS in Information from the University of Michigan and BA degrees in journalism and government and politics from the University of Maryland. Find her on Twitter at @DearPriya.

Annex

Table A.1. Privacy policy changes related to management of user information.

	Company	Timeframe 1		Timeframe 2	
		Pre-Join PRISM	Post-Join PRISM	Pre-PRISM Disclosed	Post-PRISM Disclosed
1	Facebook	2008: "When you enter Facebook, we collect your browser type and IP address."	2009: "When you **access** Facebook **from a computer, mobile phone, or other device**, we **may** collect **information from that device about** your browser type, **location**, and IP address, **as well as the pages you visit**."		
2	Facebook			2012: "This may include your IP address and other information about things like your Internet service, location, the type (including identifiers) of browser you use, or the pages you visit."	2013: "This may include **network and communication information, such as** your IP address **or mobile phone number**, and other information about things like your Internet service, **operating system**, location, the type (including identifiers) **of the device or** browser you use, or the pages you visit."
3	Microsoft		2007: **Added** "For example, we store page views, clicks and search terms used for ad personalization separately from your contact information or other data that directly identifies you (such as your name, e-mail address, etc.)."		
4	Facebook		2009: **Added** "If in any of these cases we receive data [from advertising partners] that we do not already have, we will 'anonymize' it within 180 days, meaning we will stop associating the information with any particular user."		
5	Facebook				2013: **Added** that when users delete an app connected to Facebook, "it [the app] may still hold the information you have already shared."

Table A.2. Privacy policy changes related to data sharing and tracking.

	Company	Timeframe 1		Timeframe 2	
		Pre-Join PRISM	Post-Join PRISM	Pre-PRISM Disclosed	Post-PRISM Disclosed
1	Yahoo			2013: "We respond to subpoenas, court orders, or legal process or to establish or exercise our legal rights or defend against legal claims."	2014: "We respond to subpoenas, court orders, or legal process **(such as law enforcement requests)**, or to establish or exercise our legal rights or defend against legal claims."
2	Facebook	2008: "We may **be required to** disclose user information pursuant **to lawful requests, such as subpoenas or court orders**, or in compliance with applicable laws. **We do not reveal information until** we have a good faith belief that **an information request by law enforcement or private litigants meets applicable legal standards**."	2009: "We may disclose information pursuant to **subpoenas, court orders, or other requests (including criminal and civil matters)** if we have a good faith belief that **the response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards.**"		
3	Microsoft		2007: **Added** "For example, we may select the ads we display according to certain general interest categories or segments that we have inferred based on "(a) demographic data, including any you may have provided when creating an account (e.g. age, zip or postal code, gender), general demographic data acquired from other companies, and a general geographic location derived from your IP address, (b) the pages you view and links you click when using Microsoft's and its partners' web sites and		

Table A.2. Privacy policy changes related to data sharing and tracking. (Cont.)

	Company	Timeframe 1		Timeframe 2	
		Pre-Join PRISM	Post-Join PRISM	Pre-PRISM Disclosed	Post-PRISM Disclosed
3	Microsoft		services, and (c) the search terms you enter when using Microsoft's Internet search services, such as Live Search."		
4	Microsoft		2007: **Removed** "Microsoft does not have access to the cookies that may be placed by the third-party ad servers or ad networks."		
5	YouTube	2009: "**If** you are **logged into** your YouTube Account, we may also show you advertising based on **the information** you have provided to us in your YouTube Account."	2010: "**While** you are logged in **or logged out** of your YouTube Account, we may also show you advertising based on **non personally identifiable** information you have provided to us in your YouTube Account."		
6	YouTube	2009: "Advertisers may serve ads based on **interests** associated with non-personally identifiable online activity, such as videos viewed, frequency of uploading or activity on other AdSense partner sites."	2010: "Advertisers may serve ads based on interests **and demographic categories** associated with non-personally identifiable online activity, such as videos viewed, frequency of uploading or activity on other AdSense partner sites."		
7	YouTube	2009: "Advertisers may also serve ads to you based on previous activity on that advertiser's website."	2010: "Advertisers may also serve ads to you based on previous activity on that advertiser's website **or based on non-personally identifiable information from other companies**."		
8	Yahoo				2014: **Added** "We may also set and access device identifiers which could include IP address, user agent information (browser version, OS type and version), and device provided identifiers. Once you log into Yahoo on your device, Yahoo may recognize your device to provide you with a

Table A.2. Privacy policy changes related to data sharing and tracking. (Cont.)

