Cyber Security, Civil Society, and the Impact of State Surveillance

Jonathon W. Penney
Citizen Lab, University of Toronto
Schulich School of Law, Dalhousie University
Center for Information Technology Policy, Princeton University

INTRODUCTION

- Due to the "securitization" and "militarization" of cyber security, a process that arguably began in the 2000s with states increasing their information warfare capabilities for strategic advantage, cyber security remains predominantly framed in terms of national security (Deibert, 2013). This has led to increasing calls and proposals for approaches to cyber security more focused on civil society and human rights, as well as research demonstrating how certain cyber security strategies and practices have led to less security, not more.

- This has included calls, especially since the Snowden revelations, for more research on the implications of state surveillance—both mass and targeted forms—on people and cyber security more generally, as there is good reason to believe state surveillance practices ultimately weaken cyber security, while also harming the rights and interests of citizens. Despite these calls, cyber security literature remains narrow, dominated technological or policy focused analysis (Eriksson and Giacomello, 2014). Significant gaps persists, including research on the impact of surveillance.

- This paper (in completed form) aims to address this gap in the literature, with a case study that explores recent research on the impact of surveillance and considers these insights and their implications for cyber security. Overall, present empirical studies suggest state surveillance, rather than guaranteeing cyber security, helps undermine it, both in the near term and long term, in expected and unexpected ways.

WHY SURVEILLANCE?

- Why a case study on state surveillance? First, surveillance, it is said, is "fundamental" to cyber security as it "provides tools for prevention and detection" (Yang and Tucker, 2017: 2). It would thus be noteworthy if research suggests these same state surveillance practices, in fact, undermine cyber security rather than bolster it. Second, state surveillance practices have also been key to the aforementioned "securitization" of "cyberspace" and cyber security. If a key component of this securitization is shown to be fundamentally flawed, that is, running counter to both security and human rights interests, then efforts to establish a new approach to cyber security based on human rights and civil society interests would be strengthened.

- Moreover, there has recently been a range of new interdisciplinary empirical studies on the impact and dimensions of surveillance, particularly online and digital forms, which have yet to be brought to bear on cyber security. A good reason for this is likely due to cyber security's predominant focus on national security; there is little consideration for how cyber security practices like surveillance impact civil society or human rights. This paper also addresses this gap, setting out those impacts, and linking them to cyber security.

THEORETICAL FRAMEWORK

- Surveillance today typically concerns activities and information practices that enable a nation state to track or "manage" a population by monitoring individuals (Marwick, 2010; Lyon, 2007). David Lyon (2007) defines surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction". Surveillance can take "mass" form,

which is indiscriminate and aims to track entire populations (Schneier, 2015) or more targeted forms, usually with digital tools and methods that infiltrate "the networked devices and infrastructure of specific individuals, groups, organizations and communities" (Deibert, 2017; Deibert, 2013).

- There are different theoretical approaches to understanding the impact of surveillance. The one employed here is chilling effects theory, an interdisciplinary theoretical account of how certain laws and regulatory state actions—namely surveillance—can "chill" or deter people from speaking or engaging in other legal, constitutionally protected, and even desirable activities. Though based on a mix of theoretical and empirical work in law, economics, and privacy studies, chilling effect concerns have also been investigated in a range of other disciplines like sociology and psychology.

- Schauer (1978) and Solove (2006; 2007) offer the most commonly cited accounts of chilling effects theory, with Schauer linking "chilling effects" to deterrence based on fear of legal risk, punishment, and uncertainty in the legal system. Solove extends to include surveillance and other information practices and how such activities promote a climate of self-censorship and risk comparable to "environmental pollution" (2006: 487). Since all laws are assumed to have some form of deterrent effect—criminal laws, for example, deter illegal activities—chilling effects theory and research is specifically concerned with *legal* and constitutionally protect activities that have been chilled.

