Is Your ISP Snooping on You?

Christopher Parsons

In Canada, it is illegal for Canada Post to open our personal mail. While we likely agree that opening a sealed envelope is wrong, what if postal authorities were 'just' reading parts of every postcard that was being mailed to and from every person in Canada? Moreover, what if there was the possibility for Canada Post to add advertising messages on the postcards based on what was written to your friend; what if the color of ink used to write the postcard affected delivery speeds; what if Canada Post could track almost every message that you and your friends transmitted to one another?

Similar possibilities for surveillance, inspection, delivery delays, and advertising form a cornerstone of the privacy-related concerns in contemporary Canadian telecommunications policy.

Deeply inspecting packets

When we send messages to one another online, when we browse web pages and send e-mail, our communications are typically *unencrypted*, that is, they are in a form that can be easily read. Unencrypted communications are the digital equivalent of postcards that are sent along Internet Service Providers' (ISP) networks, such as those belonging to Bell and Rogers. Various federal government agencies are examining how ISPs are using a networking technology, popularly referred to as 'deep packet inspection' (DPI), to inspect Canadians' encrypted and unencrypted data transmissions.

DPI equipment has the ability to read the addressing information of digital communications that flow through ISPs' networks as well as the content of the communications. Together, the addressing information and content compose packets of information that computer applications send to and receive from the internet. Both the address of the packet and its contents can be analyzed using DPI technologies to deliver digital communication to its destination while simultaneously analyzing key facets of its content. This content analysis can identify the application that generated the packet – whether it originated from a file sharing application like BitTorrent or Kazaa, an email client like Outlook, or a web browser like Firefox or Internet Explorer. In some cases it can identify the file that is likely being transmitted -- such as a copy of Madonna's *Like a Virgin*, a downloaded copy of James Cameron's *Avatar*, or a .pdf version of Jane Austen's *Pride and Prejudice*. Depending on how the ISPs have configured their DPI equipment, these content analyses are accurate to varying degrees and can analyze both encrypted and non-encrypted data transmissions.[1]

Given Canadians' tendency to embrace digital communications, there is a very real privacy concern that arises when telecommunications carriers install equipment that could be used for covert mass surveillance and modification of our communications. It is particularly concerning that this technology can be used to apply rule sets, which are the embedded technological regulations that DPI appliances apply to data traffic, to particular kinds of communications. There is an extensive range of uses for these rule sets; for instance, the speed of peer-to-peer (P2P) traffic, such as that which passes through BitTorrent and Kazaa, can be decreased or stopped altogether, and Voice over Internet Protocol (VoIP) providers, such as Skype, can have their communications quality degraded in favor of a VoIP solution supported or promoted by the ISP. One could experience the static and echoes of cell phones circa 1990 when using Skype, but crisp communications using the ISP's VoIP offerings. Further, using this technology, advertisements might be injected into web sites on the basis of what the ISP's DPI equipment, in tandem with marketing databases, thinks the user is interested in.

To clarify this, we might return to the packets-as-postcards analogy. Canada Post can't survey the ink color being used in creating your messages (the equivalent of the application generating the packet), delay particular postcards based on where they are purchased (which corresponds to slowing VoIP offered by competitors), or inject particular ads onto postcards based on their content. Canada's DPI-enabled ISPs, however, could theoretically configure their devices to survey applications, delay particular packets, and inject ads. These ISPs have the technical capacity to do what Canada Post cannot.

