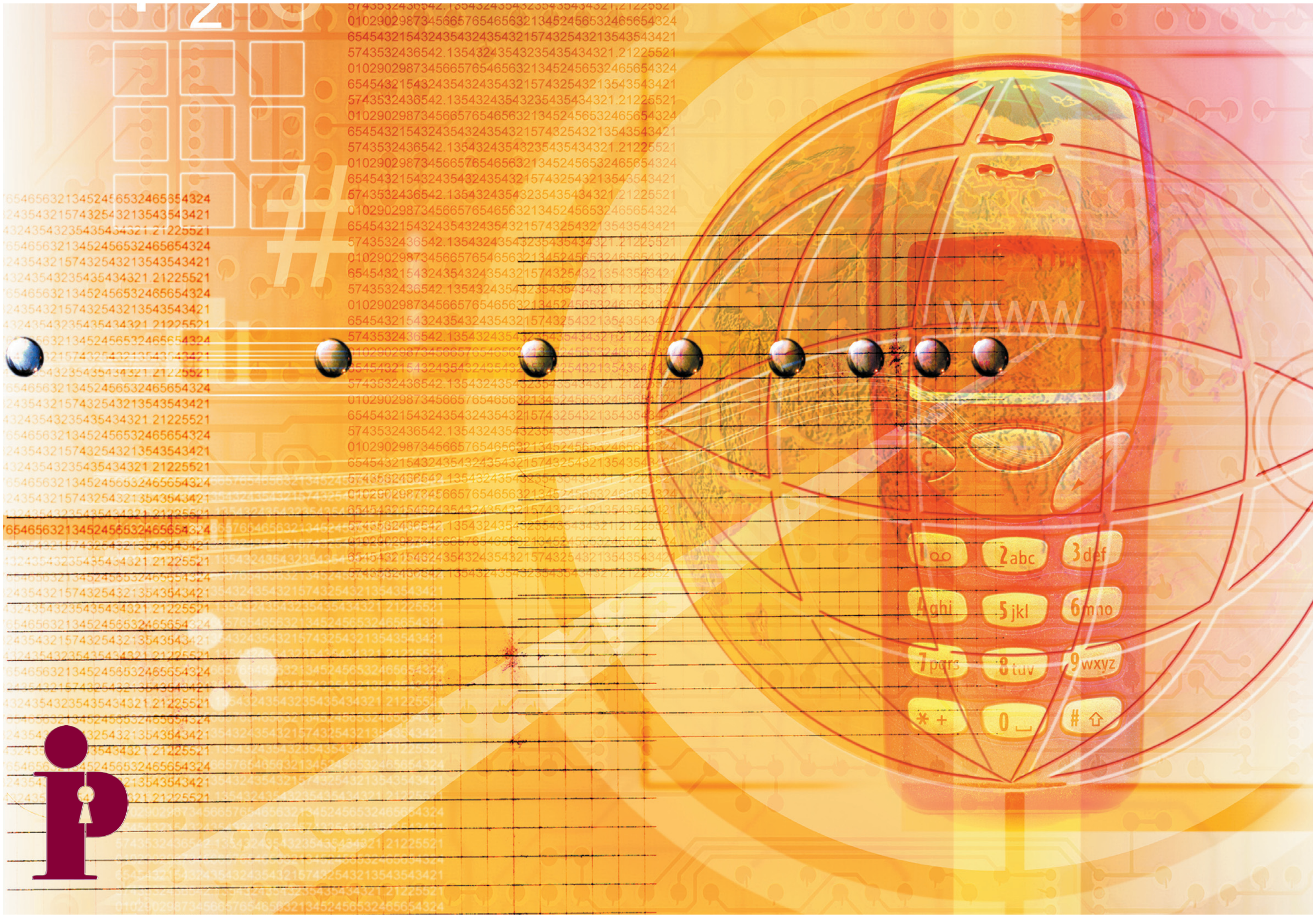
Wi-Fi Positioning Systems: Beware of Unintended Consequences

Issues Involving the Unforeseen Uses of Pre-existing Architecture

June 2011



A joint publication

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

Kim Cameron,
Identity Architect

Acknowledgements

The authors of this paper gratefully acknowledge the work of Michelle Chibba, Director of Policy, Catherine Thompson, Regulatory and Policy Advisor, and Vance Lockton, Policy Analyst, Ontario Information and Privacy Commissioner's Office, in preparing this paper.

The authors also wish to thank Ken Anderson, Assistant Commissioner (Privacy), at the Ontario Information and Privacy Commissioner's Office for his 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

Executive Summary

There are times when information architectures, developed by engineers to ensure the smooth functioning of computer networks and connectivity, lead to unforeseen uses that have an impact on identity and privacy. Against a backdrop of the popularity of smartphones and other mobile devices, there continues to be intense scrutiny of the capability of these mobile systems to track our lives, without our knowledge. The mobile ecosystem is extremely complex. It is no wonder that smartphone researchers state that "[t]oday's smartphone operating systems frequently fail to provide users with adequate control over and visibility into how third-party applications use their private data."[1] Often, these third parties operate outside of the telecommunications regulatory framework.

