Redesigning IP Geolocation:
Privacy by Design and Online Targeted Advertising

October 2010

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner,
Ontario, Canada

With contributions from:

beringmedia

Acknowledgements

This is to acknowledge Ken Anderson, Assistant Privacy Commissioner, as well as Michelle Chibba and Vance Lockton, Policy Department staff at the Information and Privacy Commissioner's Office, Ontario, Canada, for their input to this paper.

Information and Privacy Commissioner, Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

Table of Contents

Commissioner's Foreword

The Internet and its associated marketing practices have rapidly evolved, to a point where much of the online advertising is provided by companies with whom the individual does not have a direct business relationship. And yet, such companies collect and manage a great deal of data about individuals. This has opened up a broad and ongoing debate in the area of privacy and online targeted advertising. The purpose of this paper is to explore new, original contributions to this discussion, highlighting the solutions made possible through a combination of innovative thought and "baked-in" privacy – which I call *Privacy by Design*.

The subject of targeted advertising brings with it a host of privacy issues, from those directly connected with the practice (the tracking of online behaviours, the use of location data as reported by mobile devices, etc.) to broader, Internet-wide topics (IP address as personal information, etc.). Privacy choices and consumer trust have remained at the forefront of these concerns.

In this paper, we focus on a single facet of targeted advertising – the developing area of precise IP geolocation, and the potential role of ISPs in the ad serving model. In particular, we describe the work of Ontario company Bering Media, Inc. Bering Media set out to develop an innovative technology to allow ISPs that have made the decision to partner with an ad server to provide IP geolocation services, to do so with *zero* disclosure of potentially personally identifiable information about subscribers. This would further allow the ISP to partner with an ad server without the need for reading or modifying any packets travelling through the ISP's network.

As the Information and Privacy Commissioner of Ontario, part of my mandate is to conduct research into privacy-related issues involved in emerging technologies or new programs that may impact one's privacy. I am very excited to have worked with Bering Media on this project, and gratefully acknowledge the contribution to this paper of its President and CEO, Michael Ho. I am greatly appreciative when technology developers bake-in privacy from the outset, and fully embrace the concept of *Privacy by Design*.

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

1 Introduction

Advertisements displayed to potential customers through traditional media – newspapers, magazines, television, and radio – are based on what is known about the demographics of the target audience as a whole. If a particular magazine is known to be generally purchased and read by males aged 35-50, advertisements will naturally be tailored to that group. Mail-based advertising adds location data to this information, allowing tailoring based on local businesses or neighbourhood demographics.

Online advertising, however, allows for a much more direct relationship with audience members. Whereas a television network, for example, must serve ads to *all* individuals watching a particular program (or, at least, accessing the same broadcast feed), an advertiser with space on a website has the ability to select a specific advertisement to show to each *individual* visitor. Of course, in order to target a relevant ad to a specific Web user, some amount of information must be known about that person. The means by which this targeting is done can vary significantly – each having a different impact on the privacy of the individuals to whom the ads are served, particularly if the information is (or can be) associated with an identifiable person.

A common form of online advertising is based on the single current action of a user, and known as "contextual" targeting. This technique involves the delivery of ads that correspond to keywords of an Internet search, or to the content of the webpage the user is currently visiting. "Behavioural" targeting, on the other hand, aggregates these actions into a profile of an individual user, after which ads are served based on his or her stated or inferred interests. A third means of targeting ads towards specific audiences online is through geographic (or geo-) targeting. "Geo-targeting" is based on the identification of the real-world geographical location (geolocation) of an Internet-connected device in order to deliver location-based advertising online, extending the decades-old practice of offline advertising to the Internet.

To maintain the trust and confidence of consumers, approaches to targeted advertising must embrace the 'positive-sum' paradigm, which seeks to meet all legitimate business objectives – including, in this case, both the serving of relevant ads and the maintaining of Web user privacy. This can be accomplished through the principles of *Privacy by Design*, which advocates the designing-in of privacy measures at all stages of development and deployment, including business practices, physical design, and technology.

