

Interrogating Internet Service Provider Surveillance: Deep Packet Inspection and the Confluence of Privacy Regimes

Context and Research Question

Internet Service Providers (ISPs) are ideally situated to survey data traffic because all traffic to and from the Internet must pass through their networks. Using sophisticated data traffic monitoring technologies, these companies investigate and capture the content of unencrypted digital communications (e.g. MSN messages and e-mail). Despite their role as the digital era's gatekeepers, very little work has been done in the social sciences to examine the relationship between the surveillance technologies that ISPs use to survey data flows and the regional privacy regulations that adjudicate permissible degrees of ISP surveillance. With my seven years of employment in the field of Information Technology (the last several in network operations), and my strong background in conceptions of privacy and their empirical realization from my master's degree in philosophy and current doctoral work in political science, I am unusually well-suited to investigate this relationship. I will bring this background to bear when answering the following interlinked questions in my dissertation: *What are the modes and conditions of ISP surveillance in the privacy regimes of Canada, the US, and European Union (EU)? Do common policy structures across these privacy regimes engender common realizations of ISP surveillance techniques and practices, or do regional privacy regulations pertaining to DPI technologies preclude any such harmonization?*

Thesis - Literature

Given ISPs' role in governing data networks, it is crucial to interrogate the methods and technologies they utilize to survey traffic flowing through their networks. Data sent on the Internet is separated into discrete packets that are shuttled to the message's recipients and then reassembled at their destination. ISPs presently use *Deep Packet Inspection* (DPI) technologies to investigate each packet that enters and leaves their networks. These technologies effectively let ISPs open sealed letters (the packets), read their contents (the packets' payload/message), reseal the letters, and then pass them to the recipients, so long as the contents are deemed 'acceptable' by ISPs' evaluation heuristics.

ISPs operate in various privacy regimes. Each regime (e.g. Canada, America, EU) has a unique legal and technological discourse, and a particular conception of the complexity, dynamic, and diversity of processing personal data (Bennett and Raab 2006). Accompanying these regimes are divergent understandings of permissible and impermissible degrees of surveillance, and Diebert et al. (2008) have shown that state-mandates impact ISPs' content filtering practices. Diebert et al. (2008) do not, however, address the expansive surveillance possibilities of DPI, instead limiting their work to (relatively) archaic methods of monitoring and blocking Internet content. Moreover, while some scholars address facets of privacy and surveillance regulation pertaining to digital networks (Haggerty 2006, Lace 2005, Lyon 2007, Solove 2004, 2008), they focus on theoretical abstractions and digital environments, such social networking sites, without examining the surveillance capabilities of ISPs themselves.

Much of the empirical work pertaining to ISPs and data surveillance has surveyed people's *perceptions* of surveillance and privacy. These surveys have concluded that the people do not want their online activities tracked and conversations monitored (Pew Internet and American Life Project 2000), do not trust businesses to handle their personal information (Harris Interactive 2002), and that respondents generally perceive their privacy as 'very important' (EPIC 2005). *These indicate what people think about surreptitious surveillance without investigating how ISPs inspect individuals' data traffic.* Recent articles interrogating DPI technologies and data traffic (Anderson 2008, Clayton et al. 2008, Rossenhovel 2008, Topolski 2008) have focused on overviews of DPI technologies, neglecting the particular privacy regimes these technologies function in. While some work exists that concerns the abstract regulation of digital system (Lessig 2004, Galloway and Thacker 2008, Ohm 2008) it does not consider the specific regulatory situations in Canada, America, or the EU, nor does it reflect on the roles of various policy agents and their capacity to impact privacy and surveillance regulations in these privacy regimes.

By examining policy instruments, transnational actors, conceptual frameworks that motivate international privacy agreements, and legal decisions concerning privacy rights in Canada, the US, and the EU, commonalities and dissonant approaches to surveillance practices can be identified in privacy

regimes. Sabatier's (1988) advocacy coalition approach and Kingdon's (2003) work on agendas can mutually assist in identifying how and why particular policies have been developed and whether they are motivated towards a common cross-regime understanding of permissible levels of ISP surveillance.

Thesis - Methodology

Drawing on my years of experience in Information Technology, I will initially focus on the technical capabilities of DPI technologies used by ISPs. Drawing on corporate, academic, and legal technical analysis of national, transnational, and global stakeholders in DPI, I will expose the uses and technical capabilities of these technologies. With an understanding of the technologies, I will extend my investigation to relevant Canadian, American, and EU privacy codes, regulations, and fair information practices. This information will be synthesized with privacy theory and surveillance studies literature, as well as with international agreements that influence acceptable national surveillance and data handling practices. The integration of empirical, technical, theoretical, and legal literature will provide me with a firm understanding of the Canadian, American, and EU privacy regimes and how they interrelate with privacy and surveillance implications of DPI. On this foundation, I will break new ground in the social science by investigating whether these regimes pressure ISPs to adopt common surveillance practices, and can consequently be seen as substantively realizing common ISP surveillance practices across privacy regimes, or if the regimes instead provoke ISPs to adopt dissonant surveillance practices.