Smart mobile devices are required to perform a multiplicity of tasks: they operate via sophisticated geo-location software that enhances the end-user's mobile experience through a wide range of services relying on the device's location. To deliver these location services with greater speed and accuracy, Wi-Fi positioning systems (WPS) were established that rely on wireless access points for location coordinates. For the proper functioning of a wireless architecture, IEEE Project 802 defined a standard which assigns a Media Access Control (MAC) address to local area network devices. A wireless access point such as a router will be given a unique MAC address, as will Wi-Fi equipped laptops, mobile phones and even printers. An important and necessary feature of the MAC address, for the proper functioning of a wireless communications network, is that it be visible in communicated data frames, whether or not the wireless network is encrypted. In a WPS, the MAC address for a Wi-Fi access point becomes an index for a geo-location reference point. Companies known as location aggregators are building and/or maintaining databases of the MAC addresses of these Wi-Fi access points for commercial purposes, and provide access to third parties interested in location-based applications and advertising.

In this paper, we explore the identity and privacy issues that could arise from the unintended uses of the MAC address. Since the MAC address was designed to be persistent and unique over the lifetime of a Wi-Fi device, in a WPS, it identifies Wi-Fi devices that are closely associated with individuals – not only stationary routers, but personal laptops and mobile phones. When a unique identifier may be linked to an individual, it often falls under the definition of "personal information" through that data linkage and carries with it a host of regulatory responsibilities. The associated privacy issues range from lack of knowledge or consent of the mobile device owner for the use of the unique identifier, the possibility of unauthorized disclosure to third parties, or potential uses for secondary purposes.

The following observations and suggestions are made:

- Privacy is predicated on providing individual mobile device users with personal control, alongside openness and transparency on the part of the provider;
- In no case should the MAC address of an individual's mobile device be collected or recorded without the individual's consent;

[1] Full citation: William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth. *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*. Preceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation (2010) Vancouver B.C. USENIX .

- *Privacy by Design* is now the International Standard for privacy and should be considered at the outset, for a doubly-enabling outcome; therefore, engineers should use *Privacy by Design* as a standard to ensure that privacy is embedded into the architecture of various technologies and systems;
- When designing technical architecture, the potential for possible unintended uses should form part of a privacy threat/risk analysis;
- We must research and think creatively to find ways to embed privacy into Wi-Fi protocols that can randomize MAC addresses or ensure privacy through a proxy-like method of assigning addresses. Innovative solutions will be required to change the existing model of using persistent MAC addresses that remain uniquely bound to a mobile device.

Introduction

With over half of the world's population now owning mobile devices, location data are seen by service providers and advertisers as important profile elements for shaping and personalizing a user's mobile Internet experience. A new generation of 'smart' mobile devices is capable of running software applications and communicating with the web in ways that increasingly involve location data being established, shared and used (e.g. establishing your location on a map, checking the weather, and finding nearby points of interest), using Wi-Fi Positioning Systems (WPS).

Taking advantage of the rapid growth of wireless access points (Wi-Fi) in urban areas, WPS emerged as an idea to solve situations where GPS signals may be weaker, or where the use of GPS puts too much strain on the device's battery. By relying on Wi-Fi access points, WPS allows for more rapid and accurate determination of a given phone's location.

Despite the advantages to mobile phone users that WPS has introduced to this complex mobile ecosystem, recent events involving several major mobile platform operators have prompted increased scrutiny about the extent of location data collected by smart phones and disclosed to third parties who fall outside of the telecommunications regulatory environment.[2] This provides an excellent opportunity to explore other unforeseen implications of the popularity of Wi-Fi access points, including the associated architectural standards and protocols. Privacy is extremely important to individuals using mobile devices. In one survey, "98% of consumers expressed a strong desire for better control over how their personal information is collected and used via mobile devices and apps" – an unprecedented finding.[3]

This paper explores the unforeseen and unintended uses of pre-existing architecture involving the collection and use of Wi-Fi device identifiers to create Wi-Fi Positioning Systems. By advancing *Privacy by Design* as a methodology to ensuring that privacy is embedded into WPS architecture, we hope to raise awareness of identity and privacy issues among the tech community. As we begin to create the missing layer of identity on the Internet, "technologists will save a lot of trouble if [they] make [their] mobile location systems conform with reasonable expectations of privacy and security, *starting now*."[4]

[2] "House Presses Apple, Google, Others on Location-Tracking Practices." *The Wall Street Journal* (26 April 2011).

[3] TRUSTe. "Smart Privacy for Smartphones: Understanding and delivering the protections consumers want" (April 2011).

[4] Kim Cameron. *"I just did it because Skyhook did it"*. https://www.identityblog.com/?p=1105

The Unforeseen Uses of Pre-existing Architecture

The architecture of wireless communication networks involves standards and protocols for the seamless functioning of network components where computers must perform many tasks automatically. This includes the discovery of network services where packets must be sent to the network containing information that identifies the user's device to the network. [5]

The *Media Access Control Address*[6] (or, more commonly, MAC address) is an essential design feature for the proper operation of this architecture. The MAC address was created as an identifier for local area network devices by IEEE Project 802 in order to "identify items of real physical equipment, parts of such equipment, or functions that apply to many instances of physical equipment."[7] For example, a router on a network will have a MAC address assigned to it by the router's manufacturer,[8] as will any end-user device capable of connecting to that network. This includes devices that use Wi-Fi communications, such as wireless routers, laptop computers, and Wi-Fi-equipped cell phones, printers, and similar devices. Assigning unique addresses was an expedient way to allow hardware to be incorporated into any local area network without having to manage address collision.[9]

Here, it is important to note that MAC addresses associated with Wi-Fi access points and end-user devices are visible in communicated data frames, whether that wireless network is encrypted or not.[10] Only the frame body (payload) of data frames (Figure 1) will be encrypted when network encryption is turned on.