	Company	Timeframe 1		Timeframe 2	
		Pre-Join PRISM	Post-Join PRISM	Pre-PRISM Disclosed	Post-PRISM Disclosed
8	Yahoo				personalized experience, independent of your device settings.”
9	Twitter				2013: **Added** “Third-party ad partners may share information with us, like a browser cookie ID or cryptographic hash of a common account identifier (such as an email address), to help us measure ad quality and tailor ads. For example, this allows us to display ads about things you may have already shown interest in.”
10	Facebook		2009: **Added** “We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show to other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements...Even though we do not share your information with advertisers without your consent, when you click on or otherwise interact with an advertisement there is a possibility that the advertiser may place a cookie in your browser and note that it meets the criteria they selected.”		

Table A.2. Privacy policy changes related to data sharing and tracking. (Cont.)

	Company	**Timeframe 1**		**Timeframe 2**	
		Pre-Join PRISM	Post-Join PRISM	Pre-PRISM Disclosed	Post-PRISM Disclosed
11	Facebook			2012: "We use the information we receive, including the **information you provide at registration or add to your account or timeline, to deliver** ads **and to make them** more relevant to you."	2013: "**So we can show you content that you may find interesting**, we **may** use all of the information we receive **about you** to serve ads that are more relevant to you."

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 76–83
DOI: 10.17645/mac.v5i1.810

Article

Metadata Laws, Journalism and Resistance in Australia

Benedetta Brevini

Department of Media and Communication, The University of Sydney, Sydney, NSW 2006, Australia;
E-Mail: benedetta.brevini@sydney.edu.au

Submitted: 31 October 2016 | Accepted: 2 March 2017 | Published: 22 March 2017

Abstract

The intelligence leaks from Edward Snowden in 2013 unveiled the sophistication and extent of data collection by the United States' National Security Agency and major global digital firms prompting domestic and international debates about the balance between security and privacy, openness and enclosure, accountability and secrecy. It is difficult not to see a clear connection with the Snowden leaks in the sharp acceleration of new national security legislations in Australia, a long term member of the Five Eyes Alliance. In October 2015, the Australian federal government passed controversial laws that require telecommunications companies to retain the metadata of their customers for a period of two years. The new acts pose serious threats for the profession of journalism as they enable government agencies to easily identify and pursue journalists' sources. Bulk data collections of this type of information deter future whistleblowers from approaching journalists, making the performance of the latter's democratic role a challenge. After situating this debate within the scholarly literature at the intersection between surveillance studies and communication studies, this article discusses the political context in which journalists are operating and working in Australia; assesses how metadata laws have affected journalism practices and addresses the possibility for resistance.

Keywords

digital resistance; journalists; metadata; surveillance

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).

1. Introduction

The intelligence leaks from Edward Snowden in 2013 unveiled the sophistication and extent of data collection by the US's National Security Agency and major global digital firms prompting domestic and international debates about the balance between security and privacy, openness and enclosure, accountability and secrecy (Brevini, 2017). While many authors (Andrejevic, 2002, 2013; Lyon, 2014; Van Dijck, 2014) have warned about massive data collection by governments and businesses as a challenge to civil rights, there a need to encourage further public discussion around the world on the chilling effect that these data retention frameworks can have on freedom of the press, on journalists and on their ability to exert their traditional watchdog function (Lashmar, 2016). After situating this debate within the scholarly literature at the intersection between surveillance studies and communication studies, this article discusses the political context in which journalists are operating and working in Australia; assesses how metadata laws have affected journalism practices and addresses the violation of privacy for journalists and the emergence of a resistance.

2. From Surveillance Society to Resistance

Surveillance has been defined as the "collection and analysis of information about populations in order to govern their activities" (Ericson & Haggerty, 2006, p. 3) so the literature coming from surveillance studies becomes of great relevance in investigating the impact of metadata laws on journalism practices.

Yet, because of the unprecedented development of information and communication technologies, surveillance scholars have rightly pointed at the new ubiquitousness and embeddedness of surveillance in every aspects of life in current networked societies (Lyon, Haggerty, & Ball, 2012), going much beyond traditional and centralised institutional settings.

As a consequence of the accelerated development of a communication technologies, Mann and Ferenbok (2013) have also explored the possibility for “sousveillance” (Mann & Ferenbok, 2013, p. 19), surveillance from the bottom up, where the surveilled is empowered through technology to fight back and enact change from below through mutual watching and monitoring.

While digital surveillance practices have now been amply studied within surveillance studies, there is still great scope for development in the field of communication studies. In this article, I propose to investigate whether we can detect a space for resistance for journalists working within new metadata frameworks. This space is conceptualised as “field of struggles” (Bordieu, 1983)—a bourdieusian concept—that is helpful in investigating this space for agency.