These are not academic or hypothetical worries, but rather pressing issues in today's global telecommunications market. Many Canadian ISPs already use rule sets to delay P2P traffic based on payload analysis. A summary of these traffic management practices is posted at christopher-parsons.com.[2] The U.S. Federal Communications Commission (FCC) has ruled that American ISPs cannot block third-party VoIP calls.[3] Companies in the United States and United Kingdom continue to work towards bringing ad-injections to their respective marketplaces, with one of the U.S. competitors (which is now defunct) having cast an eye towards Canada.[4] In light of DPI's potential to modify traffic flows, impinge consumer choice, and forcibly modify the user's browsing experience, Canada's ISPs were recently brought before the Canadian Radio-Telecommunications Commission (CRTC) over their use of DPI equipment for internet traffic management practices[5] and had complaints filed against them with the Office of the Privacy Commissioner (OPC) of Canada.[6]

In response to CRTC and OPC investigations into DPI last year, Canada's largest ISPs presented their arguments for integrating DPI technologies into their networks. Generally, the DPI-enabled ISPs asserted that the technology is meant to mediate internet congestion – the equivalent of too many digital postcards trying to go through the ISPs' delivery networks all at once – and guarantee a high quality of service to their customers while simultaneously improving their customer subscription processes. They argue that particular types of applications, such as those used for P2P file sharing, consume disproportionate amounts of bandwidth, and that such excessive usage negatively impacts the experiences of other customers. Since many applications that transmit and receive data are sneaky – they obfuscate addressing information to confuse ISPs about the content actually carried in the packets – ISPs argue that they must burrow into a packets' content to determine its true application-of-origin. When investigating the content, it is possible to perform sophisticated computational analyses and determine what is sending the data. Such analyses and determinations are possible even if the application has encrypted its content (in effect, shifted from transmitting postcards to sealed envelopes). Algorithmic investigation will often reveal what is generating the data stream (though not its content) and then apply rule sets. Thanks to using DPI in their networks, say ISPs, customers are given an equal experience of the Internet: you won't suffer a degradation of service when the person next door uses a bandwidth-intensive application.

The catch, of course, is that, in performing these computational analyses to improve the customer experience, ISPs are examining private elements of the content that is being transmitted across their networks. This doesn't mean they are reading your e-mail, but it does mean that ISPs' networking equipment is digging into the depths of your communications, finding elements that are useful for traffic management purposes, and then applying their rule sets. This, I suggest, is a ubiquitous form of data surveillance that threatens to have serious impacts on Canadians' expressive privacy.

One way of looking at privacy-related issues is through the impact of persistent surveillance practices on the perceived freedom to speak and associate with others, which is sometimes referred to as 'expressive privacy'. In the case of DPI analyses of electronic data transfers, Canadians' expressive privacy is potentially infringed as a result of persistent communicative surveillance. Judith Wagner DeCew, an American privacy and legal scholar, argues that the "surveillance of normal, everyday activities can lead one to be distracted and feel inhibited."[7] This is corroborated by Professor Julie Cohen when she warns that "[p]ervasive monitoring of every move or false start will, at the margin, incline choices toward the bland and mainstream." Persistent ISP-level data surveillance thus "threatens to chill the expression of eclectic individuality, but also, gradually, to dampen the force of our aspiration to it."[8] Psychoanalysts such as Donald Winnicott[9] and R.D. Laing,[10] and surveillance and privacy scholars such as Daniel Solove[11] and David Lyon,[12] similarly maintain that persistent surveillance can lead to the chilling of speech and a degraded willingness to engage in free expression. In short, lawyers, sociologists, academics, and psychoanalysts alike concur that the perception of widespread monitoring of personal, private, communications transmissions can be debilitating and should register as a kind of privacy infringement.

Government responses so far

In their recent findings, the CRTC and OPC both addressed some potential privacy worries surrounding DPI.[13] In the CRTC's case, it was recognized that the technology is useful for network management and subscriber billing, and that it could be potentially be used for advertising and developing detailed awareness of subscribers' Internet habits. In light of these powers, they directed ISPs "not to use for other purposes personal information collected for the purposes of traffic management and not to disclose such information." Further, while ISPs are permitted to continue monitoring popular applications that subscribers use and record this information for network management purposes, all such information should be aggregated to afford subscriber anonymity.