- Chilling effects theory offers a helpful analytical framework to understand a range of new empirical studies investigating the impact of surveillance—particularly digital and online forms—and its implications for cyber security. See e.g., Myers West (2017); Wahl-Jorgenson et al. (2017); van Schaik et al. (2017); Dencik et al. (2017); Dencik and Cable (2017); Penney (2017); Kwon and Rao, 2017; Lashmar (2017); Stoycheff (2016); Penney (2016); Mamonov and Koufaris (2016); and Marthews and Tucker (2014); PEN America, 2013; 2015; Pew Research, 2015; 2014a; 2014b.

IMPACT ON CIVIL SOCIETY

Chilling Speech and Promoting Self Censorship and Conformity

- Several new studies suggest both mass surveillance and targeted threats have significant chilling effects on people's speech, including online speech, leading to self-censorship and conformity. Stoycheff (2016) involved an experimental study where participant internet users agreed to "terms of agreement" that reminded participants their subsequent online activities were subject to interception and surveillance. The study found that exposing participants to these "terms of agreement" chilled their willingness to express their political views, with the greatest chilling effect for those who believed their political views were not mainstream. These findings support the notion of a "spiral of silence'', whereby individual, due to fear of isolation, moderate their political expression to conform with majority or mainstream views. In short, the study found that awareness of potential surveillance "chilled" online speech, leading to self-censorship, with the potential for greater social conformity, and less political dissent, at a societal level.

- Penney (2017) similarly found evidence surveillance would cause chilling effects and self censorship. This study involved a survey, administered to more than 1,200 U.S.-based adult internet users, designed to explore the impact of surveillance or digitally delivered targeted threats by comparing and analyzing user responses to hypothetical scenarios that, in theory, may cause chilling effects or other forms of self-censorship. The findings suggested once people were made aware of different online threats, they were far less willing to speak about certain topics online, and more cautious in their speech. For example, in terms of online speech, 62% of respondents indicated they would be "much less likely" (22%) or "somewhat less likely" (40%) to "speak or write about certain topics online" due to such online surveillance by government. And 78% of respondents "strongly" (38%) or "somewhat" agreed (40%) they would be more cautious about what they say online due to

the surveillance. In other words, the findings suggested a noteworthy chilling effect on speech and other expression online due to awareness of state surveillance.

- These findings are consistent previous findings by Pew Internet studies (2015; 2014a; 2014b) wherein Americans reported self-censoring and changing their online habits after learning about government surveillance programs through news reports about the Snowden disclosures.

Negatively Impacting Engagement, Content Sharing, and Search

- Evidence suggests a range of online activities are negatively impacted as well. The same study by Penney (2017) found that once people were made aware of online threats like government surveillance, internet users were less willing to engage in a range of other activities online, including less likely to contribute to social networks online, less willing to share personally created content, and more cautious about what they searched for online.

Unequal/Disparate Impact on Different Groups

- Surveillance may negatively impact or chill certain groups more than others. Penney (2017)'s findings also suggested a greater chilling effect on women and younger internet users. In every scenario examined, the study found a statistically significant age effect, where the younger the internet user, the greater the impact or chilling effect on the user's online activities. This statistical association was strongest in the scenario involving government surveillance. There was also a gender effect, where women were more impacted in scenarios involving surveillance as well as a scenario involving a digitally delivered targeted threat (here, a legal threat).

Chilling Information Access and Corroding Democratic Deliberation

- Two recent empirical studies, centered on Snowden's NSA/PRISM surveillance revelations in June 2013, provide evidence that mass government surveillance can have a widespread chilling effect on people's online activities, in particular, topics or information they read about or search for online. An MIT based study by Marthews and Tucker (2014) analyzed Google search trends before and after June 2013 and found a statistically significant reduction in searches for privacy-sensitive topics. Similarly, Penney (2016) examined Wikipedia article traffic on topics that raise privacy concerns over a period of 32 months before and after Snowden's revelations in June 2013. The study found not only a statistically significant immediate decline in traffic for privacy-sensitive Wikipedia articles after June 2013, but also a change in the overall secular trend in the traffic to these articles, suggesting not only immediate but also long-term chilling effects resulting from online surveillance revelations. This conclusion was strengthened by the fact that the view counts for several comparator groups of Wikipedia articles, which would not raise privacy concerns, remained unaffected through the same period of time.

