dentons.com

DENTONS

Insights and Commentary from Dentons

On March 31, 2013, three pre-eminent law firms—Salans, Fraser Milner Casgrain, and SNR Denton—combined to form Dentons, a Top 10 global law firm with more than 2,500 lawyers and professionals worldwide.

This document was authored by representatives of one of the founding firms prior to our combination launch, and it continues to be offered to provide our clients with the information they need to do business in an increasingly complex, interconnected and competitive marketplace.

the risk assessment because the employee improperly sought out the complainant's information for personal reasons, the employee being the ex-spouse of the complainant's current spouse.

14 S.O. 2004, c. 3, Schedule A.

15 R.S.O. 1990, c. F.31.

16 *Reynolds v. Binstock*, [2006] O.J. No. 4356, 217 O.A.C. 146.

17 As Commissioner Cavoukian put it: "… the circumstances of that investigation are strikingly similar in nature to the circumstances of this complaint." *PHIPA* Order HO-010 at 1.

18 *Ibid.* at 2.

19 *Ibid.* at 28.

20 *Ibid.*

21 *Ibid.*

22 *Ibid*.

23 *Ibid.*

24 Initially, the investigator suggested that the complaint circumstances in PC11-34 were "analogous" to those in Order HO-010 (at 7) but later acknowledged that there were differences (at 9).

25 This is suggested by submissions made by Ministry counsel, which are quoted by the IPC investigator. It is unfortunate that the report is not entirely clear on this point given that factors motivating disclosure may have an important bearing on the nature of the remedial response to the breach.

26 *Supra* note 1 at 7.

27 *Ibid.* at 11.

28 *Ibid.* at 7.

29 *Supra* note 4 at 27.

30 *Supra* note 16.

31 R.S.O. 1995, c. M.56.

32 This was the case in both Order HO-002 and Order HO-010.

33 As I noted in my *PrivacyScan* article (*supra* note 5), in some of the arbitration decisions issuing out of Saskatchewan that Commissioner Dickson appeared to be critical of, arbitrators considered a range of factors, including the employee's personal circumstances. In one instance, the individual, whose breach was motivated out of concern rather than malice, had an otherwise clean employment record with positive performance reviews. She was also separated at the time of the discharge, which caused her considerable economic hardship. See *Canadian Union of Public Employees, Local 3967 v. Regina Qu'appelle Health Region*, [2009] S.L.A.A. No. 20 (SK L.A.) and [2010] S.L.A.A. No. 5 (SK L.A.).

34 *Supra* note 16 at para. 21.

35 At 28.

36 I have discussed this issue at length in three earlier articles. See "Personal Information in the Adjudicative Decisions of Administrative Agencies: An Argument for Limits," (2008), 43 Adv. Q. 1, "Administrative Transparency and the Protection of Privacy in a Digital Era," (2010), 37 Adv. Q. 1, and "Publicity and Privacy in Administrative Adjudication: A Right to be Forgotten?," (2011), 39 Adv. Q. 1.

37 Section 62(1) of *PHIPA* provides a party affected by a Commissioner's order issued under clauses 61(1)(c) to (h) to appeal to the Divisional Court on a question of law. This would encompass an order to disclose disciplinary details framed as "an information practice specified by the Commissioner" pursuant to s. 61(1)(g). Arguably, judicial review might still be available for a recommendation that such disclosure occur, given that the Commissioner would still be operating in an adjudicative capacity under *PHIPA*, unlike the case in *Reynolds v. Binstock.*

38 *Labour Relations and Employment Statute Amendment Act*, 1995, S.O. 1995 c. 1, ss. 82-83.

MAC AND IP ADDRESSES: PERSONAL INFORMATION?

Timothy M. Banks
Partner
Business Law Department
Fraser Milner Casgrain LLP

Introduction

A minor kerfuffle broke out at a recent (May 30, 2012) U.S. Federal Trade Commission workshop, "*In Short: Advertising and Privacy Disclosures in a Digital World*."[1] During a discussion of privacy and advertising on mobile platforms, Sara Kloek, Director of Outreach for the Association for Competitive Technology, stated that a MAC address was information about a device and not personal information. Pam Dixon, founder and executive director of the World Privacy Forum, was quick to snap back stating that a MAC address was personal information.

