Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

25 July 2008

BY COURIER AND EMAIL

Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

Dear Commissioner Stoddart:

Re: Request for an investigation and development of guidelines re: ISP use of Deep Packet Inspection technology for behavioural targeted marketing purposes

1. This is a request that your office investigate the current and potential use of deep packet inspection (DPI) technology by internet service providers (ISPs) for the purpose of behavioural targeted advertising, with a view to developing industry guidelines consistent with legal requirements under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

2. This request is separate from and in addition to our complaints made under s.11 of PIPEDA against Bell Canada (complaint #6100-02744), and by way of separate letters today, against Rogers Communications Inc., Shaw Communications Inc. and Eastlink. Those complaints focus on the use by those ISPs of DPI for the purpose of traffic management.

3. Given the speed with which DPI technology is being deployed, the variety of purposes for which it is being marketed, and the obvious privacy concerns that it raises, we submit that the time is ripe for your office to investigate these matters on an industry-wide basis and to develop guidelines for PIPEDA-compliant use of DPI by ISPs, in the context of behavioural targeting as well as traffic-shaping.

4. Our research suggests that some Canadian ISPs may be engaging or preparing to engage in the collection of subscriber data via DPI in order to target advertising at individual users. We question whether such collection and use of personal data is necessary for advertising

Université d'Ottawa • University of Ottawa
Faculté de droit • Faculty of Law
57 Louis-Pasteur, Ottawa (Ontario) K1N 6N5 Canada
(613) 562-5800 (2553) • (613) 562-5417 (Téléc/Fax)
www.cippic.ca • cippic@uottawa.ca

purposes, whether subscribers have consented to such uses of their personal data, and whether the practice is in any event appropriate in the circumstances.

5. In particular, we submit that the practice of behavioural profiling and/or targeting by ISPs raises a number of concerns under PIPEDA:[1] specifically, that ISPs engaging in this practice:

   a. Fail to obtain informed consent from affected individuals to the collection and use of their personal information gleaned from traffic data for purposes of targeted marketing; (Principle 4.3);
   b. Fail to limit the collection of personal information to that which is necessary for the ISP's stated purposes (Principle 4.4); and
   c. Fail to make readily available to the public specific information about their policies and practices insofar as such practices involve the collection and analysis of personal information for targeted marketing purposes (Principle 4.8).

6. Moreover, we question whether the collection and use of user traffic data by ISPs for the purpose of behavioural targeted advertising by themselves or third parties constitutes a purpose "that a reasonable person would consider appropriate in the circumstances", as required under s.5(3) of PIPEDA.

I FACTS

A. Behavioural Targeting and Deep Packet Inspection

7. "Behavioural targeting" is the marketing practice of targeting advertisements to consumers on the basis of observed or known characteristics of the consumer. In the internet context, marketers may observe the browsing habits of a particular consumer, classify the consumer within categories on the basis of those observations, and serve ads targeted to members of that classification.[2] For example, a newspaper website might observe a consumer browsing webpages that include articles on sports, technology, and pop music, and accordingly classify the consumer in a category that likely includes young males. The website would then serve ads appropriate to that demographic.

---

[1] These same concerns form the basis of our specific complaints filed against Rogers, Shaw, and Eastlink.
[2] Specific Media: Behavioral Targeting, "What is Behavioral Targeting?", online: <http://www.behavioraltargeting.com/what-is-behavioral-targeting.html>.

8. Service providers such as Phorm, Inc.,[3] NebuAd, Inc.[4] and Front Porch, Inc.[5] are now offering services to ISPs that are capable of supporting behavioural targeting marketing on the basis of deep packet inspection of the entirety of the ISP consumers' internet traffic. Such traffic potentially includes consumers' browsing habits, media streaming consumption, email communications, instant messaging and IRC chatting, and communications such as Skype messaging that employ peer-to-peer protocols. Unlike website-based tracking, that can no longer collect information from a user who navigates away from the webpage, ISPs can collect data about user activity across all websites visited and all uses of the web. This capability raises privacy concerns an order of magnitude beyond any prior form of behavioural targeting in the marketplace.[6]

9. ISPs outside Canada, such as BT[7] in the United Kingdom and Charter Communications[8] in the United States, have participated or have considered participating in behavioural targeting through the use of DPI.