- Given how Google search and Wikipedia are extremely popular online tools for millions of internet users to attain information, these two studies raise significant civil society and democratic concerns about whether citizens, under mass surveillance, will continue to seek out information about controversial matters of public importance (like terrorism) in order to stay informed and engage in healthy democratic deliberation.

Dampening Journalism and Activism

- A series of other recent qualitative and quantitative studies document how state surveillance impacts or chills journalistic practices while also dampening or rendering more difficult certain forms of activism: Myers West (2017); Lashmar (2017); Wahl-Jorgenson et al. (2017); Dencik et al. (2017); Dencik and Cable (2017); PEN America, 2013; 2015.

IMPLICATIONS FOR CYBER SECURITY

Undermines Cyber Security by Promoting or Maintaining Security Vulnerabilities

- A common and powerful criticism targeted state surveillance is that it undermines cyber security by promoting and maintaining security vulnerabilities that can be exploited by criminals and foreign adversaries (Deibert, 2013). Cyber security's predominant national security emphasizes *offensive* capabilities, in addition to defensive, wherein states exploit vulnerabilities in software and hardware to attack others (Schneier, 2015). Targeted surveillance often involves either actively inserting "backdoors" and other security vulnerabilities in software and hardware or leaving known vulnerabilities unpublished or unreported to exploit later for offensive operations like hacking, cyber-espionage, or surveillance tech. Snowden's revelations, for example, documented a number of instances where the NSA took steps to insert vulnerabilities into commercial software and weaken encryption standards (Schneier, 2015). With states working to covertly weaken hardware and software security while stockpiling vulnerabilities rather than publishing or disclosing to vendors—citizens, journalists, activists—entire populations—are less secure and safe.

Renders Populations More Vulnerable to Cyber Security Exploitation Overall

- A society under surveillance is one far more vulnerable to cyber security problems and exploitation. Several recent empirical studies provide evidence on this count. For example, Dencik and Cable (2017), a study based on multiple focus groups among U.K. citizens as well as semi-structured interviews with political activists—documented a phenomenon they called "surveillance realism" wherein a "lack of transparency", "knowledge" and "control over" surveillance and data gathering practices has led to "feelings of widespread resignation" (though not consent) to "status quo" surveillance (764). Mamonov and Koufaris (2016), an experimental study of the impact of surveillance on citizens, similarly found evidence that exposure to news about government surveillance led to "learned helplessness"—exposure to an "uncontrollable aversive stimulus" leads to deficits in motivation to act to address the issue, here being government surveillance.

- This "surveillance realism" and learned helplessness has very real and serious consequences for cyber security. Mamonov and Koufaris (2016), in fact, found participants exposed to news about electronic government surveillance caused the participants to use weaker passwords compared to those exposed only to general government-related news stories (62). The best explanation, the authors surmised, was learned helplessness about the inevitability of state surveillance. These findings were also consistent with van Schaik et al. (2017) who also found, in a study on risk perception and cyber security, that users who felt in control were more likely to utilize cyber security tools like security add-ons and anti-virus software.

- Surveillance may also undercut cyber security in other ways as well, by chilling citizens from seeking out information about state surveillance, including information about how to protect themselves and their data (See Marthews and Tucker, 2014; Penney, 2016).

Makes Citizens More Vulnerable to Disinformation, Propaganda, and Fake News

- A emerging and increasingly complex civil society *and* national security challenge is the prevalence, spread, and consumption of misinformation, rumors, and "fake news", by citizens, particularly in online contexts like social media network sites (Kwon and Rao, 2017; Tufekci, 2017).

- Kwon and Rao (2017)'s study is among the first to empirically examine how the "threat" of internet surveillance impacts the spread of rumor and disinformation among the general public online (308). In two surveys conducted in South Korea, the authors found, counter intuitively, citizen concerns about government surveillance online actually "increased their willingness to engage in cyber-rumor

sharing" (308). The authors hypothesized that state surveillance concerns led citizens to distrust government as an information gatekeeper, rendering them more likely to engage in rumour and misinformation as alternative information sources.