In this thought piece, we examine the application of the positive-sum paradigm shift to one particular method of targeted advertising – precise IP geolocation – through the work of Toronto company Bering Media, Inc. Bering Media identified privacy issues inherent with the current implementations of geo-targeting, and redesigned the technique to improve functionality while enhancing privacy in the shift to precise IP geolocation. In describing this system, we do not suggest that it is the only privacy-protective targeted advertising or IP geolocation model possible. Instead, we present it as a representative of the solutions made possible by the combination of innovative thought and *Privacy by Design*, and encourage all entities in the advertising sector to evaluate the application of the *PbD* principles to their own technologies.

2 IP Geolocation

The geographic targeting of advertisements is a well-established practice in the offline world. Flyers, posters, billboards and so forth are distributed and displayed based on proximity to a business or event, or the known demographics of the area. In the same way, geolocation technologies look to present individuals with locally relevant advertising in a globally accessible space.

When a user connects to the Internet, the websites they browse do not recognize the visitor as an individual, unless the user has volunteered his or her own personal information. Instead, the user is known by his or her IP address, which has been assigned to him or her, typically on a dynamic basis, by an Internet Service Provider (ISP). The geographic location of a wireline connected computer is generally not reported by the device itself, but instead inferred based on this IP address – hence the term, IP geolocation.

Traditionally, the geolocation of IP addresses is determined in a database-lookup model. IP geolocation database aggregators collect location information from a variety of sources about large numbers of IP addresses,[1] and disclose or sell access to this data to websites and advertisers. For every IP address queried, the database-lookup model returns the known or inferred geographical location data. Currently, this data is most accurate at the country and province/state levels[2], and can be applied to geo-fencing (directing users to google.ca, instead of google.com, for instance) and credit card fraud detection, as well as for advertising purposes.

However, geolocation technologies are looking to shift towards greater levels of granularity – identifying IP addresses by postal code or ZIP+4 information.[3] This shift to more precise IP geolocation changes the privacy considerations associated with targeting ads to Internet users based on their offline location. In particular, understanding the level of precision in IP geolocation is important due to the risk of associating an individual with a particular IP address.

2.1 Precision and Risks to Privacy

When IP addresses are geolocated to a large area (a country or province, for example), there will typically be a sufficient number of both IP addresses and individuals within that region to prevent the linkage of a specific IP address back to an identifiable person. However, if an advertiser is provided IP geolocation data at a high level of granularity (postal code or ZIP+4, for example), there is an increased risk of re-identification of individuals (and hence their association with a particular IP address). IP geolocation database companies often state that the information they hold is not personally identifiable.[4] Many academics have found, however, that in combination with other

1 One such company, Quova, claims to track and map "nearly 2 billion" IP addresses. By contrast, the current IPv4 addressing model allows a maximum of ~4.3 billion (2 ^ 32) addresses. http://www.quova.com/documents/Datasheet.pdf

2 A PriceWaterhouseCooper audit of Quova's geolocation database found that it was 99.9% accurate at the country level, and 98.2% accurate at the US state level. http://www.quova.com/press-releases/pricewaterhousecoopers-pwc-completes-annual-audit-of-quova-ip-geolocation-data-2

3 See, for instance: Davis, W. (2010, Feb. 25) Start-Up Links 65 Million IP Addresses to Users, Readies Targeting Platform. *The Daily Online Examiner.* Available online at: http://bit.ly/d8gwzz

4 For instance: "Throughout [the data collection] process, ClearSight receives no PII." http://www.clearsightinteractive.com/clearprofile.html

databases (many of which are freely available online), 'de-identified' records such as those found in traditional geolocation lookup databases can often be linked back to specific individuals. [5]

Dr. Khaled El Emam, at the University of Ottawa, for instance, has studied the likelihood that an individual can be re-identified by a Canadian postal code.[6] For purposes of this paper, Dr. El Emam's research helps to determine the following: consider a scenario in which Person A is known to live within a certain postal code in Canada (as found in an online database), and that IP address B has been assigned to a household within that postal code (as determined by precise IP geolocation). With what probability of correctness could one guess that IP address B is assigned to a computing device associated with Person A?

Suppose first that only the leading three characters of the postal code in question (the "forward sortation area", or FSA) were known. Since the median FSA represents about 8,000 households[7], there is, on average, a one in 8,000 chance that IP address B would be assigned to Person A. This data (on its own) would thus not be considered significantly likely to create a potential association between an individual and an IP address.