10. Typically, an ISP will partner with a company – such as NebuAd or Phorm – that specializes in DPI-based behavioural targeting. The behavioural targeting companies install their hardware on the ISP network, gaining access to users' web traffic information including all the sites visited by users, web search terms, page views, page and ad clicks, duration of website visit, browser information as well as potentially instant messaging and other web-oriented programs.

11. Behavioural targeting companies collect, analyze, and store information in user profiles. Every user is assigned a randomized hash number. (In the case of NebuAd information collected is assigned a second hash number and used to develop interest categories). Based on the web traffic data collected about him/her, a user is categorized into potential

---

[3] Phorm, online: <http://www.phorm.com/>.
[4] NebuAd, online: <http://www.nebuad.com/>.
[5] Front Porch, online: <http://www.frontporch.com/html/index.html>.
[6] Peter Whoriskey, "Every Click you Make: Internet Providers Quietly Test Expanded Tracking of Web Use to Target Advertising," *Washingtonpost.com*, April 4, 2008, online: <http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html>; Saul Hansell, "The Mother of All Privacy Battles", *New York Times: Bits Blog*, (March 25, 2008), online: <http://bits.blogs.nytimes.com/2008/03/25/the-mother-of-all-privacy-battles/>.
[7] Eric Pfanner, "3 Internet Providers in Deal for Tailored Ads" *New York Times* (February 18, 2008), <http://www.nytimes.com/2008/02/18/technology/18target.html>.
[8] Saul Hansell, "Charter Will Monitor Customers' Web Surfing to Target Ads" *New York Times* (May 14, 2008), <http://bits.blogs.nytimes.com/2008/05/14/charter-will-monitor-customers-web-surfing-to-target-ads/>.

consumer types.[9] By entering into partnerships with advertising firms and web publishers, the companies broker the sale of advertising that is aimed at individual visitors according to their assembled profiles. When a user visits an affiliated web page, they are presented with advertising aimed at them.[10]

12. Companies typically provide an opt-out mechanism to users. These mechanisms vary from company to company. It is unclear precisely how each company's mechanism works. In particular, it is unclear whether users who opt-out are merely not served targeted advertising and still have their information collected or whether the companies somehow refrain from tracking that user altogether.

13. In one opt-out mechanism, data collection companies to place a cookie on the computers of those users who have opted out. A leaked internal Phorm evaluation report the company described some of the shortcomings of the model:

> "Users opt-out by navigating to a web-site and downloading an opt-out cookie. **Should they subsequently clear their cached data, they will be silently opted back-in**. A mechanism may be required to inform a user at this point that they have opted back-in, though **a technical solution for this is not obvious**.
> The current opt-out method does not actually avoid the system entirely. A user who has opted-out will still have their web pages tagged and partial JavaScript execution will occur on every page browsed, although no data collection of any kind will occur"[11]

14. The *Wired* blog *Threat Level* discussed some more of the technical questions surrounding the efficacy of behavioural targeting opt-out mechanisms, with a specific focus on those of NebuAd. The blog noted that "…because of the way web cookies work, [the opt-out] cookie can only be read by *NebuAd.com*, or a website that includes content served from that domain. There's no technical way for NebuAd's sniffer to access the cookie and know not to log and analyze an opted-out user's web usage."[12] The post goes on to note:

> "Indeed, it is possible that the cookie system works to prevent opted-out users from receiving the third-party ads, and it could stop NebuAd from sharing a user's profile with third-party ad networks -- assuming those networks include a NebuAd image file, or some other embedded code, in the ads they