Thesis - Preparation and Coursework

I began my doctoral studies in the Political Science Department at the University of Victoria this September, and will complete my dissertation by 2012. Recognizing this topic's boldness, I am working under the supervision of Dr. Colin Bennett, a world expert in the governance of privacy. To prepare for my dissertation, I am taking graduate classes in comparative policy, international relations, multi-disciplinary theory, and surveillance studies. These will assist in refining my methodological approaches and sensitize my work to the global, transnational, national, and provincial/state challenges concerning the governance of privacy. In addition, I am attending the 10th Annual Privacy and Security Conference in February 2009 to discuss my research with government officials, technology experts, and academics. Next summer, I am attending the Surveillance Studies Summer Seminar, where leading international faculty in surveillance studies will lead seminars on the topics of surveillance and privacy.

Relevant Experience and Thesis Dissemination

I am a research assistant for the New Transparency Project (NewT), which in part aims to render transparent the flows of digital information as they pertain to surveillance. As part of my duties, I am preparing working papers on surveillance technologies, assisting faculty associated with this sub-branch of the project, and will be the major research assistant for the 2011 workshop on digitally mediated surveillance. Organizing a multidisciplinary graduate conference in May 2008 has provided me with experience that will be useful in assisting with this workshop. NewT's resources offer me the opportunity to disseminate my research at annual workshops, through edited books, and confirmed special edited journals. Additionally, Dr. Arthur Kroker has invited me to co-author, and present, a paper with Dr. Bennett in 2009 on the topic of privacy and citizenship implications of ISP surveillance. Beyond these academic disseminations, I will continue providing research findings to government bodies investigating issues of digitally mediated surveillance, as well as public legal groups, and members of the media.

Over the course of the fellowship, I will pursue these lines of dissemination. In addition, I will establish an interactive website with the assistance of a (tentatively) contracted web development firm. This website will initially let Canadians identify how their ISP is using DPI technologies, alert them to its implications, and suggested ways of protesting the surveillance. In subsequent years, information on American and EU ISPs will be added. In addition, I will continue to update my personal website, where I share my research through a collaborative wiki, as well as through blog posts concerning emerging technologies' privacy and surveillance implications. *My dissertation, accompanied with public outreach, will contribute to contemporary surveillance and privacy literature, and public awareness, by interrogating ISP surveillance practices and their relationship to privacy regimes to uncover commonalities and dissonances of ISP surveillance practices across privacy regimes.*

Works Cited

- Anderson, Nate (2008). "Throttle 5 million P2P users with \$800K DPI monster," *ArsTechnica*.
Published May 12, 2008, at <http://arstechnica.com/news.ars/post/20080512-throttle-5m-p2p-users-in-real-time-with-800000-dpi-monster.html>
- Bennett, Colin J and Charles Raab (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, Mass.: The MIT Press.
- Clayton, Richard, et al. (2006). "Ignoring the Great Firewall of China," from *6th Workshop on Privacy Enhancing Technologies*, at <http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf>
- Deibert, Ronald et al. (eds.) (2008). *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, Mass.: The MIT Press.
- Electronic Privacy Information Center (EPIC) (2005). *Public Opinion on Privacy* at <http://epic.org/privacy/survey/>
- Galloway, Alexander R., Eugene Thacker (2008). *The Exploit: A Theory of Networks*. Minneapolis: University of Minneapolis Press.
- Goldsmith, Jack and Tim Wu (2006). *Who Controls the Internet? Illusions of a Borderless World*. Toronto: Oxford University Press.
- Haggerty, Kevin D. and Richard V. Ericson (eds.) (2006). *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.
- Harris Interactive (2002). *Privacy on and off the Internet: What consumers want*. Hackensack, NJ.
- Kingdon, John W. (2003). *Agendas, Alternatives, and Public Policies (Second Edition)*. Toronto: Addison-Wesley Educational Publishers Inc.
- Lace, Susanne (ed.) (2005). *The Glass Consumer: Life in a surveillance society*. Bristol: National Consumer Council.
- Lyon, David (2007). *Surveillance Studies: An Overview*. Cambridge, UK: Polity.
- Ohm, Paul (2008). "The Rise and Fall of Invasive ISP Surveillance," *SSRN eLibrary*, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261344
- Pew Internet and American Life Project (2000). *Trust and Online Privacy: Why Americans want to rewrite the rules*. Published August 20, 2000.
- Rossenovel, Carsten (2008). "Peer-to-Peer Filters: Ready for Internet Prime Time?" *Internet Evolution*, at http://www.internetevolution.com/document.asp?doc_id=148803&page_number=1
- Sabatier, Paul A. (1988) "An advocacy coalition framework of policy change and the role of policy-oriented learning," *Policy Studies*, vol. 21, pp. 129-168.
- Solove, Daniel J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.
- Solove, Daniel J. (2008). *Understanding Privacy*. Cambridge, Mass.: Harvard University Press.
- Topolski, Robert M. (2008). "NebuAd and Partner ISPs: Wiretapping, Forgery, and Browser Hijacking" *Free Press and Public Knowledge*. Published June 12, 2008.