The OPC was tasked with investigating whether or not Bell Sympatico, in particular, used DPI technology to "collect and use personal information from its customers without consent," with the complainant alleging that this collection exceeds the minimal amount of personal information Bell requires to provide internet service to its customers. The OPC found that Bell needed to update the information on their web page to notify consumers of their use of the technology, as well as of their limited and temporary collection of personal information resulting from the association of subscriber numbers and the internet protocol (IP) address assigned to their users.

Thus, while the CRTC and OPC both have begun to etch out what are permissible applications of the technology and how customers should be notified of its use, we can still learn from some of the responses to DPI in the European Union and United States to extend Canada's protections.

In the face of the potential privacy-invasive uses of DPI technologies, the U.S. House of Representatives' Telecommunications and Internet Subcommittee held hearings into the relationship between DPI and marketing. The committee was deeply critical of DPI-related advertising practices.[14] Partially in light of DPI and similar surveillance technologies, House member Rick Boucher is preparing a bill meant to prevent American ISPs (and other telecommunications companies, like Google and Yahoo!) from using surveillance equipment like DPI to track customers' online activities for advertising purposes.[15] Also, the FCC is looking to establish network neutrality principles but, after suffering a devastating legal setback,[16] must first succeed in classifying broadband providers as providing common carrier services.[17] Principles established following this reclassification of broadband services could limit ISPs' legal ability to unnecessarily inspect and disrupt data transmissions without cause.

In Europe, the European Commission is threatening to bring the U.K. government to court over their willingness to let ISPs use DPI to survey and modify data content in the very near future. The Commission's argument is premised on two points: first, that ensuring "digital privacy is key for building trust in the internet" and second, that British ISPs' use of DPI is non-compliant with provisions of the EU's *Directive on Privacy and Electronic Communications.* It is expected that the only way for the U.K. to escape the Commission's wrath is to change their laws to make future uses of DPI for advertising purposes illegal.[18]

The CRTC has begun establishing provisions echoing those of the FCC and EU in their rulings on using DPI for traffic management by limiting the permissible uses of the technology. Further, the OPC has pushed the ball forward in both demanding greater openness of what information DPI equipment collects in Canada and in supporting efforts to increase public awareness of the technology.[19] Neither the CRTC's nor the OPC's responses, however, are as strong as the legislative limitations on privacy-invasive uses of the technology being pursued in the U.S. and that are already codified in the EU.

Rather than be satisfied with the present state of affairs, Canadians should demand continuing progressive legislative efforts to entrench the CRTC's decisions and mediate other potentially privacy-invasive uses of DPI technologies. Policy learning from other Western powers is required given how rapidly the technological landscape shifts. The Canadian government should be applauded if they import privacy-protective measures that further limit privacy infringing uses of technology which threaten Canadians' expressive privacy and inhibit their constitutional rights to free speech and association.

Additional Resources:

Organizational Websites:

OPC website on DPI: http://dpi.priv.gc.ca/
Deep Packet Inspection Canada: http://www.deeppacketinspection.ca
EPIC on DPI: http://epic.org/privacy/dpi/default.html
[d]packet: https://www.dpacket.org/

Papers:

Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials: http://www.surveillanceproject.org/files/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf
NebuAd and Partner ISPs: Wiretapping, Forgery, and Browser Hijacking: http://www.freepress.net/node/41737
Digging Deeper Into Deep Packet Inspection: http://www.getadvanced.com/learning/whitepapers/networkmanagement/Deep%20Packet%20Inspection_White_Paper.pdf
Deep packet inspection meets 'Net neutrality', CALEA: http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars
Modifying the Data Stream: Deep Packet Inspection and Internet Censorship: http://giganet.igloogroups.org/publiclibr/hyderabad/3rdgiganet%7E2/wagnerpdf%7E2
Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection: http://userpage.fu-berlin.de/%7Ebendrath/ISA09_Paper_Ralf%20Bendrath_DPI.pdf
Disclosure, Deception, and Deep-Packet Inspection: The Role of the Federal Trade Commission Act's Deceptive Conduct Prohibitions in the Network Neutrality Debate: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1516705
Deep Packet Inspection: The end of the internet as we know it? http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf
This is the way the Internet ends: not with a bang, but DPI: http://arstechnica.com/tech-policy/news/2009/03/does-deep-packet-inspection-mean.ars