The *Service Set Identifier (SSID)* is an additional identifier for Wi-Fi access points (those devices, such as wireless routers, that provide Wi-Fi access to end-user devices). Often referred to as the 'network name,' this SSID is included in a 'management beacon,' which communicates to all nearby devices information about the network (connection speeds supported, identifiers, etc.). While the Wi-Fi Access Point's SSID broadcast feature can be disabled, the SSID will nevertheless appear in some of the management packets transmitted on that wireless network. [11]

[5] Tuomas Aura, Janne Lindqvist, Michael Roe and Anish Mohammed. *Chattering Laptops*. In *Privacy Enhancing Technologies, Lecture Notes in Computer Science*, ed. Nikita Borisov and Ian Goldberg. Vol. 5134. Berlin: Springer, 2008. p. 167-186.

[6] Also called Extended Unique Identifier or 'EUI-48', is a mix of numbers and the first six letters of the alphabet (e.g. 00-1F-3F-D7_3C-58).

[7] IEEE Standards Association. *Guidelines for Use of EUI*. http://standards.ieee.org/regauth/oui/tutorials/UseOfEUI.html (accessed January 13, 2011), p. 4.

[8] Stroz Friedberg. *Source Code Analysis of gstumbler: Report prepared for Google and Perkins Coie* (3 June 2010). http://www.google.com/googleblogs/pdfs/friedberg_sourcecode_analysis_060910.pdf (accessed January 13, 2011).

[9] IEEE Computer Society. *802 IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture* (2002).

[10] Prabhaker Mateti, "Hacking Techniques in Wireless Networks", in "The Handbook of Information Security", Hossein Bidgoli (Editor-in-Chief), John Wiley & Sons, Inc., 2005. http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm

[11] Ibid.

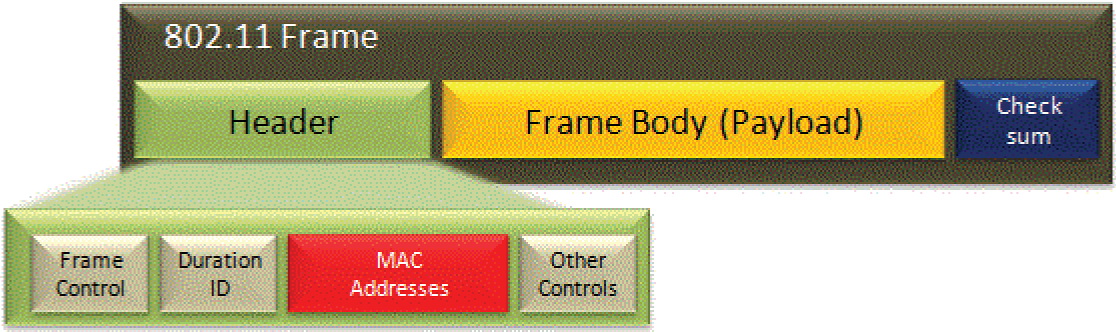


Figure 1 - Packets are encapsulated in frames which contains MAC addresses for source and destination devices [12]

The static and persistent nature of the MAC address, and its appearance in the clear in data frames, were choices made by engineers during the development of networking protocols. However, sometimes engineering choices made early on in the development of key information architectures, such as those meant to ensure the smooth functioning of computer networks (e.g. transmitting MAC address in the clear), can lead to unforeseen uses that impact on identity and privacy.

How the MAC Address IS Being Used: Wi-Fi Positioning Systems

A prominent way in which the MAC address is being used for purposes other than the support of networked communication is the development of Wi-Fi Positioning Systems. Geo-location services like interactive maps, navigation apps and those that link to social networks are increasingly popular on mobile devices such as smartphones. In addition, location and location history are seen by service providers and advertisers as important profile elements for shaping a person's mobile Internet experience. While several geo-positioning systems exist (e.g. GPS and cell tower calculation),[13] WPS has become an important geo-location tool in urban areas where GPS signals can be weaker or where the use of GPS puts too much of a strain on the mobile device's battery. Companies such as Apple, Google, Microsoft, RIM, Skyhook and others are in the process of building and/or maintaining these systems.

WPS functions by mapping the locations of Wi-Fi access points, indexed by their MAC addresses, and comparing these against the access points visible to an end-user device to determine the device's location. A vast array of these access points has been constructed by individuals and businesses, in addition to the 'hot spots' available in airports, hotels, coffee shops, public libraries, etc. Numerous municipal projects have also been completed or are underway to bring Wi-Fi accessibility to entire cities (Figures 2, 3).

[12] Kim Cameron. *Gstumbler tells all*. http://www.identityblog.com/?p=1120

[13] See Appendix B for an overview of major positioning systems.