However, some targeted advertisers using geolocation technology may prefer the level of precision associated with the *full* postal code. This changes the possibility of re-identification significantly, as the median six-character postal code in Canada represents only 19 households. At least one-quarter of all Canadian postal codes represents seven or fewer households; in fact, at least one-quarter of postal codes in Alberta, Quebec, the Maritimes and Yukon represent five or fewer households. That is, in the latter cases, there would be a 20 percent or greater chance of associating an IP address to an individual based on postal code geolocation.[8] Furthermore, a postal code can even represent a single household, in some instances.

Due to the above, it should be recognized that a database (or other means of distribution) of IP addresses and associated precise geolocations (as represented by full postal code, or ZIP+4 in the United States) carries a risk of re-identification of individuals. There are two potential courses of action to mitigate this risk. First, advertisers could consider a lower level of granularity for targeting purposes. For instance, if it is sufficient to know only that a user is coming from Canada, the use of an IP geolocation database that contains *only* country-level information creates far fewer privacy concerns than the use of a postal code level database. However, if neighbourhood or postal code information is required for marketing purposes, another model of IP geolocation which follows the tenets of *Privacy by Design* – using built-in protections to ensure individual privacy, while allowing the desired functionality – may be needed to achieve a 'positive-sum' outcome.

5 See, for instance:

- Sweeney, L. (2000) Uniqueness of Simple Demographics in the U.S. Population. *LIDAP-WP4*. Carnegie Mellon University, Laboratory for International Data Privacy.
- Narayanan, A., & Shmatikov, V. (2008) Robust De-anonymization of Large Sparse Datasets. In Proc. of 29th IEEE symposium on Security and Privacy, Oakland, CA, pp. 111-125.
- El Emam, K,. Brown, A., & AbdelMalik, P. (2009) Evaluating Predictors of Geographic Area Population Size Cut-Offs to Manage Re-Identification Risk. *J Am Med Inform Assoc*. v. 16, p. 256-266.

6 El Emam, K. (2009, Dec. 4) Can postal codes re-identify individuals? *Electronic Health Information Laboratory*. Available online at: http://bit.ly/d5oNM1

7 "More Information on Postal Code." (2009) *Statistics Canada*. Available online at: http://www12.statcan.ca/census-recensement/2006/ref/dict/geo035a-eng.cfm

8 El-Emam, K. (2009, Dec. 4) Can postal codes re-identify individuals?

3 Building Privacy Into IP Geolocation

3.1 Privacy by Design

In the context of online targeted advertising, we must consider informational privacy – the right of an individual to exercise control over the collection, use, disclosure and retention of his or her personal information. Personal information (also known as personally identifiable information, or PII) is any information, recorded or otherwise, relating to an identifiable individual. Almost any information, if linked to an identifiable individual, can become personal in nature, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational. This definition of personal information is quite broad in scope. The challenges for privacy and data protection are equally broad – but are always best addressed by designing-in solutions from the outset.

Privacy by Design (PbD) is a concept developed in the mid-nineties (see Appendix A). In brief, *PbD* is a concept that involves embedding privacy into the design specifications of technologies. This may be achieved by building the principles of Fair Information Practices into the design, operation and management of information processing technologies and systems. While *PbD* has information technology as its primary area of application, it has since expanded in scope to include two other areas. In total, the three areas of application are: (1) information technology; (2) accountable business practices; and (3) physical design and infrastructures. The current era is one of near-exponential growth in the creation, dissemination, use and retention of personally identifiable information. Whether applied at the level of information technology, business practices or systems, it is more critical now than ever to embrace the *Privacy by Design* approach if privacy, as it is currently known, is to survive well into the 21st century.

Given the necessity of establishing user trust in order to gain public and political acceptance of their technologies, the targeted advertising industry must 'think *Privacy by Design*' as new products are developed, marketed and deployed. In the next sections, we will discuss the particular IP geolocation technology developed by Toronto company Bering Media, Inc. – and the ways in which their solution was motivated by an overall desire to design-in privacy from the outset.