In the launch edition of a new journal Big Data and Society, Couldry and Powell (2014) developed the argument that a question of agency is paramount to our understanding of big data, thus opening up a new research agenda for investigating not only dominant forms of data power, but also alternative forms of datafication emerging from civil society groups, community organisations, journalists .This study takes up this challenge by focusing specifically on the field of struggle (Bordieu, 1983) where journalists operate.

2.1. The Australian Context

Since the attacks of September 2001, there has been a steady increase in number of national security laws in Australia. Over fifty laws were passed to create new criminal offences, new detention, extended investigative powers for security and police officers, new tools to control people’s movements and activities without criminal convictions (Ananian-Welsh & Williams, 2014). There is also a worrying tendency to limit courts’ powers to review the legality of government action especially on matters of national security. At the same time, there is a clear trend towards an intensification of government secrecy and an extension of its own powers to limit the public’s rights of access to information, thus making court reviews in these areas even more crucial (Human Rights Law Centre [HRLC], 2016).

In this context, the Snowden leaks (Brevini, 2017) and their challenges to state secrets can explain the haste that has characterised discussion and implementation of three major pieces of new national security laws in Australia between 2014 and 2015. As Attorney General George Brandis explained during the reading of the bill amending the Australian Security Intelligence Organisation Act 1979 (ASIO Act) and the Intelligence Services Act 2001 (IS Act), the reform is justified by a clear intent to curb whistleblowing activities:

> As recent, high-profile international events demonstrate, in the wrong hands, classified or sensitive information is capable of global dissemination at the click of a button. Unauthorised disclosures on the scale now possible in the online environment can have devastating consequences for a country’s international relationships and intelligence capabilities. (Brandis, 2014)

The newly created metadata laws cannot be properly understood without considering the overall context of increased tightening of national security laws and investments in cybersecurity. In light of this, the Australian government announced in its 2015 budget that it will provide:

> $450 million to strengthen Australia’s intelligence capabilities, including updating information technology systems and to counter extremist messaging. This includes $131 million to help the telecommunications sector upgrade its systems to retain metadata for two years. (Australian Government, 2015a)

As I will discuss later, the newly established framework is clearly at odds with a more recent tendency that is emerging in courts throughout Europe and the US and backed by international human rights mandates, where a clearly hostile attitude towards disproportionate digital surveillance is being displayed (see for example, Cannataci, 2016; Kaye, 2015).

3. Data Retention in Australia

The revised Telecommunications (Interception and Access, TIA) Act, passed in 2015, sought to specify “the types of data the telecommunications industry should retain for law enforcement and national security purposes or how long that information should be held”. Rapid, ongoing changes occurring in the telecommunications environment have, apparently, “undermined” any systematic access to the tools and data that may be available (The Parliament of the Commonwealth of Australia, 2015a, p. 2). Recognising the variations that exist in the holding and maintenance of types of data in the telecommunications industry, the TIA Act demands the “standardisation” of such records for governmental use (The Parliament of the Commonwealth of Australia, 2015a). It is claimed that previous inconsistencies have impeded governmental efforts to “investigate and to prosecute serious offences” (The Parliament of the Commonwealth of Australia, 2015a).

Both houses have, therefore, passed this Bill, which oversees the implementation of a national data retention scheme. This scheme compels telecommunications service providers to “retain, for two years, particular types of telecommunications data” (The Parliament of the Commonwealth of Australia, 2015a).

The TIA Act cites several recommendations delivered by the Parliamentary Joint Committee for Intelligence and Security (PJCIS) as the basis for its framework, including that:

- the data retention obligation only applies to telecommunications data (not content) and internet browsing is explicitly excluded;
- service providers are required to protect the confidentiality of retained data by encrypting the information and protecting it from unauthorised interference or access;
- mandatory data retention will be reviewed by the PJCIS by three years after its commencement (The Parliament of the Commonwealth of Australia, 2015a, p. 3).

Telecommunications data, in this instance, has been largely characterised as metadata: that is data excluding "content" (The Parliament of the Commonwealth of Australia, 2015a, p. 7) such as the source and destination of a communication, subscribers' information, date, time and duration of a communication or connection to a service.[1]

The 2015–2016 Budget includes $153.8 million over four years to "support the implementation and ongoing management" of the data retention scheme, including $131.3 million over three years for telecommunications service providers (Australian Government, 2015b).