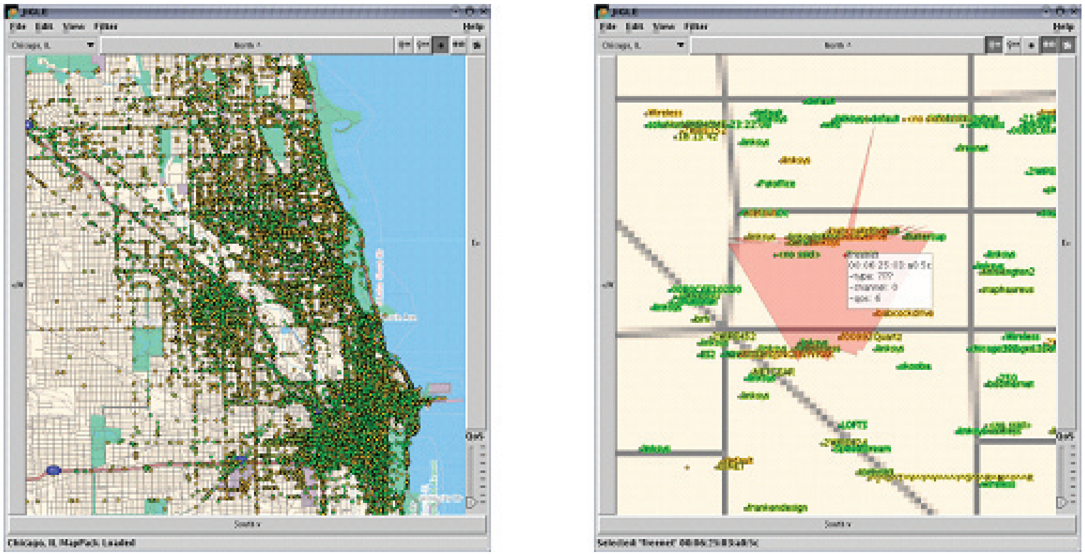


Figure 2 illustrates Wi-Fi access points in downtown Chicago. Figure 3 is a zoomed in frame of streets in Chicago showing SSID names.[14]

WPS can be divided into two primary stages: the collection of MAC addresses of Wi-Fi access points and their associated locations into a database, and the use of this database to locate end-user devices. Though these two functionalities will, in practice, occur simultaneously and inform each other, for clarity we will separate the two in the discussion that follows.

Collecting and Locating Wi-Fi Access Points for a WPS Database

The initial mapping of Wi-Fi access points is a resource-intensive task, as the mapping device must pass through the relatively limited signal range of each access point. Thus, in order to create (or update) a database of these locations, organizations will often turn to a technique called 'wardriving.' Wardriving refers to the practice of searching a target area for Wi-Fi networks using a portable computer or PDA, generally while travelling by car (though 'warwalking,' 'warbiking,' and other similar techniques may also be used). When the computing device detects a wireless network, it collects the MAC address (and potentially the SSID) of the access point, associates this with the location (usually determined by GPS or other automated means) and signal strength of the detected network, and uploads the entire record to a database.

The collection of MAC addresses from Wi-Fi access points can be achieved in two ways – active and passive scanning.[15] Active scanning involves sending out a probe to nearby access points and recording the network access device identifiers (e.g. the wireless router MAC address and SSID)[16]. Passive scanning records the periodic beacon frames (or, potentially, other type of frames) transmitted by each wireless access point. Those who build WPS databases for commercial purposes by geo-tagging Wi-Fi access point data are dubbed "location aggregators." These aggregators provide third parties with access to their WPS databases for location-based application development and advertising.

[14] Images from http://wigle.net/gps/gps/main/screenshots/

[15] Article 29 Data Protection Working Party. Opinion 13/2011 on Geolocation Services on Smart mobile devices (adopted on 16 May 2011), p. 6.

[16] "Active software like NetStumbler, dStumbler, and MiniStumbler actually broadcast probe request frames to elicit responses from APs." Yu-Xi Lim, Tim Schmoyer, John Levine, and Henry L. Owen. Wireless Intrusion Detection and Response. Proceedings of the 2003 IEEE, Workshp on Information Assurance, United States Military Academy. West Point, NY, June 2003. http://users.ece.gatech.edu/owen/Research/Conference%20Publications/wireless_IAW2003.pdf (accessed January 25, 2011), p. 69.

Recall that owners of Wi-Fi networking equipment are not provided the ability to opt-out of the collection of the access point's MAC address. There has been some discussion that as MAC addresses are in plain view, this information should be considered public, and thus freely accessible – even though such use would be outside of its intended use and context, of directing network transmissions.

The discussion of whether publicly observable facts constitute information for which a person has a reasonable expectation of privacy is not new. Researchers have argued that there should be a distinction between data that is observable in public versus data in public that is recorded. Recorded data of public actions and movements that are otherwise observable only by others occupying the same public space have been argued to be deserving of privacy protection. It is argued that a distinction should be drawn between observable location information and recorded location information because the latter is often better quality, and more revealing[17]. In the context of a cell phone conversation, for example, "[t]he recorded data will also reveal the identities of the caller and of the recipient of the call" which "goes well beyond what could be observable by bystanders."[18] Records, as opposed to observations, are concrete, precise, potentially permanent, and may easily be analyzed and combined with other information.[19]

The potential for unintended uses of the MAC address increases significantly if additional data is added to that captured by a WPS system. Identifying, classifying, and storing information about uniquely identified devices in WPS databases raises the possibility for data linkage. Data, and databases, cannot be considered in isolation; in fact, it is frequently in combination with other information that data will become a significant privacy concern. It is known, for instance, that multiple services exist which can convert any numerical location (such as latitude / longitude) of a Wi-Fi access point to an identifiable location (an address, for instance). Once this has been established, the address could be combined with White Pages information (if the location is a house) to infer the name of the access point's owner.