3.2 Bering Media's IP Geolocation Technology

Bering Media has developed an alternative to the collection and disclosure model of traditional IP geolocation lookup databases by recognizing that as network operators and owners of the IP address space allocated to their network, ISPs are in the unique position of already having knowledge of IP geolocation information for their subscribers. This information is required as part of the ISPs normal course of operation – thus, avoiding the need for any third party collection of IP geolocation data.

Of course, an ISP's disclosure of precise IP geolocation data to a third party would be no more privacy-protective than the traditional database-lookup model.

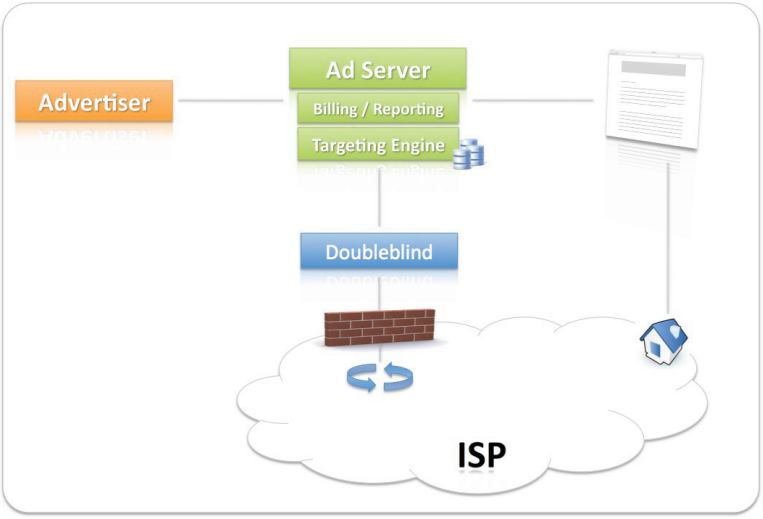
To address this, Bering Media has created technology which allows ISPs and ad servers to collaborate in order to serve targeted advertisements to Internet users based on precise IP geolocation location information, without the disclosure of any precise IP geolocation information. Through a sophisticated technology platform, the targeting occurs without any sensitive information being disclosed by either the ISP or the ad server – each remains aware only of the information of which they are already in possession. The various privacy protections associated with Bering Media's technology are explained in the following sections, as example implementations of the *Privacy by Design* concept.

3.2.1 Doubleblind Privacy Architecture – Zero Disclosure

In their re-imagining of IP geolocation, Bering Media started with the goal of allowing ISPs to become involved in the geo-targeting process without ever having to disclose personally identifiable information, including postal code and ZIP+4 information, about their subscribers. Patent-pending privacy technologies were then developed to form the basis of an overall privacy architecture in order to accomplish this goal.

Bering Media is aware that privacy must be considered in the design of any ISP targeted advertising solution. At the most fundamental level, Bering Media decided to solely focus on location and to actively avoid the collection of behavioural or any other online activity data, as well as the reading or modification of any data packets being sent to or from Internet users. This translated to a basic architectural decision that avoids any interaction with routers, deep packet inspection (DPI) equipment and any other networking or insertion equipment. Bering Media leverages a completely passive deployment model that leaves the existing online ad-serving model intact.

Bering Media's technology is based on its *doubleblind privacy* architecture, by which the ISP and the ad server never need to disclose PII or otherwise sensitive information to each other, yet can achieve granular ad geo-targeting. The ISP, for instance, already knows the physical geographical location associated with every IP address currently under its control – as an element of its service provision – and with Bering Media's technology, the ISP will not learn any information about the ads being delivered to those IP addresses, or advertisers' criteria for targeting ads to particular areas. Similarly, the ad server already knows to what IP address it needs to deliver an ad – information required to perform *its* service – and with Bering Media's technology, the ad server will not learn the physical location (or precise geolocation) of that IP address. In effect, a firewall is created between the ISP and the ad server that pushes all geo-matching decisions down into the ISP's secure network.



In the traditional database-lookup model, the ad server first queries a geolocation database with an IP address. The database then returns what has previously been determined to be the physical location associated with that IP address, allowing the ad server to perform the geo-matching process based on the targeting criteria set out by advertisers.