Who is right? Why is it that we are still debating this fundamental issue? And is the answer different for IP addresses? This article attempts to unpack these issues in the context of Canadian privacy laws and principles.

What's a MAC address?

A Media Access Control ("MAC") address is an alpha-numeric number that is assigned to a hardware device that connects to a computer network. In simple terms, a MAC address is part of the addressing system that will allow one device to route packets of information to another device. I'm a lawyer and not a technologist but I understand that it is fair to say that the MAC address for my smart phone will, for example, be visible to a retailer operating a wireless network when I come within range of that network. The MAC address will be used by that wireless network when I connect to access the Internet or network services of that retailer.

Each device has a unique MAC address (leaving aside counterfeiting and spoofing). Therefore, the MAC address for the device may be harnessed as a unique identifier for more than network functionality when it is visible or when an application installed on my device inspects and relays the MAC address. So, a MAC address could be a potential gateway to collecting information on the activities of users of that device when connected to the Internet. I referred to "users" because even though there is probably only one user of my smartphone, the same may or may not be true for any family's laptop and other devices.

A MAC address can also be used as a tool in tracking the movements of the device. For example, Wi-Fi access points will have a MAC address that can be mapped geographically. When a device (such as a smartphone, tablet or laptop) interacts with a Wi-Fi network, the MAC address for that device will also be visible, thereby permitting anyone interacting with the device to determine the location of the device, provided that that person (a) knows the location of the Wi-Fi access point and (b) can see the MAC addresses of the access point and the device.

What is an IP address?

An Internet Protocol ("IP") address is a numerical label that is assigned to an addressable connection to the Internet. The IP address is also part of the addressing system (at a higher level than the MAC address). It is used in routing packets of information over the Internet. Again, I am not a technologist but my understanding is that, for most consumers, the IP address is probably not static or permanently assigned to their device. Instead, the IP address will be dynamic. The consumer's Internet service provider ("ISP") will assign an IP address for a period of time, which might be reassigned to someone else after the consumer disconnects. However, an ISP is able to correlate the IP address at a specific date and time to a subscriber to whom it is providing Internet service access, assuming it retains that information.

The issue gets a bit tricky when a wireless network router is involved. Consider my home wireless network as an example. The router gateway to the ISP may be assigned an IP address by the ISP. That IP address may be changed from time to time. Each device connected to the home network will each have an individual IP address internally to the network system.

What's personal information?

Personal information is defined in most Canadian private and public sector privacy legislation as *information about an identifiable individual*.[2] There are some exceptions and variations in wording, but that is the basic definition.

Although reasonable people can debate the point, one justification of privacy legislation—whether applicable to the private sector or the public sector—is that it is necessary to protect individuals from unreasonable surveillance. Indeed, there was a telling exchange at the FCC workshop mentioned at the outset of this article, when Pam Dixon said that the MAC address was personal information, since, after all, it could be *correlated* to an individual and be subject to a *subpoena*.

Unreasonable surveillance may be viewed as inimical to personal liberty and potentially used as a tool of manipulation or, in its worst form, oppression. Even when an organization engages in surveillance to advance the "public good" or passively, without seeking to manipulate, some view this as a significant intrusion, since the information obtained through that surveillance may be conscripted by the state for other purposes.

The problem that privacy advocates face is that the gateway concept of "personal information" as currently drafted in Canadian privacy legislation is probably too amorphous in many cases to constrain systematic surveillance in a coherent way.

For example, in *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*,[3] the Alberta Court of Appeal concluded that in order for information to be about an "identifiable individual," the person must be identifiable. As the court held, the information "must have some precise connection to one individual."[4] It must also relate to an individual rather than to an object. The court held: "Information that relates to objects or property is, on the face of the definition, not included."[5] In order to be "personal," the information must be about the individual—that is, directly related to the individual. Information did not become *personal* information simply by being associated indirectly with an individual through ownership. As the court held:[6]

> Information that relates to an object or property does not become information 'about' an individual, just because some individual may own or use that property. Since virtually every object or property is connected in some way with an individual, that approach would make all identifiers 'personal' identifiers.