Some passive scanning techniques used by wardrivers may also be capable of recording all Wi-Fi frames, not just broadcast beacons. Even setting aside the issue of potential capture of payload data, for each data frame captured, the MAC address of both the Wi-Fi access point and the end-user device are present – and it is not clear whether location aggregators distinguish between the two. According to the European Article 29 Data Protection Working Party, "If this type of scanning is done without proper application of privacy by design, it can lead to the collection of data exchanged between access points and the devices connected to them. This way, the MAC addresses of desktop computers, laptops and printers could be recorded."[20] Not only is this type of collection possible, it is occurring: in a recent investigation of a Wi-Fi collection incident, the French National Commission on Informatics and Liberties found that, not only were MAC addresses for Wi-Fi access points collected, but also MAC addresses of devices that were connected to those access points, including smartphones.[21]

[17] As acknowledged by the European Court of Human Rights: "Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain." European Court of Human Rights, Judgement of 25 September 2001 (*PG and JH v. The United Kingdom*) no. 44787/98, at 57.

[18] Teresa Scassa. *Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy* (2009). Canadian Journal of Law and Technology, p. 2-28, p. 11.

[19] Ibid.

[20] Article 29 Data Protection Working Party. Opinion 13/2011 on Geolocation services on smart mobile devices (adopted on 16 May 2011), p. 6.

[21] Délibération n'2011-035 de la formation restreinte prononçant une sanction pécuniaire a l'encontre de la société Google Inc. *Commission Nationale de L'Informatique et des Libertés* (CNIL), (17 Mars 2011) :« ...les Google cars enregistraient non

Passive scanning that captures the MAC address of an end-user device in a frame transmitted to a Wi-Fi access point creates a clear association between the two devices – particularly if frames containing the same access point and end-user device MAC addresses are collected on multiple distinct occasions. If the location of the Wi-Fi access point is a home, it is likely that the end-user device owner lives at that location (and, as we have previously established, his or her name may also be known). If the Wi-Fi access point corresponds to a place of business, it is likely that the end-user device owner is employed at (or at least frequently visits) that location. With sufficient resources to frequently sample data frames, it may even be that the same end-user device can be associated with multiple locations, creating an effective profile of the device's (and, by association, its owner's) movements.

Recall, however, that for a small enough target area, 'sufficient resources' to frequently sample data frames may involve only a car, a laptop computer, and freely available software. For instance, an individual (for clarity, we call him 'Bob') could drive up and down the streets of a neighbourhood each evening (at a time when residents are likely to be home) and quickly compile a database of the MAC addresses of most of the Wi-Fi enabled phones and computers owned by the residents of that neighbourhood.[22] Extending this scenario, by setting up a wireless access point in a nearby park, Bob could then capture the MAC address of nearby people carrying Wi-Fi enabled phones – which could then be compared against the database Bob collected earlier to determine the home addresses of those individuals. In this way, Bob can determine personal information (address and potentially name, via White Pages) of a person who, prior, would have been a stranger passing by in a public location – and he can do so without that person's consent or knowledge.

It is important to understand that the privacy and data rules that apply to telecommunications companies may not cover the collection of WPS data. Telecommunications companies have always been able to locate devices to provide telecommunications coverage under a regulated environment; this tracking is network-based.[23] However, many new location-based services, such as WPS, are enabled by third parties who fall outside of this regulatory environment, which again introduces new privacy issues. For example, U.S. law requires a telecommunications carrier to obtain customer approval before using, disclosing or providing access to "customer proprietary network information" which includes location information and phone numbers.[24] However, Wi-Fi location technology providers may not necessarily be considered a telecommunications carrier.[25]

In the U.S., it has been recommended that several laws be updated in light of Wi-Fi technologies, including the *Electronic Communications Privacy Act*, and the *Telecommunications Act* ('CPNI Rules').[26] As early as 2004, the International Working Group on Data Protection in Telecommunications also raised this same issue:

seulement les adresses MAC des points d'accès Wi-Fi, mais aussi les adresses MAC de l'ensemble des terminaux connectes a ces points d'accès (ordinateurs personnels, imprimantes et autres périphériques, *smartphones*, etc.)» p. 11-12.

[22] Kim Cameron. *What harm can possibly come from a MAC address?* http://www.identityblog.com/?p=1111

[23] In Canada, as of February 1, 2010, and pursuant to Telecom Decision 2003-53 and Telecom Regulatory Policy CRTC 2009-40 the CRTC generally requires that all Canadian wireless service providers implement a form of wireless enhanced 9-1-1 (E9-1-1) service whereby the telephone number, cell site/sector information, and longitudinal and latitudinal information regarding the location of wireless E9-1-1 callers are automatically conveyed to the appropriate E9-1-1 call centre or public safety answering point.