Bering Media's *doubleblind privacy* architecture, on the other hand, departs from this traditional dataflow, as follows. First, when an advertising campaign is created, the advertiser's potentially proprietary demographic or geographic targeting information is converted into non-descript geo-codes. These codes represent the geographic area to be targeted by a particular advertising campaign (which itself is referred to only by a campaign ID number, not by the ad's actual content) – no information about why these particular codes were selected is present. These campaign IDs and associated geo-codes are then distributed to Bering Media's specially designed privacy technology, which is wholly owned and operated by an ISP.[9] Behind the ISP's firewall, Bering Media's technology is then able to determine which IP addresses should be served which advertising campaigns, by geo-matching the ISP's precise geographic location information against the geo-codes submitted by the advertiser. Finally, when an ad server queries an IP address, the resulting matched campaign IDs are returned – not precise geolocation information.

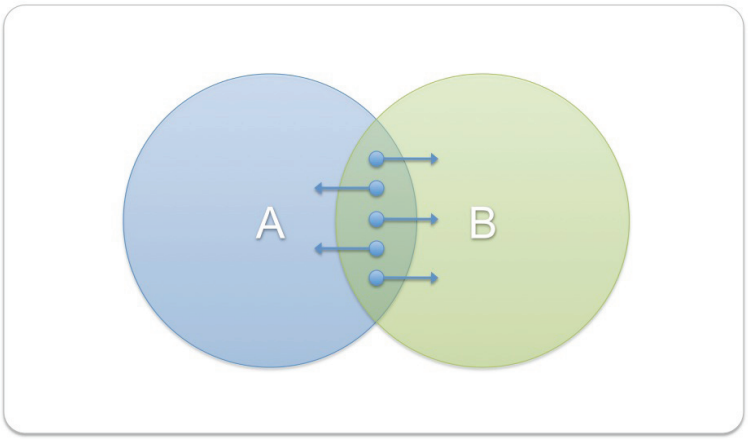
Thus, the ad server does not disclose its proprietary targeting information and the ISP does not disclose PII about its subscribers – but the effective geo-targeting of advertisements is able to occur.

3.2.2 Minimum-match Thresholds / Anti-inference Algorithms

Meeting the original goal of zero disclosure of personally identifiable information was only part of the privacy solution, however – protections must also exist that ensure that PII cannot be *inferred* through the use of Bering Media's system. As mentioned earlier, postal code and ZIP+4 cannot always be considered – in the context of re-identification – aggregate information. Furthermore, an arbitrary definition of geographic area (for example a single square mile) also cannot always be considered aggregate information, due to variable factors such as population density (urban vs. rural, etc.). As a result, two additional privacy technologies – minimum match threshold and anti-inference algorithms – were developed and integrated into the *doubleblind privacy* architecture to proactively ensure that all campaigns always meet sufficiently aggregate privacy counts to properly address privacy and security needs.

The use of anti-inference algorithms and the minimum match threshold can be illustrated with the following example. Suppose, as in the figure below, an advertising network has been contracted by two businesses (A and B), which want to serve online ads to individuals within 10 km of their respective locations. The minimum-match threshold ensures that each individual ad campaign matches against a sufficient number of individuals as to mitigate the risk of re-identification. It may be the case, though, that the ad serving criteria for businesses A and B overlap on only a small number of individuals – a single postal code with the median 19 households, for example. Should the ad network then serve ads for both A and B to a particular IP address, the ad network would know that that IP address was assigned within the 'overlap' postal code – raising the risk of re-identification as described in section 2.1.

9 As this technology is wholly owned and operated by the ISP, Bering Media does not operate as a 'trusted third party' in this ad-serving model. Bering Media receives neither information regarding campaign geo-codes nor ISP subscriber information – they act solely as a technology provider.



Should this situation occur, the Bering Media technology would detect this overlap, and randomly assign the IP addresses in question to match to only the ad campaign for store A or store B. This removes the possibility that a third party could infer precise geolocation information about this small group based on the overlap between target regions.

The development and inclusion of such algorithms demonstrates the importance of going beyond baseline data protection to consider and address any possible actions of an adversary – such as re-identification of 'anonymous' or 'aggregate' data. This approach, of identifying and protecting against *potential* threats as well as known ones, is key to the effective protection of privacy.