Access to citizens' metadata is therefore conferred without judicial oversight. No warrant is required by the 21 criminal law-enforcement agencies that have been permitted the capacity to requisition these records (Farrell, 2016; The Parliament of the Commonwealth of Australia, 2015a).

The explanatory memorandum for the TIA Act does, however, set out a "compatibility with human rights" statement, in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011 (The Parliament of the Commonwealth of Australia, 2015a, p. 5). This statement, which is expanded upon over the course of 30 pages, includes certain caveats and safeguards to ensure the Act's compliance with the upholding of basic civil liberties. It therefore assures, among other things, that:

> The Bill…amends the TIA Act to bolster the privacy protections associated with the access to, and use of, telecommunications data. It achieves this by limiting the agencies which may authorise access to telecommunications data, and by providing that agencies' access to, and use of, telecommunications data is subject to comprehensive oversight by the Commonwealth Ombudsman. (The Parliament of the Commonwealth of Australia, 2015a, p. 6)

The statement asserts that the Bill "is compatible with human rights because it promotes a number of human rights". This is, however, followed by the disclaimer that "to the extent that (the Bill) may also limit human rights, those limitations are reasonable, necessary and proportionate" (The Parliament of the Commonwealth of Australia, 2015a, p. 36).

4. TIA Act and Its Impact on Journalists

In 2015, an amendment to the proposed TIA Act was put forward in the wake of concerns about how a data retention scheme might affect the media. It was recognised that a data retention scheme could "adversely affect" the media's capacity "to provide accurate and reliable information" (The Parliament of the Commonwealth of Australia, 2015b, p. 33) and leave sources vulnerable. The House of Representatives, thus, agreed to the implementation of a "journalist information warrant" regime, which prohibits agencies from "making authorisations to access journalists or their employers' data for the purpose of identifying a confidential source unless a journalist information warrant is in force" (The Parliament of the Commonwealth of Australia, 2015b, p. 33). This also means that journalists' metadata can always be accessed unless the agency is seeking data specifically for the purpose of identifying a journalist's source.

It is at the discretion of an "issuing authority" to issue or refuse the authorisation of a journalist information warrant, based on their understanding of the public interest (The Parliament of the Commonwealth of Australia, 2015a, p. 79). Issuing authorities are judicial officers approved by the minister or members of the Administrative Appeals Tribunal, or lawyers who are appointed by the minister.

It should also be noted that in the case of ASIO, it will be the minister that will issue the warrant. (The Parliament of the Commonwealth of Australia, 2015a, p. 33). According to the law, information warrants will be issued only when the "public interest in the issue of the warrant outweighs the public interest in maintaining the confidentiality of the source" (The Parliament of the Commonwealth of Australia, 2015a, p. 33).

The installation of (a) Public Interest Advocate(s) should be an additional measure by which the Act seeks to establish independence (The Parliament of the Commonwealth of Australia, 2015a, p. 33). The Public Interest Advocate can make submissions to requests for journalists' data, defending the need to maintain or discard

[1] In January 2016, Australian Privacy Commissioner Timothy Pilgrim appealed a decision of the Administrative Appeals Tribunal (Telstra Corp Ltd and Privacy Commissioner [2015] AATA 991 of 8 December 2015) that mobile phone metadata held by telecom provider Telstra were not "personal information" about its customers under the Australian Privacy Act 1988 This appeal has given the Federal Court a landmark opportunity to establish whether metadata constitutes personal information thus redefining data protection law in Australia. In 19 January 2017 the Federal Court has closed the case and delivered a groudbreaking decision that will have long lasting implications on how metadata is understood by Australians, and the access private citizens will be granted to their own data and digital trails: the Court decided that the mobile phone in question was not "personal information", effectively enshrining this interpretation into law and drastically narrowing the definition of "personal information" under the Privacy Act.

confidentiality, which the minister must consider as a part of the warrant's application. These may include conditions and/or restrictions (The Parliament of the Commonwealth of Australia, 2015a, p. 83). The Public Interest Advocate will, however, not be allowed to seek the advice of media entities, be it the journalist or the organisation, addressed in the journalist information warrant (Keane, 2015a). Indeed, the status of journalists and media organisations as parties subject to a warrant will not be permitted for disclosure (Keane, 2015a). It is so secret that there are two-year jail terms for disclosure, of the mere existence or non existence of a journalist information warrant, while journalists will not be informed of the request being pursued.