[24] Telecommunications Act of 1996 § 222(c); see also §222(d) for exceptions, including for emergency services. N King. *Direct marketing, mobile phones, and consumer privacy: Ensuring adequate disclosure and consent mechanisms for emerging mobile advertising practices* (2008). Federal Communications Law Journal 60: p. 229.

[25] Testimony of M Altschul before the *Committee on Energy and Commerce*, House of Representatives (24 February 2010), p.3.

[26] Testimony of J Morris before the Committee on Energy and Commerce, U.S. House of Representatives (24 February 2010), p. 6-10; See also Peter Schaar, Federal Commissioner of Data Protection. *Smart phones always under control?* http://www.bfdi.bund.de (9 July 2010) for a similar issue in Europe.

> … mobile electronic commerce will lead to the creation of a wealth of new services based on knowledge about the more precise location of the user. However, such services will most likely not only be provided by telecoms operators, but also by third parties which may not be legally bound by the restrictions of telecommunications secrecy.[27]

Locating End-User Devices with a WPS Database

Once a sufficient number of Wi-Fi access points have been uploaded to a location database, this information can be used to locate end-user devices. When an end-user device uses a WPS service to request its location, it first identifies Wi-Fi access points in its range. After submitting of the MAC addresses of these points to the WPS database, the known positions of one or more of these points is retrieved, allowing the device's location to be triangulated. The accuracy of WPS thus depends on the number of Wi-Fi access points entered into the reference database. Skyhook's WPS localization service for instance, requires a five-step process:[28]

1) The end-user's mobile device with Skyhook's location software broadcasts a probe and requests frame data on all nearby Wi-Fi access points;

2) Wi-Fi access points reply to the device with a beacon containing that Wi-Fi access point's frames, including MAC addresses;

3) The device collects the beacons and associated signal strengths, and sends the collected MAC addresses via encrypted channel to the WPS database (this requires that the device be connected to the Internet);

4) The WPS database compares the MAC addresses sent by the device to the MAC addresses stored in the database. It then returns the location of those MAC addresses to the device in encrypted form;

5) The device determines its position based on the information received using a proprietary algorithm.

[27] International Working Group on Data Protection in Telecommunications. *Common Position on Privacy and location information in mobile communications services* http://www.datenschutz-berlin.de/attachments/193/local_neu_en.pdf?1177594792 (accessed March 31, 2011)

[28] N O Tippenhauer, K B Rasmussen, C Popper, and S Capkun. *Attacks on public WLAN-based positioning systems* (2009) MobiSys'09. *June 2009, Krak´ow, Poland*, p. 30. http://www.it.uu.se/edu/course/homepage/datakom2/vt10/papers/wlanattacks-mobisys09.pdf (accessed January 25, 2011);,

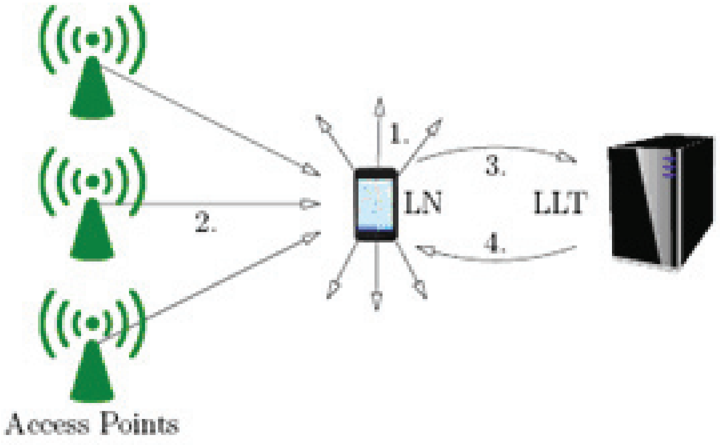


Figure 4 illustrates the five phases of a location aggregator's WPS localization process[29]

These queries can also be used to update and/or refine the WPS location database, as any access point that is either not in the database, or which was previously associated with a different geographic location, will be identified during this process and the point's new location calculated. In this way, the updating the network of reference points can be crowdsourced, making the WPS database 'self-healing.'

As with Wi-Fi access point owners, owners of end-user devices may not be aware of the data being disclosed by their devices, or may not wish to have their location queries used to update a commercial database. As such, there are privacy concerns which may arise in the construction of WPS databases.

In addition, if a location aggregator assigns a unique identifier to each querying device, the company may be able to create a profile of a user's movements.[30] Detailed location data collected in real time is said to introduce a new dimension to the collection of location data.[31] It is predicted that "constant accessibility, visibility, and exposure" will confront traditional notions of "personal space and boundaries, and the privacy expectations that accompany them."[32] Questions are also being raised about the impact of location-based technologies on the separation between the public and private spheres, and the shift in concept of 'movement' as a means of avoiding surveillance to 'movement' as being the subject of surveillance.[33] For example, location information stored on service provider servers may be retained and accessed, whereas in the past such information

[29] Ibid. Acronyms LN and LLT refer to 'localized node' and 'location lookup table.'