---

[9] Peter Whoriskey, "Every Click you Make: Internet Providers Quietly Test Expanded Tracking of Web Use to Target Advertising," *Washingtonpost.com*, April 4, 2008, online: <http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html>.
[10] NebuAd, "Advertisers" online: NebuAd <http://www.nebuad.com/advertisers/advertisers.php>; NebuAd, "Publishers" online: <http://www.nebuad.com/publishers/publishers.php>; Phorm, "Open Internet Exchange" online: <http://www.phorm.com/oix/>.
[11] Wikileaks, "British Telecom Phorm PageSense External Validation Report", online: <http://www.wikileaks.org/wiki/British_Telecom_Phorm_Page_Sense_External_Validation_report> at 18 [emphasis added].
[12] Ryan Singel, "Can Charter Broadband Customers Really Opt-Out of Spying? Maybe Not", *Wired: Threat Level* (May 16, 2008), online: <http://blog.wired.com/27bstroke6/2008/05/theres-no-optin.html#previouspost>.

> serve on the web. But NebuAd's claim that you can opt-out of the surveillance itself remains unexplained."[13]

15. Despite information provided by NebuAd-affiliated ISPs to the public indicating that their opt-out mechanisms make use of cookies, NebuAd claims not to utilize a cookie-based identification. Instead the company claims to rely on a patent-pending identification algorithm that looks at a user's browser information and IP address. Threat Level notes, "If the system actually relies on IP addresses as part of the identification number, then the opt-out could actually expire every time the ISP assigns a new dynamic IP address to the customer."

B. Behavioural Targeting and Canadian ISPs

16. There is reason to believe that this practice is coming to Canada, if it is not already here. According to a *Financial Post* article published April 14, 2008 and entitled "New hardware raises bar on surveillance on Internet", NebuAd, a company that behaviourally targets approximately 10% of broadband users in the U.S., is looking to move into the Canadian market. The article states that NebuAd CEO Robert Dykes confirmed that "his company is testing its hardware with a number of undisclosed Canadian Internet service providers and has launched a sales team in Canada to locate more business."[14]

17. The arrival of behavioural targeting in other jurisdictions has often not been accompanied by robust disclosure and notice to consumers. In the U.K. in 2006, 18,000 BT customers were subject to trials of Phorm technology without being made aware of it and in 2007 a trial of similar scale occurred without customers being informed.[15] In the U.S., the Economist notes that, "Several American ISPs have quietly switched on NebuAd's system,

---

[13] *Ibid*.
[14] David George-Cosh, "New Hardware Raises Bar on surveillance on Internet" *National Post* (April 14, 2008), online: <http://www.financialpost.com/story.html?id=443523>.
[15] Darren Waters, "BT Advert Trials were 'Illegal'", *BBC News*, (April 1, 2008) online:bbc.co.uk, <http://news.bbc.co.uk/2/hi/technology/7325451.stm>. BT has publicly admitted that it conducted trials with Phorm technology without disclosing the tests to affected subscribers. Subsequently, evaluation report from the 2006 trials has been leaked online. See "BT Admits Misleading Customers over Phorm experiments", *The Register*, (March 17, 2008), online: www.theregister.co.uk, <http://www.theregister.co.uk/2008/03/17/bt_phorm_lies/> and see Wikileaks, "British Telecom Phorm PageSense External Validation Report", online: <http://www.wikileaks.org/wiki/British_Telecom_Phorm_Page_Sense_External_Validation_report>.

inserted a brief reference to it in their terms and conditions, and hoped that nobody would mind."[16]

II APPLICATION OF PIPEDA TO BEHAVIOURAL TARGETING

A. DPI based behavioural targeting involves the collection and use of "personal information"

18. Section 2 of *PIPEDA* defines "personal information" as "… information about an identifiable individual …." Any factual information therefore constitutes personal information as long as it can be linked to an identifiable individual.[17] Information gathered in the course of behavioural targeting may potentially be linked with identifiable subscribers, despite behavioural targeting companies' association of collected data with hash numbers instead of IP addresses.

19. There is a distinction between the collection and the storage and use of information. While behavioural targeting companies have gone to lengths to assure others that they do not store or use personal information, the technology may nonetheless collect user information.