It is difficult not to see the flaws in this system and its detrimental effects on the practice of journalism. The journalist information warrant operates in secret, while journalists and their media organisation will never know if access was granted. It will still allow journalists' metadata to be accessed to identify a journalist's sources, while the public interest advocates won't be able to argue in defence of the public watchdog role of news organisation and their responsibility to protect the identity of a source. As journalist Laurie Oakes recalled: "metadata collection is the great press freedom issue of the internet age". The aggressive attitude towards whistleblowers means that governments "now hunt down those leakers with zeal and this means that metadata is their friend" (Oakes, 2015).

5. From Metadata Laws to Special Intelligence Operations Reform: Targeting Journalist's Sources

As discussed, the metadata retention scheme enforced by TIA 2015 has obvious consequences not only for journalists but for their sources, and whistleblowers. However, TIA, combined with another amendment of Australian National Security laws, specifically section 35P of the ASIO has even a greater detrimental impact on journalists' sources.

Under Section 35P of the ASIO Act 1979, those who have "disclosed information relating to a special intelligence operation" may be imprisoned for five to ten years (The Parliament of the Commonwealth of Australia, 2014, p. 71). A "special intelligence operation" can be understood as operations where ASIO agents are granted legal immunity for engaging in a range of otherwise criminal conduct. The most "basic" breach, in which information is simply disclosed, can result in a five-year penalty. Where a disclosure endangers "the health or safety of a person", the Act permits a penalty of ten years. This penalty applies regardless of whether the citizen or journalist in question is aware of an operation's status.

In a report commissioned by the Department of the Prime Minister and Cabinet (DPMC), the impact of this piece of legislation is suggested to be twofold: a gag order like 35P may instil a "chill effect" on publications about the activities of ASIO, and prevent "reprehensible conduct" by ASIO insiders from being susceptible to public scrutiny (DMPC, 2015). According to the report, such an impact is "unjustified" despite the need for secrecy in many ASIO operations. The inadequate protection of the rights of "outsiders", it argues, "infringes the constitutional protection of freedom of political communication" (DPMC, 2015). This new provision is concerning for a number of reasons. First, without an explicit verification from ASIO, it is extremely difficult for a journalist to know whether an ASIO operation is a special intelligence operation or not. Additionally, the new section criminalises both intentional and reckless disclosure, so journalists are likely to take a conservative approach to publication and avoid pursuing reporting of ASIO's activities for fear of being prosecuted. This will indeed lead to a progressive self-imposed censorship of journalists and a progressive lack of public reporting in formal publications or through anonymous disclosures and scrutiny of intelligence activities.

As the controversy around Australian asylum seekers policy arose, in 2015,[2] the Australian Government expanded secrecy laws frameworks and penalties for whistleblowers through the controversial Border Force Act. The legislation makes it unlawful for a Department of Immigration and Border Protection's employee or contractor, such as a social worker, a nurse, a doctor or welfare services provider, to disclose or record certain information obtained while carrying out their duties. The penalty for such a disclosure is up to two years in jail (HRLC, 2015).

As The Guardian's Paul Farrell commented:

> This is a move that should alarm all citizens. It's not an attack on any particular news outlet. It's an attack on those who have reported on matters of significant public interest in the increasingly secretive area of asylum seeker policy….These kind of attacks [sic] severely damage the confidence between reporters and their sources and pose a grave threat to effective and responsible journalism. When the federal police go knocking on the doors of a reporter's sources, sources will soon dry up. People will be scared. And that is exactly the point. (Farrell, 2015)

It is important to note that the Border Protection Act has been amended in October 2016 exempting health professionals from the definition of "immigration and border protection workers" following the pressures coming from the health professionals who challenged the Government in the High court (Hall, 2016). However, the current ban remains in place for others, such as child protection workers and teachers, who witnessed abuses in offshore detentions (Hall, 2016).

[2] For a good summary of controversial Australian Asylum policies and United Nations (UN) criticism please, see "Australia Asylum: Why Is It Controversial?" available at http://www.bbc.com/news/world-asia-28189608

6. A Look at the Current International Context

The newly established metadata scheme regime clearly posits new challenges not only for journalism practices but for the effectiveness of shield laws which are meant to prevent journalists from being forced to reveal their sources. It is also quite unclear how the current Australian national framework for data collection corresponds to, or addresses, existing international conventions, treaties or policies on free speech, political, economic and cultural inclusion. For example the European Court of Justice in April 2014 invalidated the EU's Data Retention Directive, which is very similar to the Australian scheme. In particular, "the Court held that the Directive entailed serious interference with the rights to privacy and personal data protection of individuals guaranteed by the Charter of Fundamental Rights, and also failed to establish limits on access by competent national authorities, such as prior review by a judicial or an independent administrative authority" (Data Retention Directive, 2014). The lack of safeguards around the access and use of metadata was a key reason for the directive to be in breach of the fundamental right to privacy.