[30] Some aggregators explicitly state that they do not track users in this manner. For example, "Skyhook CAN NOT, DOES NOT and WILL NOT track your location", http://www.skyhookwireless.com/howitworks/privacypolicy.php; "Microsoft doesn't store or use any unique device identifiers … that would allow tracking or creating a location history of your device in connection with Microsoft's location services", http://www.microsoft.com/windowsphone/en-us/howto/wp7/web/location-and-my-privacy.aspx; "Apple is not tracking the location of your iPhone. Apple has never done so and has no plans to ever do so" http://www.apple.com/pr/library/2011/04/27location_qa.html

[31] See generally, ACLU of Northern California. *Location-Based Services: Time for a Privacy Check-in*. (November 2010). www.dotrights.org. Office of the Information and Privacy Commissioner. *Privacy in a Wireless World* (2002). http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=334 (accessed April 15, 2011). The Surveillance Project. *Location Technologies: Mobility, Surveillance and Privacy* (2005). http://www.sscqueens.org/research/loctech (accessed January 18, 2011).

[32] Anne Uteck. *Ubiquitous Computing and Spatial Privacy*. In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, ed. Ian Kerr, Valerie Steeves and Carole Lucock. Oxford: Oxford University Press, 2009. http://idtrail.org/content/view/799 (accessed January 13, 2011). , p. 83

[33] Colin Bennett and Priscilla Regan. *Surveillance and Mobilities* (2004). Surveillance & Society 1(4): p. 449-455; Sjaak Nouwt. *Reasonable Expectations of Geo-Privacy?* (2009). SCRIPTed, 5(2): p. 398.

would not be available.[34] Access to such location data raises concerns, especially if the location visited (e.g. HIV clinic) can reveal damaging and perhaps embarrassing information, or lead to discrimination. These concerns can be exacerbated should other information be collected from the end-user device. For instance, a company called BlueCava "fingerprints" devices to match individuals with online advertisers based on their behaviours and has done so for approximately 200 million devices. BlueCava anticipates that it will identify about one tenth of all devices in the world, and is considering matching device profiles with off-line information, such as publicly available property and vehicle registration records.[35]

When companies have a 'privacy by disaster' mindset in which privacy protections are only built, or practices explained, after a significant incident, the fallout can be damaging and very public. Consider the significant media and public scrutiny generated as a result of the recent study showing that Apple's iPhones, iPads and Google's Android phones record location information.[36] This resulted in several companies appearing before a U.S. House of Representatives Committee Hearing, having to explain their data collection and usage practices.[37] During these hearings, RIM stated in a letter to the House that its geolocation database is "built using a collection of GPS, cell tower and Wi-Fi access point information that is regularly collected, transmitted and deleted from BlackBerry SmartPhones," but that this database did not personally identify users.[38] Reports also indicate that Microsoft's Windows Phone 7 transmits information including device unique ID, Wi-Fi and GPS coordinates.[39]

Although transparency and notice vary widely among the mobile device operating system developers, there were criticisms that such disclosure to users is not direct or meaningful (see Figure 5).[40] One of the key messages associated with criticisms of the above practices was not that the location transfer was occurring, but that it was occurring *without sufficient transparency and informed consent from the user.*

[34] Nouwt, p. 402.

[35] J Angwin and J Valentino-Devries. *Race Is On to 'Fingerprint' Phones, PCs*. The Wall Street Journal (30 November 2010).

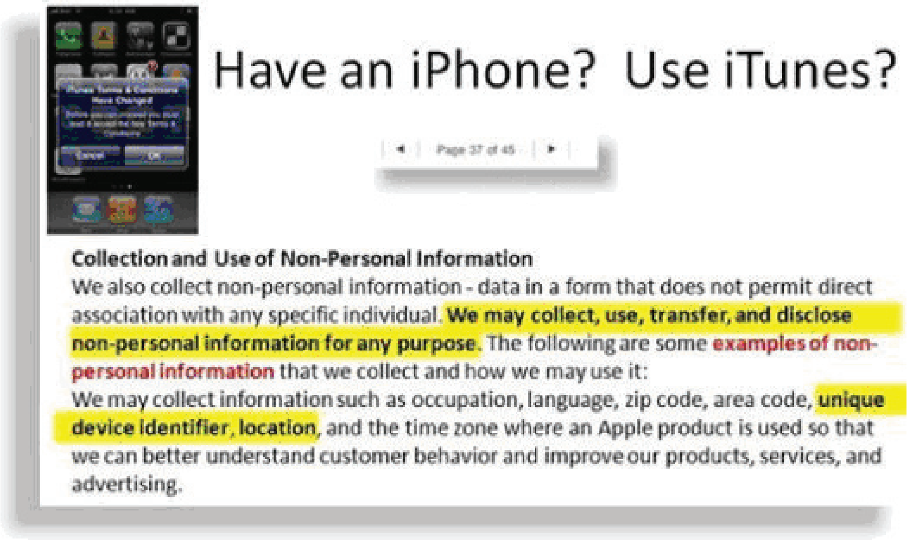
[36] Alasdair Allan and Peter Warden. "Got an iPhone or 3G iPad? Apple is recording your moves." http://radar.oreilly.com/2011/04/apple-location-tracking.html

[37] "House Presses Apple, Google, Others on Location-Tracking Practices." *The Wall Street Journal* (26 April 2011). See also McCullagh, Declan. "Android data tied to users? Some say yes." *CNET News*.(22 April 2011).