20. Even if the third party behavioural targeting companies use hash functions to de-identify individual users, technically ISPs may first collect personally identifiable information before passing it along to those companies who subsequently assign it a hash number. This means that ISPs would be collecting information when it was still linkable to an individual. (In fact, this is how Phorm's behavioural targeting system is designed for an upcoming trial in Britain.[18])

21. Further, it may be possible for the information stored in companies' databases to be de-anonymized or associated with identifiable individuals. Extensive research has called into question the security of anonymous data. Very little supplementary data has been required

---

[16] "Not Necessarily a Bad Idea; Behavioural Targeting" *The Economist* (June 5, 2008), <http://www.economist.com/opinion/displaystory.cfm?story_id=11496835>.
[17] Office of the Privacy Commissioner of Canada, *A Guide for Businesses and Organizations: Your Privacy Responsibilities* (updated March 2004) "Definitions: Personal information," online: <http://www.privcom.gc.ca/informaiton/guide_e.asp> [Guide]; PIPEDA Case Summary #319, "ISP's anti-spam measures questioned" (November 8, 2005), online: <http://www.privcom.gc.ca/cf-dc/2005-319_20051103_3.asp>.
[18] BT, "BT Webwise | Customer Choice Process", online: <http://webwise.bt.com/webwise/customer_choice.html>.

to associate information from anonymous databases with identifiable individuals.[19] The amount of information stored on behavioural targeting companies' servers is considerable and may include postal codes, web browser information or other useful information for one looking to identify users. Firms' plans to compile information to facilitate the development of sophisticated profiles of individual users. The wealth of information gathered may well permit re-identification.

22. The information collected need not be immediately associated with a name or IP address to be information about an identifiable individual. Information would be regarded as personal, for the purposes of *PIPEDA*, if it could be linked with an identifiable individual.

23. Nor does collected information need to be associated with a common identifier such as a name or address in order to "identify" an individual. Information may be associated with a less common identifier such as an assigned number. This is the interpretation of "identifiability" that is prevalent across other jurisdictions. In a 2007 publication intended to guide interpretation of its data protection Directive, the European Commission wrote that information can be considered to lead to the identification of an individual when the information allows an individual to be singled out from a group.[20] This is also the interpretation provided by the United Kingdom's Information Commissioner's Office.[21] The European Commission stresses that one need not know an individual's name for the individual to be identifiable. Rather, information gleaned through web traffic surveillance, though associated with a less common identifier such as an assigned number, can still consist of personal information.[22]

24. The European Commission states in its publication that determinations about what information leads to identification are context specific. Categorical level information,

---

[19] Bruce Schneier, "Why 'Anonymous' Data Sometimes Isn't", *Wired* (December 13, 2007), online: <http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213/>.
[20] EU Data Protection Working Party, "Re: Article 29, Opinions 4/2007 on the concept of personal data," adopted 20 June 2007, online: <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf> [EU Data Protection] at 12 – 13.
[21] Information Commissioner's Office, "Data Protection Act 1998: Legal Guidance", online: www.ico.gov.uk, <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf> and Information Commissioner's Office, "Determining What is Personal Data: Quick Reference Guide", online: www.ico.gov.uk, <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/160408_v1.0_determining_what_is_personal_data_-_quick_reference_guide.pdf>.
[22] EU Data Protection, *supra* note 15 at 13.

particularly when compiled across a number of categories, is sufficient to single out an individual and thus constitute personal information.[23]

25. Behavioural targeting centers on collecting information in order to identify individuals of interest to advertisers and to single them out from a group. Behavioural targeting firms boast about their ability to drill down "to find the right users" and their "unparalleled targeting capability".[24] Firms compile information to develop sophisticated and detailed profiles of individual users that will, in turn, enable increasingly specific targeted marketing. The information collected and stored is both specific and categorical-level information. In this way, behavioural targeting companies are collecting and using information about identifiable individuals, regardless of the fact that they make use of a less common identifier such as an assigned number.

B. Principle 4.3: Knowledge and Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

26. Under Canadian law, ISPs and other commercial entities must obtain the informed consent of users to the collection, use or disclosure of their personal information for purposes other than those listed in s.7 of PIPEDA. Behavioural targeting clearly constitutes a purpose for which informed consent is required.