Australia's attitude towards metadata frameworks is not unique in international settings. The first report issued by the UN rapporteur on privacy has noted that the country monitoring process of the last year has "revealed several examples of legislation being rushed through national parliaments in an effort to legitimise the use of certain privacy-intrusive measures by Security and Intelligence Services (SIS) and law enforcement agencies" (Cannataci, 2016, p. 6). Moreover, the report notes that there is a contradictory trend between governments and international attitude towards metadata regimes:

> The tensions between security, corporate business models and privacy continue to take centre stage but the last twelve months have been marked by contradictory indicators: some governments have continued, in practice and/or in their parliaments to take privacy-hostile attitudes while courts world-wide but especially in the USA and Europe have struck clear blows in favour of privacy and especially against disproportionate, privacy-intrusive measures such as mass surveillance or breaking of encryption. (Cannataci, 2016, p. 21)

The stand of the mandate of the International rapporteur on Privacy (Cannataci, 2016) is consistent with the indications of the UN, voiced by the former Rapporteur for Freedom of Information Frank La Rue.

> National data retention laws are invasive and costly, and threaten the rights to privacy and free expression. By compelling communications service providers to create large databases of information about who communicates with whom via a telephone or the Internet, the duration of the exchange, and the users' location, and to keep such information (sometimes for years), mandatory data retention laws greatly increase the scope of State surveillance, and thus the scope for infringements upon human rights. Databases of communications data become vulnerable to theft, fraud and accidental disclosure. (La Rue, 2013, p. 18)

The recommendations of the Rapporteur are clearly at odds with the newly approved Australian framework:

> Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law. (La Rue, 2013, p. 21)

7. Metadata Laws: Is There Room for Journalists' Resistance?

I have argued elsewhere (Brevini, 2017) that the revelations by whistleblower Edward Snowden triggered the birth of a new "new culture of disclosure" that has seen journalists, lawyers and software developers coming together to develop secure online protections and security of their sources. One of the most famous examples are Secure Drop and GlobaLeaks (Brevini, 2017) projects that aim at supporting the practice of whistleblowing by giving people the software tools necessary to start their own initiative. Unlike WikiLeaks (Brevini & Murdock, 2013), GlobaLeaks is an open-source software provider whose intentions are focussed on providing a platform for whistleblowers to use. GlobaLeaks does not handle any leaked documents but assists in the potential creation of whistleblowing sites such as OpenLeaks, MafiaLeaks, BalkanLeaks and BrusselsLeaks. However, there is also a more mainstream response to metadata laws: The New Yorker, the US not-for-profit investigative newsroom ProPublica, the Pierre Omidyar-backed start-up The Intercept and The Guardian are just a few examples of news providers that implemented a newly created open-source whistleblowing platform-SecureDrop to guarantee protections for their sources (Brevini, 2017).

In Australia,[3] the only platform of this kind is mediadirect.org, a platform that aims to encourage encrypted

[3] The paper adopted a multilayered methodological approach that combines policy and legal analysis with interviews with ten investigative Journalists in Australia that prefer to keep their anonymity.

disclosure by anonymous whistleblowers, thus protecting sources from the newly enhanced metadata laws. With a budget of about US$ 3,000 (Interview B)[4] the platform through encrypted interactions connects whistleblowers, who access it via the Tor network, and journalists (Keane, 2015b).

In light of the new metadata frameworks implemented in Australia, one would expect journalists rushing to demand an improved set of encryption tools, as well as formal training on anonymity mechanisms to protect their sources. However, our findings confirm not only a lack of knowledge of encrypting communications but also a lack of understanding of the risks of the newly established frameworks (Interview A, 2016).[5]

As one security consultant revealed:

> In a recent example, I just set them up to deal with the data, because they did not know how to deal with a major data leak. And when I got in there for the first meeting, one of the journalists said, "We'll print everything out". And I'm shocked: it's a million pages and hundreds of thousands of emails, how can we possibly print them? (Interview B, 2016)

Improving journalists' knowledge of encryption tools and their awareness of metadata laws should be a priority for media organisations, and perhaps one of the goals for Media Entertainment Alliance Australia.

Interviewees seemed to agree that the reasons for media institutions not to invest in security tools and training for their journalists has to do with the current financial crisis of journalism and the precarious conditions of reporters: when faced with the clear risk of losing their job, journalists are less keen to take risks and expose wrongdoings.