- Another explanation might be found in the previously discussed studies finding surveillance can have a noteworthy chilling effect on citizen's willingness to seek out controversial or privacy concerning information and content online (Marthews and Tucker, 2014; Penney, 2016; Penney, 2017). This means citizens under state surveillance may be chilled from searching about controversial or contentious news stories to determine their truth or veracity, rendering them less able to critically assess rumours or misinformation and thus more likely to share or be duped or exploited. Moreover, studies by Stoycheff (2016) and Penney (2017) suggest surveillance promotes self-censorship and a "spiral of silence" among citizens; people less willing to speak out may also self-censor on controversial rumours or misinformation, thus also contributing to the problem.

Pushes Activists to Adopt Dangerous Cyber Security Practices

- Surveillance, both targeted and mass forms, also can push activists to adopt dangerous cyber security practices. Myers West (2017)'s observational study of the impact surveillance and other threats had on activist communities revealed a tension between practices taken to protect communications from surveillance—like encryption and anonymizing tools—and the need (and importance) of greater visibility and transparency to reach a broader audiences/affect the larger "information environment". Dencik et al. (2017)'s study, which included in-depth interviews with "social justice activists", revealed similar tensions, with Snowden revelations leading more technology savvy activists to adopt stringent measures and tools to protect privacy and anonymity, with other activist communities avoiding basic security measures out of need for transparency that they have "nothing to hide" in terms of their aims and methods.

Undermines Reporting, and thus Public Awareness, on National Security Matters

- There is also evidence that surveillance will make journalism and investigative reporting more difficult, meaning fewer news sources and less quality information for citizens, particularly on national security matters, which are often complex and require confidential government sourcing. Lashmar (2017), in a qualitative study involving interviews with journalists after the Snowden revelations, found all participants believed existence of mass government surveillance would "chill" and deter confidential sources from speaking with journalists. Wahl-Jorgenson et al. (2017) also found reporters struggled with the reality of mass government surveillance, leading them to mostly focus on surveillance of elites and other "legitimating" narratives, rather than more complex stories centered on mass surveillance programs. Similarly, journalists also report self-censorship on certain topics post-Snowden (PEN America, 2013; 2015).

DIRECTIONS FORWARD

- Dutton (2017) recently noted that despite a realization cyber security is no longer the domain of technical experts, there has not been corresponding "strong" programs of research "aimed at understanding the attitudes, values, and behaviour of users with respect to cyber security" (2). Ultimately he calls for more user-focused empirical studies in cyber security drawing on social science research and methods, in particular, "qualitative or quantitative research on end-users..." (9).

- Indeed, if cyber security is to ever shed its national security tilt in favour of civil society or human rights, then its discourse and literature needs to consider more systematically and empirically the impact that cyber security practices have on citizens, end-users, groups, and populations, drawing not just on technical studies, but well designed social scientific investigations. This paper has aimed to do so in relation to state surveillance, but far more cyber security practices deserve scrutiny.

SOURCES

Andrew, N. L. (2016). Reconceptualising Cyber Security: Safeguarding Human Rights in the Era of Cyber Surveillance. *International Journal of Cyber Warfare and Terrorism (IJCWT), 6*(2), 32-40. doi: 10.4018/ijcwt.2016040103

Azmi, R., Tibben, W., & Win, K. T. (2016). Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy.

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. doi: 10.1111/ips.12048

Bayerl, P. S., & Akhgar, B. (2015). Online Surveillance Awareness as Impact on Data Validity for Open-Source Intelligence? In H. Jahankhani, A. Carlile, B. Akhgar, A. Taal, A. G. Hessami & A. Hosseinian-Far (Eds.), *Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security: 10th International Conference, ICGS3 2015, London, UK, September 15-17, 2015. Proceedings* (pp. 15-20). Cham: Springer International Publishing.

Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue, 44*(2), 147-164. doi: 10.1177/0967010613478323

Brantly, A. F. (2014). The Cyber Losers. *Democracy and Security, 10*(2), 132-155. doi: 10.1080/17419166.2014.890520

Carr, M. (2013). Internet freedom, human rights and power. *Australian Journal of International Affairs, 67*(5), 621-637. doi: 10.1080/10357718.2013.817525

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs, 92*(1), 43-62. doi: 10.1111/1468-2346.12504

Cavelty, M. D., & Balzacq, T. (2016). *Routledge handbook of security studies*: Routledge.

Cavelty, M. D., & Van Der Vlugt, R. A. (2015). A Tale of Two Cities: Or How the Wrong Metaphors Lead to Less Security. *Geo. J. Int'l Aff., 16*, 21.

Deibert, R. (2012). Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace. *2012, 14*(2).

Deibert, R. J. (2013). *Black Code: Inside the Battle for Cyberspace*. Toronto: Signal.

Deibert, R. (2015). Cyberspace Under Siege. *Journal of Democracy, 26*(3), 64-78.

Deibert, R. (2016). *Cyber Security*: Routledge.

Deibert, R. (2017). Digital Threats Against Journalists. In S. Khorana & J. Henrichsen (Eds.), *Journalism After Snowden: The Future of the Free Press in the Surveillance State*. New York: Columbia University Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2012). *Access contested: security, identity, and resistance in Asian cyberspace*: MIT Press.

Deibert, R., & Rohozinski, R. (2010). Cyber Wars. *Index on Censorship, 39*(1), 79-90. doi: 10.1177/0306422010362176

Deibert, R. J. (2013). *Black code: Inside the battle for cyberspace*: Signal.

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the snowden leaks. *International Journal of Communication, 11*, 763-781.

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society, 3*(2), 2053951716679678. doi: 10.1177/2053951716679678

Domingo, F. C. (2015). Cyber War Versus Cyber Realities: Cyber Conflict in the International System by Brandon Valeriano and Ryan C. Maness. *Journal of Information Technology & Politics, 12*(4), 399-401. doi: 10.1080/19331681.2015.1101039

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. doi: 10.1111/misr.12023

Dutton, W. (2017). Fostering a cyber security mindset. *Internet Policy Review, 6*(1).

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review, 27*(3), 221-244. doi: 10.1177/0192512106064462

Eriksson, J., & Giacomello, G. (2014). International relations, cybersecurity, and content analysis: a constructivist approach. In *The Global Politics of Science and Technology-Vol. 2* (pp. 205-219). Springer Berlin Heidelberg.

Hardy, S., Crete-Nishihata, M., Kleemola, K., Senft, A., Sonne, B., Wiseman, G., . . . Deibert, R. J. (2014). *Targeted threat index: characterizing and quantifying politically-motivated targeted malware*. Paper presented at the Proceedings of the 23rd USENIX conference on Security Symposium, San Diego, CA.

Khorana, S., & Henrichsen, J. (2017). *Journalism After Snowden: The Future of the Free Press in the Surveillance State*: Columbia University Press.

Kovacs, A., & Hawtin, D. (2013). *Cyber security, cyber surveillance and online human rights.* Paper presented at the Stockholm Internet forum on Internet freedom for global development.

Kwon, K., & Rao, R. (2017). Cyber-rumor sharing under a homeland security threat in the context of government Internet surveillance: The case of South-North Korea conflict. *Government Information Quarterly, 34*(2), 307-316. doi: https://doi.org/10.1016/j.giq.2017.04.002

Lashmar, P. (2017). No More Sources? *Journalism Practice, 11*(6), 665-688. doi: 10.1080/17512786.2016.1179587

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics, 10*(1), 86-103. doi: 10.1080/19331681.2012.759059

Lawson, S. T., Yeo, S. K., Yu, H., & Greene, E. (2016). *The cyber-doom effect: The impact of fear appeals in the US cyber security debate.* Paper presented at the Cyber Conflict (CyCon), 2016 8th International Conference on.

Lyon, D. (1994). The electronic eye: The rise of surveillance society. Minneapolis: University of Minnesota Press.

Lyon, D. (1991). "Bentham's Panopticon: From moral architecture to electronic surveillance," *Queen's Quarterly*, volume 98, number 3, pp. 596–617.