Other Key Texts

- Allot Communications Ltd. (2007). *Digging Deeper Into Deep Packet Inspection*, at http://www.getadvanced.net/learning/whitepapers/networkmanagement/Deep%20Packet%20Inspection_White_Paper.pdf
- Anderson, Nate (2007). "Deep packet inspection meets 'Net neutrality, CALEA,'" *ArsTechnica*.
Published June 25, 2007, at <http://arstechnica.com/articles/culture/Deep-packet-inspection-meets-net-neutrality.ars>
- Bennett, Colin (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca: Cornell University Press.
- Bennett, Colin (1997). "Convergence Revisted: Toward a Global Policy for the Protection of Personal Data," in *Technology and Privacy: The New Landscape*, Phillip E. Agre and Marc Rotenberg (eds). Cambridge, Mass.: The MIT Press. pp. 99-123.
- Bennett, Colin (2001). "Cookies, Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web," *Ethics and Information Technology*, vol. 3, pp. 197-210.
- Bennett, Colin, and Rebecca Grant (1999). *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: University of Toronto Press.

- Bond, Jonathan C. (2008). "Defining Disclosure in a Digital Age: Updating the Privacy Act for the Twenty-First Century," *The George Washington Law Review*, vol. 76(5), pp. 1233-1258.
- Clayton, Richard (2008). "The Phorm 'Webwise' System," *Light Blue Touchpaper: Security Research Computer Laboratory, University of Cambridge (Blog)* at <http://www.cl.cam.ac.uk/~rnc1/080404phorm.pdf>
- Dutrisac, James George (2007). *Counter-Surveillance in an Algorithmic World*. Unpublished master's thesis, Queens University, CA.
- European Union (1995). *Directive 95/46/EC of the European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Brussels, OJ no. L281 (24 October 1995).
- Howlett, Michael, M. Ramesh (2003). *Studying Public Policy: Policy Cycles and Policy Subsystems (Second Edition)*. Toronto: Oxford University Press.
- Industry Canada (1998). "The Protection of Personal Information: Building Canada's Information Economy and Society," *Task Force on Electronic Commerce, Industry Canada, Justice Canada*, at <http://www.ifla.org/documents/infopol/canada/privacy.pdf>
- Lyon, David (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.
- OECD (1985). *Declaration on Transborder Data Flows*. OECD: Paris, at http://www.oecd.org/document/25/0,3343,en_2649_34255_1888153_1_1_1_1.00.html
- OECD (1992). *Guidelines for the Security of Information Systems*. OECD: Paris, at <http://www.oecd.org/dataoecd/16/22/15582260.pdf>
- OECD (1997). *Cryptography Policy: The Guidelines and the Issues*. OECD: Paris, at http://www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1.00.html
- Raab, Charles and Colin Bennett (1996). "Taking the Measure of Privacy: Can Data Protection be Evaluated?," *International Review of Administrative Sciences*, vol. 61, pp. 535-556.
- Ponemon Institute and the Information and Privacy Commissioner/Ontario (2004). *Cross-National Study of Canadian and US Corporate Privacy Practices*, at <http://www.ipc.on.ca/images/Resources/cross.pdf>
- Solove, Daniel J. and Marc Rotenburg, Paul M. Schwartz (2006). *Privacy, Information, and Technology*. New York: Aspen Publishers Inc.
- Schoeman, Ferdinand David. (ed.) (1984). *Philosophical Dimensions of Privacy: An Anthropology*. New York: Cambridge University Press.
- Zhang, Jian, Phillip Porras, Johannes Ullrich (2008). "Highly Predictive Blacklisting," from USENIX Security '08, at http://www.usenix.org/events/sec/tech/full_papers/zhang/zhang_html/index.html