So, a driver's licence is personal information in Alberta but a licence plate is not. The driver's licence is uniquely connected to a person. Indeed, the driver's licence card functions in Canada as an identification card—that is, government-issued identification. On the other hand, in Alberta, at least, a licence plate is connected to the vehicle and only linked through a database to an individual. Reasonable people can debate the Alberta decision and whether other appellate courts should follow when the issue arises.

So what's the answer?

In one sense, the answer is easy. The Office of the Privacy Commissioner of Canada considers that an IP address *may* constitute personal information *if* the IP address is associated with or linked to an *identifiable* individual.[7]

Similarly, in a commendable and comprehensive study of the issues, the Information and Privacy Commissioner of Ontario and Kim Cameron argue that MAC addresses, *as unique identifiers, may* be *linked* to individuals and, therefore, *may* constitute personal information.[8]

The precautionary principle suggests that organizations should treat MAC and IP addresses as personal information. However, in many (most?) cases, MAC and IP addresses may not be directly linked to individuals. An ISP will be able to associate the IP address to a home or business account but not (at least in the ordinary course) to any particular person using a device linked to the Internet, particularly if we are talking about my access to the Internet through a Wi-Fi system at a coffee shop. A MAC address does not disclose who actually has possession of the device. However, there is a greater *probability* of correlation between the owner of the device and the MAC address than there is of an IP address and an individual.

So we are back to where we always are with personal information. A MAC address or an IP address information is rarely going to be in and of itself information about an identifiable individual in the sense of having a precise connection and being directly related to an identifiable individual. It is the context of how the MAC address or IP address is combined with other information (or could reasonably be combined with other information) that has privacy advocates concerned. In each case, of course, if you knew and combined enough on-line and off-line information you might have enough data to make a highly probably guess about who was doing what and where. But the same could be said about a licence plate number.

So who was correct (from a Canadian perspective) at the FTC workshop? Both. In and of itself, a MAC address (and an IP address) are likely not personal information but they are rich gateways to the collection and the accumulation of data points that can transform them into personal information if privacy (anti-surveillance) measures are not built into the technologies using these addresses. Ultimately, what

is personal information is fundamentally determined by context. The debate will continue.

[1] <http://www.ftc.gov/bcp/workshops/inshort/index.shtml>.

[2] For example, without listing every statute, according to the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 2(1), "personal information" means information about an identifiable individual, but does not include […]; according to the *Privacy Act*, R.S.C. 1985, c. P-21, s. 3, "personal information" means information about an identifiable individual that is recorded in any form including […]; according to the *Personal Information Protection Act*, SBC 2003, c. 63, s. 1, "personal information" means information about an identifiable individual and includes employee personal information but does not include […]; according to the *Personal Information Protection Act*, SA 2003, c. P-6.5, s. 1(1)(k), "personal information" means information about an identifiable individual; and according to the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31, s. 2(1), "personal information" means recorded information about an identifiable individual, including […]. The Quebec definition is somewhat different—*An Act respecting the Protection of personal information in the private sector*, R.S.Q., c. P-39.1, s. 2 (Personal information is any information, which relates to a natural person and allows that person to be identified; Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier).

[3] [2011] AJ No. 338.

[4] *Ibid.* at para. 47.

[5] *Ibid.*

[6] *Ibid.* at para. 48.

[7] Office of the Privacy Commissioner of Canada, "Interpretations: Personal Information" (Ottawa, 2011-10-06), <http://www.priv.gc.ca/leg_c/interpretations_02_e.asp>.

[8] Ann Cavoukian and Kim Cameron, "Wi-Fi Positioning Systems: Beware of Unintended Consequences Issues Involving the Unforeseen Uses of Pre-existing Architecture" (Toronto: Information and Privacy Commissioner, June 2011), *e.g.*, at p. 1. June 2011 <http://www.ipc.on.ca/images/Resources/wi-fi.pdf>.