27. Major Canadian ISPs have not obtained customers' informed consent for behavioural targeting. Our review of major Canadian ISP Privacy Policies found no references to behavioural targeting.[25] To the extent that Canadian ISPs are profiling individual users for such purposes, ISPs must provide adequate notice to and obtain consent from users to the collection of personal information for this purpose.

28. Such consent should not be assumed (e.g., obtained via opt-out methods) where the information being collected is sensitive or potentially sensitive. Even where opt-out methods of obtaining consent are acceptable, our research suggests that the companies involved in behavioural targeting (e.g., in the USA and UK) use ineffective opt-out mechanisms. Indeed, they may even collect information from individuals who have

[23] *Ibid*. at 13.
[24] Phorm, "The Open Internet Exchange", online: <http://www.phorm.com/oix/>.
[25] See previous complaint against Bell and accompanying complaints against Rogers, Shaw, and Eastlink.

explicitly withdrawn their consent to data collection for behavioural targeting. This is the case where, when a subscriber opts-out of the behavioural targeting program, the company places a cookie on their computer to identify them as having opted-out. However, the user may not appreciate that one must opt out on each individual computer and in each individual browser one is using. Further, if one periodically deletes the cookies on one's computer – as is generally good internet safety practice – then one may be surreptitiously opted back in to behavioural targeting. [26]

29. Even non-cookie based opt-out mechanisms may have difficulty recognizing users across different computers in their own home. IP-based opt-out mechanisms might have trouble recognizing users to whom ISPs have assigned a dynamic IP address.[27] When their IP address changes, those who have opted-out on their computer may also still have their information collected and used as a part of the behavioural targeting technology.[28]

30. Without an effective opt-out mechanism, current behavioural targeting practices do not meet individuals' "reasonable expectations" referred to in Principle 4.3.5. Most individuals would not find it reasonable to have to opt-out of a system repeatedly, nor to have that opt-out fail to remove them from the system they wish to avoid. This characteristic of behavioral targeting technology frustrates the requirement, under Principle 4.3.8 that "an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice." Though some behavioural targeting technology providers claim to be addressing this issue, an effective opt-out mechanism, if not an opt-in approach, must be in place prior to any trial of the technology.

C. Principle 4.4: Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization.

31. Collecting personal information through DPI is unnecessary for the purpose of advertising or providing potential consumers with information regarding a product or service.

---

[26] BT Retail Technology, "PageSense External Validation Report" (January 15, 2007), online: WikiLeaks <http://www.wikileaks.org/wiki/British_Telecom_Phorm_Page_Sense_External_Vali> at 18.
[27] Ryan Singel, "NebuAd defends murky system to 'Opt-Out' from Charter Snooping", *Wired: Threat Level Blog*, (May 29, 2008), online: <http://blog.wired.com/27bstroke6/2008/05/eavesdropping-o.html>.
[28] *Ibid*.

Advertising currently operates by firms targeting content providers that they think would interest and attract their desired market. Advertising space is then purchased according to factors such as time of day, geographic location, and product image. ISPs can also provide consumers with information via email or the contact information provided by the subscriber through traditional means.

32. Online advertising companies appear to be operating under the premise that any and all information about internet users is "necessary for the purposes" of secondary marketing, such that identifying marketing as a purpose is sufficient to justify the collection of a never-ending and infinitely detailed amount of information about individuals. Such an interpretation makes a mockery of PIPEDA, insofar as it places no limits on collection whatsoever in the context of marketing.

33. It is time to set some limits on the ever-expanding profiling of consumers by the advertising industry, especially in the context of online behavioural targeting using technologies such as DPI. We urge the OPC to take on this challenge.

D. Principle 4.8: Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

34. The Privacy policy documents of Bell, Rogers, Shaw and Eastlink do not provide any information about the use of DPI for behavioural targeting. This may be because none of these companies is currently using DPI for that purposes. However, if an ISP were to engage in behavioural targeting without disclosing that it was doing so in a conspicuous manner, it would fail to comply with Principle 4.8.