REFERENCES

[1] In a recent study performed by Internet Evolution, we find that DPI equipment can accurately identify applications that generate encrypted traffic (though this identification doesn't extend to the content the application is transmitting). It is relatively easy to

update equipment to account for new applications' data traffic. http://www.internetevolution.com/document.asp?doc_id=178633

[2] I have composed, and made publicly available, a relatively recent summary based on regulatory documents of major Canadian ISPs using DPI technology. http://www.christopher-parsons.com/blog/technology/comment-canadian-isps-and-internet-traffic-management/

[3] Federal Communications Commission. (2005). *Madison River Communications Order* FCC 4295. Last accessed January 2, 2010. Accessible at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf

[4] Noted in CIPPIC's 2008 filing to the OPC, which is accessible at: http://www.cippic.ca/uploads/CIPPIC_RequestforIndGuidelines-DPI-BehTarg_25July08.pdf

[5] Record of the CRTC proceedings: http://www.crtc.gc.ca/PartVII/eng/2008/8646/c12_200815400.htm

[6] For documents pertaining to this complaint: http://www.cippic.ca/index.php?mact=News,cntnt01,detail,0&cntnt01articleid=419&cntnt01returnid=15

[7] Wagner DeCew, Judith. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithica, New York: Cornell University Press.

[8] Cohen, Julie. (2007). "Examined Lives: Informational Privacy and the Subject as Object," 52 *Stanford Law Review* 1373.

[9] Winnicott, Donald. (1965). *The Maturational Processes and the Facilitating Environment: Studies in the Theory of Emotional Development*. New York: International Universities Press.

[10] Laing, R.D. (1967). *The Politics of Experience*. New York: Ballantine Books.

[11] Solove, Daniel J. (2008). *Understanding Privacy*. Cambridge, Mass.: Harvard University Press. 2009.

[12] Lyon, David. (2008). *Surveillance Studies: An Overview*. Malden, MA: Polity Press.

[13] CRTC decision: http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm OPC's Report of Findings: http://www.cippic.ca/uploads/File/OPC-Bell-DPI.pdf

[14] Timmer, John. (2008). Markey to NebuAd: "When did you stop beating the consumer?" *Ars Technica*. Published July 17, 2008. Last accessed January 3, 2009. Available at: http://arstechnica.com/business/news/2008/07/markey-to-nebuad-when-did-you-stop-beating-the-consumer.ars

[15] Kaye, Kate. (2009). House Members Plan to Draft New Online Privacy Bill," *ClickZ*. Published April 14, 2009. Last accessed January 3, 2009. Available at: http://www.clickz.com/3633511 The draft version of the discussion draft of Boucher's proposed bill is available at: http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf

[16] Wyatt, Edward. (2010). "U.S. Court Curbs F.C.C. Authority on Web Traffic," *The New York Times*. Published April 6, 2010. Last accessed August 3, 2010. Available at: http://www.nytimes.com/2010/04/07/technology/07net.html

[17] Julius Genachowski, Chairman of the FCC, outlined his proposed redefinition of broadband service providers as common carriers in a speech entitled "The Third Way: A Narrowly Tailored Broadband Framework." The speech is available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-297944A1.pdf

[18] Williams, Chris. (2009). “UK gets final warning over Phorm trials,” *The Register*. Published October 29, 2009. Last accessed January 3, 2009. Available at: http://www.theregister.co.uk/2009/10/29/eu_phorm/

[19] To date, the OPC has launched their own “What is Deep Packet Inspection” website (http://dpi.priv.gc.ca/index.php/what-is-deep-packet-inspection/) and supported the creation of Deep Packet Inspection Canada (http://www.deeppacketinspection.ca/).