3.2.3 Dynamic IP Address Management

Dynamic IP addressing, the process by which ISPs periodically change the IP addresses assigned to their subscribers, provides Internet users with an added layer of privacy while online. Bering Media is also in the process of developing technologies and intellectual property to assist ISPs with dynamic IP addressing change frequency. As a subscriber's IP address serves, effectively, as a unique online identifier for him or her for the length of time that it is assigned to that subscriber,[10] frequent changes are beneficial to user privacy. Bering Media recognized that their technology is capable of notifying an ISP when a particular IP address has been queried a disproportionately large number of times – implying the need for a change to increase privacy protection for subscribers. Again, this shows the benefits of instilling a culture of privacy within an organization – when privacy is always at the forefront of thought, innovative solutions to problems will arise.

3.2.4 Persistent Opt-out

In addition to keeping PII within the ISP's network, Bering Media's technology introduces the ability for individuals to opt out of the use of their location information for targeting ads – and this choice is persistent. The United States recently proposed Boucher-Stearns Privacy Bill recommends that targeted advertising opt-out mechanisms should ensure that the choices of users are preserved

10 Websites are aware of the IP address of each visitor. Whether this address is stored, or associated with any other data, is a choice of each individual organization.

and protected from incidental or accidental deletion.[11] Currently, one of the most common means of opting out of the collection of information for advertising purposes is the 'opt-out cookie.' In this system, ad companies looking to place an 'advertising cookie', which is able to track the user's behaviour across sites with which that company has a relationship, first checks to see if an 'opt-out cookie' – a small text file indicating the user's choice – has been placed. If so, the advertiser is prevented from placing the tracking cookie.[12] Though initially effective, this method often risks the user inadvertently deleting the opt-out cookie when he or she clears his or her web browser cookies (a recommended security practice). Thus, opting out is possible, but often isn't preserved.

By embedding the opt-out choice into technology, though, it is possible to create a truly persistent opt-out. Google, for instance, has augmented its cookie-based opt-out for the DoubleClick cookie with a browser plug-in that lets a user keep their opt-out status even after deleting all of the cookies on his or her computer.[13] This effectively embeds a permanent opt-out of the collection of information by DoubleClick into the web browser technology.

Similarly, Bering Media embedded an opt-out mechanism into their geolocation architecture. The mechanism is network based (as opposed to being located on the individual's computer), allowing an ISP using Bering Media's technology to provide and maintain a permanent opt-out that is not based on cookies or IP addresses and therefore avoids any incidental or accidental deletion. As a result, once an individual has opted out, they are permanently removed from any current or future geo-matching until they decide to change their status. This results in a no-response to any advertiser query, as the user no longer exists within the Bering Media system. By embedding the opt-out mechanism into the technology, a truly persistent opt-out is created in order to properly support the individual users' privacy choices.

3.2.5 Notice to Users

Many of the issues frequently raised when discussing online targeted advertising center around a lack of transparency. Users are often unclear about what information is being collected about them, what organization is collecting this information, how it is used, or how (or if) they can opt out of a service. In a number of situations, users have been wholly unaware that data is being collected for online targeted advertising – and were thus not even in a position to make inquiries about the practice.

This lack of visibility is, fortunately, beginning to change. Many standards documents are suggesting or mandating notice, choice, transparency, and general user education about advertising practices.[14] Companies are beginning to explain their practices to consumers, either through educational material

11 Boucher, R. and Stearns, C. (2010, May) Unnamed Privacy Bill. Draft released for discussion May 4, 2010. Draft text available online at: www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf

12 The Network Advertising Initiative has created a single website at which users can check their computer for the presence of nearly 50 different tracking cookies from various ad networks, and place opt-out cookies for any or all of those networks. http://www.networkadvertising.org/managing/opt_out.asp

13 http://www.google.com/ads/preferences/plugin/. The plug-in is available for Internet Explorer and Firefox (~83% of total browser market share as of May 2010); alternative opt-out instructions are available for Safari and Chrome (~15% of browser market share).