E. Subs.5(3): Appropriate Purposes in the Circumstances

An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

35. Internet users expect ISPs to collect and use their personal information only as necessary for the deliver of the internet services they contract for. They do not expect ISPs to monitor, track, or examine their communications or activities online, especially not for purposes such as marketing that have no necessary relation to internet service. Even aside

from issues of notice and consent, it is questionable whether ISPs should be engaging in this practice at all. We submit that many reasonable internet users would not consider marketing to be an appropriate purpose for ISPs to collect user information via deep packet inspection or other technologies.

III REQUEST FOR INDUSTRY-WIDE INVESTIGATION LEADING TO BEHAVIOURAL TARGETING GUIDELINES

A. The need for an industry-wide investigation aimed at formulating guidelines

36. Given the rate at which behavioural targeting is developing, and the serious privacy concerns that it raises, we submit that the time is ripe for your office to launch an industry-wide investigation with a view to developing industry guidelines before the practice becomes entrenched. The practice of behavioural targeting is the result of a business climate and trends larger than any single company. Globally, a number of ISPs are partnering with behavioural targeting companies to experiment with and develop behavioural targeting practices and technologies.[29] This segment of the advertising industry promises exponential growth with the estimated U.S. spending on behavioural targeted advertising projected to more than quadruple from $775 million in 2008 to over $4 billion in 2012.[30] Moreover, behavioural targeting companies promote their wares as a way for ISPs – who otherwise face a high volume, low margin business model – to gain new, lucrative revenue sources.[31]

37. Recognizing the broad character of the behavioural targeting phenomenon, CIPPIC has been working with the Washington D.C.-based Center for Democracy and Technology (CDT) and other consumer and privacy advocates to highlight and address concerns. Our research has centered on the identifying the behavioural targeting practices of ISPs and how those practices differ from earlier forms of behavioural targeting.

---

[29] In the United Kingdom, BT is undertaking a trial to test the behavioural targeting company Phorm's system on 10,000 subscribers and completed non-disclosed trials in 2006 and 2007. *The Economist* noted in June that a number of U.S. ISPs have discretely experimented with behavioural targeting systems. See "Not Necessarily a Bad Idea; Behavioural Targeting" *The Economist* (June 5, 2008), <http://www.economist.com/opinion/displaystory.cfm?story_id=11496835>; c.f. The Register, "American ISPs already sharing data with outside ad firms", (April 10, 2008), online: <http://www.theregister.co.uk/2008/04/10/american_isps_embrace_behavioral_ad_targeting/>.

[30] Internet Advertising Bureau, "Industry Stats & Data by eMarketer", online: <http://www.iab.net/insights_research/iab_research/1675>.

[31] Phorm, "Partners: Phorm: ISPs Benefit by Working with Phorm", online: <http://partners.phorm.com/>; NebuAd, "NebuAd / Service Providers", online: <http://www.nebuad.com/providers/providers.php>.

38. Other jurisdictions have already completed or are starting examinations of the privacy concerns associated with behavioural targeting. In the U.K., the Office of the Information Commission recently reviewed behavioural targeting company Phorm's practices and found that merely providing users with an opt-out did not constitute obtaining adequate consent to behavioural targeting.[32]

39. In the U.S., the Federal Trade Commission (FTC) is developing privacy principles to guide company self-regulation of behavioural advertising.[33] The New York State Legislature is contemplating instituting fines for collecting data and using it for advertising purposes without consent.[34] On July 17, The U.S. House of Representatives Subcommittee for Telecommunications and the Internet began hearings looking into behavioural targeting and other DPI technology uses.[35] Representative Edward Markey, Chairman of the House of Representatives Subcommittee for Telecommunications and the Internet, recently wrote a letter to Charter Communications asking them to halt their trials with behavioural targeting company NebuAd until the committee could address the issue.[36] More recently, Rep. Markey and Rep. John Dingell, Chairman of the House of Representatives Committee on Energy and Commerce, wrote another letter to U.S. ISP Embarq, raising questions about the company's NebuAd trials which took place with no direct notice to consumers and raised "serious privacy red flags".[37] The U.S. Senate Commerce Committee is also considering guidelines governing behavioural targeting practices.[38]