8. Conclusion

The newly established metadata scheme regime in Australia clearly undermines the work of journalists and the effectiveness of shield laws which were due to protect journalists from being forced to reveal their sources. As Crikey journalist Bernard Keane noted: "The threat arises from the existence and maintenance of data. That creates the chilling effect. You don't need a warrant to investigate a journalist if the agency can access the data of the whole department that the leak came from" (Keane 2015a).

The chilling effect on journalists and whistleblowers' activities are very consistent with findings of the scholarship in surveillance studies that have detected for example a similar pattern of "self censorship" on activists's or civil society groups' activities (see for example, Starr, Fernandez, Amster, Wood, & Caro, 2008).

There are obviously limits to what encryption and anonymity technologies can do to protect journalism practices, but the Australian case certainly shows that, aside from a few exceptions, journalists are currently not well equipped with the necessary know-how and awareness. In Bordieu's terms, journalists in the Australian context have not fully developed the resources or "capital" (Bordieu, 1983) to successfully oppose the collection and processing of personal data, thus developing a space for resistance to surveillance, radically different from "sousveillance" (Mann & Ferenbok, 2013).

It should also be noted that the findings of this study diverge from a recent study by Mills and Sarikakis (2016) that focused only on investigative journalists and found how investigative journalist in Western and non Western countries are engaging increasingly with technological and other communities to defend their work. Future research from Communication Studies perspective should engage with this recent scholarship to shed light on the crucial interplay between new metadata frameworks and journalism.

Conflict of Interests

The author declares no conflict of interests.

References

Ananian-Welsh, R., & Williams, G. (2014). New terrorists: The normalisation and spread of anti-terror laws in Australia. *The Melbourne University Law Review*, *38*, 362–408.

Andrejevic, M. (2002). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *2*(4), 479–497.

Andrejevic, M. (2013). *Infoglut: How too much information is changing the way we think and know*. Oxford: Routledge.

Australian Information Commissioner. (2015). Ben Grubb and Telstra Corporation Limited. *Austlii*. Retrieved from http://www.austlii.edu.au/au/cases/cth/AICmr/2015/35.html

Bourdieu, P. (1983). The field of cultural production, or: The economic world reversed. *Poetics*, *12*(4/5), 311–356.

Brandis, G. (2014). National Security Legislation Amendment Bill (No. 1) 2014, Second reading. *Parliament of Australia*. Retrieved from http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=CHAMBER;id=chamber%2Fhansards%2F232fa1a8-d7e8-4b22-9018-1a99b5a96812%2F0116;query=Id%3A%22chamber%2Fhansards%2F232fa1a8-d7e8-4b22-9018-1a99b5a96812%2F0173%22

Brevini, B. (2017). WikiLeaks: Between disclosure and whistle- blowing in digital times. *Sociology Compass*, *1*(3), 1–11.

Brevini, B., & Murdock, G. (2013). Following the money: WikiLeaks and the political economy of disclosure. In

[4] Interview via Skype, 10 May 2016.

[5] Interview via Skype, 3 May 2016.

B. Brevini, A. Hintz, & P. McCurdy (Eds.), *Beyond WikiLeaks: Implications for the future of communications, journalism and society* (pp. 35–55). Basingstoke: Palgrave Macmillan.

Cannataci, J. A. (2016). Report of the special rapporteur on the right to privacy. *Human Rights Council*. Retrieved from www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc

Couldry, N., & Powell, A. (2014). Big data from the bottom up. *Big Data & Society*, *1*(2). doi:10.1177/2053951714539277

Data Retention Directive. (2014). *European Union: ECJ invalidates data retention directive*. Retrieved from http://www.loc.gov/law/help/eu-data-retention-directive/eu.php

Department of the Prime Minister and Cabinet. (2015). *Report on the impact on journalists of section 35P of the ASIO Act*. Retrieved from https://www.dpmc.gov.au/pmc/publication/report-impact-journalists-section-35p-asio-act

Ericson, R. V., & Haggerty, K. D. (2006). *The new politics of surveillance and visibility*. Toronto: University of Toronto Press.