14 See, for instance, "FTC Staff Report: Self-Regulatory Principles for Online Behavioural Advertising." (2009, Feb.) Available online at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf or "Self-Regulatory Principles for Online Behavioural Advertising." (2009, July). Available online at: http://www.iab.net/media/file/ven-principles-07-01-09.pdf

linked from banner ads[15] or through text-links or icons featured near ads served based on targeting mechanisms.[16] These efforts parallel a long-standing effort by the IPC to promote a practical approach to privacy. In 2005, for instance, the International Association of Privacy Professional's *Privacy Innovation Award* was received by the IPC in recognition for work on Privacy Short Notices – a concise, easily understood notice informing individuals of how their personal information is being used[17]. In the acceptance speech, it was noted that, "creating privacy notices that are short and easily understood maximizes our effectiveness in reaching the public."

Bering Media understands the importance of notice and transparency, and works with ISPs who implement their geolocation technology to provide up front notice and education about the targeting system. This gives the user the opportunity to make an *educated* choice in regard to their participation in this type of targeted advertising, and allows both Bering Media and the ISP the opportunity to explain their commitment to privacy, and the technological and policy means by which this commitment is enforced.

4 Conclusions

This paper is intended to show that privacy-protective versions of standard online targeted advertising practices can indeed be developed to achieve the desired 'positive-sum' outcome. Users *must* be aware of the targeting process, why they are being served targeted advertisements and how data about them is being collected, used and disclosed. As well, as with any system that uses personal data, users must retain control of data use – being able to access and understand any profile data about themselves, and being able to stop the process at any time. At the very least, a clear, easily accessible and well-explained opt-out mechanism must be in place, and the user must actively be made aware of this option – it should not be available only to those who accidently 'discover' its presence, along with the presence of the online advertising itself.

The online targeted advertising industry is attempting to change public opinion regarding their practices by addressing privacy concerns and highlighting user (and industry) benefits. The best way for this change to occur is for privacy to be fully addressed along the lines of *Privacy by Design* principles, wherein data protection becomes the default, and users are educated about the various processes involved. In the presence of *Privacy by Design*, the benefits of targeted advertising may be easily recognized. In the words of the chair of the U.S. Federal Trade Commission, Commissioner Jon Leibowitz, as long as consumer choice and control are preserved, targeted ads are "usually good for consumers, who don't have to waste their time slogging through pitches for products they would never buy; good for advertisers, who efficiently reach their customers; and good for the

15 See, for instance, AOL's 'Mr. Penguin' campaign – video resource available online at: http://corp.aol.com/o/mr-penguin/

16 See, for instance, the Microsoft advertising network page: http://choice.live.com/ or the "Power I" initiative, described in Kaye, K. (2010, Jan. 27) New Ad Industry Group Icon Could Symbolize Non-Behavioural Targeting, Too. *ClickZ*. Available online at: http://www.clickz.com/3636298

17 More information about Short Notices is available at: http://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=728 (or http://bit.ly/9V6GDw)

Internet, where online advertising helps support the free content everyone enjoys and expects."[18] This represents positive-sum thinking, all the way!

Bering Media has embraced the spirit of *Privacy by Design*, demonstrating an innovative technology that functions in a positive-sum manner and allows for online targeting through IP geolocation in a privacy-protective manner. To protect the future of privacy, we need to shift the paradigm of advertising, such that it is no longer the case that more and more personally identifiable data is believed to be necessary to effectively and efficiently market products and services to consumers. We look forward to seeing additional privacy-protective developments in other areas of targeted advertising.

18 Eggerton, J. (2010, May 12) Leibowitz: FTC Not Interested in Regulating Behavioral Ads. *Multichannel News*. Available online at: http://www.multichannel.com/article/452585-Leibowitz_FTC_Not_Interested_In_Regulating_Behavioral_Ads.php

Appendix A – The 7 Foundational Principles of *Privacy by Design*

Available online at: http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Privacy by Design is a concept developed by Dr. Ann Cavoukian in the 1990's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* – ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following 7 Foundational Principles:

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* (*PbD*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. *PbD* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the ***Default***

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

3. Privacy ***Embedded*** into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. ***Full*** Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

6. Visibility and Transparency

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

Bering Media, Inc.
107 Atlantic Avenue
Suite 303
Toronto, Ontario
Canada M6K 1Y2
E-mail: info@beringmedia.com

October 2010

http://www.privacybydesign.ca | http://beringmedia.com

beringmedia