---

[32] Information Commissioner's Office, "Phorm – Webwise and Open Internet Exchange" online: Information Commissioner's Office <http://www.ico.gov.uk/Home/about_us/news_and_views/current_topics/phorm_webwise_and_oie.aspx>.
[33] Federal Trade Commission, "FTC Staff Propose Online Behavioral Advertising Privacy Principles", (December 10, 2007), online: <http://www.ftc.gov/opa/2007/12/principles.shtm>.
[34] Louise Story, "A Push to Limit Tracking Web Surfers' Clicks" *New York Times* (March 20, 2008), <http://www.nytimes.com/2008/03/20/business/media/20adco.html>.
[35] The House Committee on Energy and Commerce, "Hearing – 110th Congress: What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies", online: <http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.071708.DeepPacket.shtml>.
[36] Congressman Edward Markey, "Markey, Barton Raise Privacy Concerns about Charter Comm.'s Plans" Press Release (May 16, 2008), online: Congressman Edward Markey <http://markey.house.gov/docs/telecomm/letter_charter_comm_privacy.pdf>.
[37] Congressman Edward Markey, "Markey: Embarq's Web Tracking Raises Privacy Concerns" Press Release (July 15, 2008), online: Congressman Edward Markey <http://markey.house.gov/index.php?option=com_content&task=view&id=3410&Itemid=141>.
[38] Saul Hansell, "Senators Weigh Possible Rules for Advertising and Online Privacy", *The New York Times: Bits Blog*, (July 9, 2008), online: <http://bits.blogs.nytimes.com/2008/07/09/senators-weigh-possible-rules-for-advertising-and-online-privacy/>.

40. Guidelines regarding behavioural targeting would be of great value to both consumers and industry. Behavioural targeting undermines consumers' trust in the internet – a cornerstone of the medium's rapid economic, social and cultural success. Long-standing internet norms have precluded the interception and inspection of traffic and consumers have come to expect as much. A number of different companies in the internet value chain have expended great efforts to build user trust. To allow ISPs to engage in behavioural targeting runs the risk of making Canadians wary of conducting their business online and undermining earlier trust-building efforts. Further, these new practices impose significant adjustment costs on knowledgeable consumers who wish to avoid them, while leaving unwitting consumers vulnerable to exploitation. Enforceable guidelines would help to safeguard vital consumer and privacy interests and would provide oversight of an industry and practice that has been marked thus far by a notable lack of disclosure and notice.

41. Behavioural targeting guidelines would be a boon to industry online. Guidelines would provide greater certainty for business to develop practices consistent with privacy obligations. In the U.S. the uncertainty around behavioural advertising has become an issue for ISPs. Indeed, ISPs Charter, CenturyTel, Embarq and Knology, have all suspended planned NebuAd trials out of fear about potential legal liability.[39] Companies may devote resources to and make investments in implementing a practice and a technology that is ultimately incongruent with privacy law and principles. By providing increased certainty, OPC guidelines would help companies navigate issues that arise as practices and technologies develop. As the emergence of DPI and behavioural targeting underscore, what is technically impractical one day is eminently feasible the next.

B. Conclusion

42. We therefore request that the Office of the Privacy Commissioner undertake an industry-wide investigation of actual and potential uses of Deep Packet Inspection for behavioural targeting purposes by Canadian ISPs, with a view to formulating guidelines concerning the current and potential future uses of behavioural targeting technologies by ISPs.

[39] DSL Reports, "Congress 'grills' NebuAd CEO", *DSL Reports*, (July 10, 2008), online: <http://www.dslreports.com/shownews/Congress-Grills-NebuAD-CEO-96006>.

43. We hope that you share our view that such an initiative is needed, and look forward to hearing your response. Should you have any questions, please do not hesitate to contact the undersigned.

Sincerely,

Original Signed
Rishi Hargovan
CIPPIC Summer Intern

Original Signed
Philippa Lawson
Director, CIPPIC

cc: Bell Canada, Rogers Communications Inc., Shaw Communications Inc., Eastlink, CAIP