Farrell, P. (2015). Journalism is not a crime. So why are reporters being referred to police? *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2015/jan/22/journalism-is-not-a-so-why-are-reporters-being-referred-to-police

Farrell, P. (2016). Lamb chop weight enforcers want warrantless access to Australians' metadata. *The Guardian*. Retrieved from http://www.theguardian.com/world/2016/jan/19/lamb-chop-weight-enforcers-want-warrantless-access-to-australians-metadata

Hall, B. (2016). 'A huge win for doctors': Turnbull government backs down on gag laws for doctors on Naurus and Manus. *Sydney Morning Herald*. Retrieved from http://www.smh.com.au/federal-politics/political-news/a-huge-win-for-doctors-turnbull-government-backs-down-on-gag-laws-for-doctors-on-nauru-and-manus-20161019-gs6ecs.html

Human Rights Law Centre. (2016). *Safeguarding democracy*. Retrieved from http://www.bmartin.cc/dissent/documents/rr/HRLC16.pdf

Kaye, D. (2015). Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. *Human Rights Council*. Retrieved from http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361

Keane, B. (2015a). Finally the Labor coalition surveillance deal revealed. *Crikey*. Retrieved from http://www.crikey.com.au/2015/03/19/finally-the-labor-coalition-surveillance-deal-revealed/?wpmp_switcher=mobile

Keane, B. (2015b). Media direct: Towards better security for whistleblowers. *Crikey*. Retrieved from https://www.crikey.com.au/2014/05/26/media-direct-towards-better-security-for-whistleblowers

La Rue, F. (2013). Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. *United Nations Human Rights*. Retrieved from http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40

Lashmar, P. (2016). No more sources? The impact of Snowden's revelations on journalists and their confidential sources. *Journalism Practice*. doi:10.1080/17512786.2016.1179587

Lyon, D., Haggerty, K. D., & Ball, K. (2012). Introducing surveillance studies. In D. Lyon, K. D. Haggerty, & K. Ball (Eds.), *Routledge handbook of surveillance studies* (pp. 1–12). Oxford: Routledge.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1–13.

Mann, S., & Ferenbok, J. (2013). New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society*, *11*(1/2), 1–13.

Mills, A., & Sarikakis, K. (2016). Reluctant activists? The impact of legislative and structural attempts of surveillance on investigative journalism. *Big Data & Society*, *3*(2), 1–13.

Oakes, L. (2016). *Speech delivered at the Melbourne Press Club, 27 September 2015*. Retrieved from http://www.melbournepressclub.com/wp-content/uploads/2015/09/150925_Melbourne_Press_Freedom_Dinner_Oakes_speech.pdf

The Parliament of the Commonwealth of Australia. (2014). National security legislation amendment bill (No. 1) 2014: Bill as passed by both houses. *Parliament of Australia*. Retrieved from http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s969

The Parliament of the Commonwealth of Australia. (2015a). Telecommunications (Intercept and Access) Amendment (Data Retention) Bill 2015: Revised explanatory memorandum. *Parliament of Australia*. Retrieved from http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5375

The Parliament of the Commonwealth Australia. (2015b). Data Retention Bill: Budget Review 2015–16. *Parliament of Australia*. Retrieved from http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview201516/Telco

Australian Government. (2015a). *Budget 2015*. Retrieved from http://www.budget.gov.au/2015-16/content/highlights/nationalsecurity.html

Australian Government. (2015b). *Budget 2015–16* (Budget Paper no.2). Retrieved from http://www.budget.gov.au/2015-16/content/bp2/download/BP2_consolidated.pdf

Privacy Commissioner. (2015). Privacy Commissioner lodges appeal to Federal Court re Telstra Corporation Limited v Privacy Commissioner. *Office of the Australian Information Commissioner*. Retrieved from https://www.oaic.gov.au/media-and-speeches/state ments/privacy-commissioner-lodges-appeal-to-federal-court-re-telstra-corporation-limited-v-privacy-commissioner

Starr, A., Fernandez, L. A., Amster, R., Wood, L. J., & Caro, M. J. (2008). The impacts of state surveillance on political assembly and association: A socio-legal analysis. *Qualitative Sociology*, *31*(3), 251–270.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208.

About the Author

Benedetta Brevini is Senior Lecturer in Communication and Media at the University of Sydney, Visiting Fellow of Centre for Law Justice and Journalism at City University and Research Associate at Sydney Cyber Security Network. She is co-editor of the volume *Beyond WikiLeaks: Implications for the Future of Communications, Journalism & Society* (Palgrave MacMillan, 2013) and the author of *Public Service Broadcasting Online: A Comparative European Policy Study of PSB 2.0* (Palgrave MacMillan in August 2013). Before joining academia she has been working as a journalist in Milan, New York and London.

Media and Communication (ISSN: 2183-2439)

Media and Communication is an international open access journal dedicated to a wide variety of basic and applied research in communication and its related fields. It aims at providing a research forum on the social and cultural relevance of media and communication processes.

www.cogitatiopress.com/mediaandcommunication

COGITATIO