Lyon, D. (2001). Surveillance society: Monitoring everyday life. Buckingham: Open University Press.

Lyon, D. (2006). Theorizing surveillance: The panopticon and beyond. Cullompton, Devon: Willan Publishing.

Lyon, D. (2007). *Surveillance studies: An overview*: Polity.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society, 1*(2), 2053951714541861. doi: 10.1177/2053951714541861

Lyon, D. (2015). Surveillance After Snowden. Cambridge, MA: Polity Press.

Mamonov, S., & Koufaris, M. (2016). The impact of exposure to news about electronic government surveillance on concerns about government intrusion, privacy self-efficacy, and privacy protective behavior. *Journal of Information Privacy and Security, 12*(2), 56-67. doi: 10.1080/15536548.2016.1163026

Marthews, A., & Tucker, C. (2014). Government Surveillance and Internet Search Behavior. *MIT Sloane Working Paper No. 14380*.

Marwick, A. E. (2012). The public domain: Social surveillance in everyday life. *Surveillance & Society, 9*(4), 378.

Michaelsen, M. (2017). Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran. *Surveillance & Society, 15*(3/4), 465.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev., 79*, 119.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*: Stanford University Press.

Nye, J. (2010). Cyber power. *The Future of Power in the 21st Century* Belfer Center for Science and International Affairs.

Nye, J. (2011). Cyberspace wars. *International Herald Tribune, 28*.

PEN America (2013). Chilling Effects: NSA Surveillance Drives US Writers to Self-Censor. *New York: PEN American Center*.

PEN America (2015). Global Chilling: The Impact of Mass Surveillance on International Writers. *New York: PEN American Center*.

Penney, J. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Tech. LJ, 31*, 117.

Penney, J. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review, 6*(2).

Penney, J. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Tech. L.J., 31*, 117-182.

Pew Research Center. (2014a). Global Opposition to U.S. Surveillance and Drones, But Limited Harm to America's Image.

Pew Research Center. (2014b). Social Media and the 'Spiral of Silence'.

Pew Research Center. (2014c). Public Perceptions of Privacy and Security in the Post-Snowden Era.

Pew Research Center. (2015a). Americans' Privacy Strategies Post-Snowden.

Pew Research Center. (2015b). Americans' Attitudes About Privacy, Security and Surveillance.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security, 31*(4), 597-611.

Prakash, B. A. (2015). Graph Mining for Cyber Security. In S. Jajodia, P. Shakarian, V. S. Subrahmanian, V. Swarup & C. Wang (Eds.), *Cyber Warfare: Building the Scientific Foundation* (pp. 287-306). Cham: Springer International Publishing.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*: WW Norton & Company.

Schauer, F. (1978). Fear, Risk, and the First Amendment: Unraveling the 'Chilling Effect' *Boston University Law Review, 58*, 685-732.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*, 477-564.

Solove, D. J. (2007). The First Amendment as Criminal Procedure. *New York University Law Review, 82*, 112.

Stoycheff, E. (2016). Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. *Journalism & Mass Communication Quarterly*. doi: 10.1177/1077699016630255

Taddeo, M. (2015). The Struggle Between Liberties and Authorities in the Information Age. [journal article]. *Science and Engineering Ethics, 21*(5), 1125-1138. doi: 10.1007/s11948-014-9586-0

Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*: Yale University Press.

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*(Supplement C), 547-559. doi: https://doi.org/10.1016/j.chb.2017.05.038

Wahl-Jorgensen, K., Bennett, L. K., & Cable, J. (2017). Surveillance Normalization and Critique. *Digital*

Journalism, 5(3), 386-403. doi: 10.1080/21670811.2016.1250607

Wang, V., & Tucker, J. (2017). Surveillance and identity: conceptual framework and formal models. *Journal of Cybersecurity*.

West, S. M. *Ambivalence in the (Private) Public Sphere: How Global Digital Activists Navigate Risk*.

Wang, V., & Tucker, J. (2017). Surveillance and identity: conceptual framework and formal models. *Journal of Cybersecurity*.