[38] RIM - Letter to Honorable Fred Upton, May 9, 2011. http://republicans.energycommerce.house.gov/Media/file/Letters/050911rim.pdf.

[39] McCullagh, Declan. "Microsoft collects locations of Windows phone users." *CNET News* (25 April 2011).

[40] Tara Whalen, Office of the Privacy Commissioner of Canada. "Position Statement. Making Tracks: Mobile Devices, Surveillance, and Geoloaction Privacy", April 2011. http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Whalen-Making-Tracks.pdf



Have an iPhone? Use iTunes?

Collection and Use of Non-Personal Information
We also collect non-personal information - data in a form that does not permit direct association with any specific individual. **We may collect, use, transfer, and disclose non-personal information for any purpose**. The following are some **examples of non-personal information** that we collect and how we may use it:
We may collect information such as occupation, language, zip code, area code, **unique device identifier**, **location**, and the time zone where an Apple product is used so that we can better understand customer behavior and improve our products, services, and advertising.

Figure 5 – Example of a privacy policy allowing for the disclosure of unique device ID detailed at page 37 and 45 of the policy.[41]

The 'Unknowing Informant Model'

Under the crowdsourced database updating model, it is known that users of WPS services may unwittingly be aiding the proprietor of the service to update and refine their database, based on the list of Wi-Fi access point MAC addresses submitted with each query. This model may not concern everyone – after all, it leads to improvement in the service's locating capabilities. But consider if even more information was being provided to the WPS service? For instance, suppose it were the case, when a mobile user was querying for location, that he or she was also able to unknowingly detect the MAC addresses of mobile devices in range in addition to Wi-Fi access points.

The initial user's device may then relay the MAC addresses of friends, family members, and co-workers, turning him or her into an 'unknowing informant,' revealing the location of others, who are not necessarily participating in location-based services.[42] Associating the MAC addresses of other people's devices with the calculated location of the informant may potentially reveal the home, workplace, conference attendance, or business client location of others.[43] These individuals may have explicitly opted-out of location tracking – but if their MAC addresses (static, unique identifiers for each phone) remain visible to another mobile device, then their locations may be reported to a WPS service, regardless.

In the above unintended use case scenarios, the MAC address becomes more than simply a device identifier. Instead, it identifies devices that are closely associated with people – including their personal computers and mobile phones. These identifiers are persistent, remaining constant over

[41] Kim Cameron. *Apple giving out your iPhone fingerprints and location*. http://www.identityblog.com/?p=1136 (accessed January 18, 2011). Consumers have privacy concerns regarding the sharing of their location information, and can be confused about who they should get in touch with regarding these concerns. Federal Trade Commission. *Beyond Voice: Mapping the Mobile Marketplace* (2009), p. 16. http://www.ftc.gov/reports/mobilemarketplace/mobilemktgfinal.pdf (accessed January 25, 2011). Privacy policies tend to be vague, including regarding the possibility of third parties combining their data with other data about them. See *Gratton*.

[42] Kim Cameron. *Harvesting phone and laptop fingerprints for its database*. http://www.identityblog.com/?p=1133 (accessed January 19, 2011); OPC, at 27: "Google stated that it cannot accurately distinguish between WiFi networks and wireless devices. It can, however, identify the unique number of basic service set identifiers (a.k.a. BSSIDs), which generally identify a single WiFi access point. Although the BSSID does identify an access point, it does not indicate how many devices or networks connect through the access point."

[43] Ibid.

the lifetime of the device. They are "identifiers that are extremely reliable in establishing identity by virtue of being in people's pockets or briefcases."[44] They become, in turn, that is, personal identifiers – and, due to the static nature of the MAC address, they are identifiers that tend not to change for the life of the device.

In a recent opinion, the Article 29 Working Party[45] concluded that geolocation data constitutes private data. Peter Hustinx, Europe's Data Protection Supervisor (EDPS), and member of the working group noted, "location data is certainly, in many instances, private data, and there then follows the obligations to inform users, and the opportunity to opt in or opt out." Similarly, in the U.S., there are a number of bills that, among other things, expand the definition of personal information to include, for example, "unique identifier information." This term could mean "a unique persistent identifier associated with an individual or a networked device, including a customer number held in a cookie, a user ID, a processor serial number, or a device serial number."[46]

The MAC address is not alone in its status as a static, unique identifier that has been inadvertently used for unintended purposes. For instance, an analysis of the data transmitted from applications installed on iPhones and iPads showed that 68 per cent of applications transmitted the iOS Universal Device Identifier (UDID), a 40-digit unique serial number, to vendor controlled servers, each time the application was launched.[47]

[44] Kim Cameron. *The Laws of Identity smack Google*. http://www.identityblog.com/?p=1100 See also, Peter Scharr, *Smart phones always under control?*: "Additionally, smart phones often transmit current characteristic data of surrounding WLANs to the service provider so that the corresponding WLAN-data bases can be appropriately supplemented and updated. In this way, the smart phone user will become – without his knowledge – the data collector for service providers."

[45] Article 29 Data Protection Working Party. Opinion 13/2011 on Geolocation services on smart mobile devices (adopted on 16 May 2011). 881/11/EN WP185.

[46] John Kerry Website. "Commercial Privacy Bill of Rights." http://kerry.senate.gov (accessed May 17, 2011). Kim Cameron notes that "This clear and central statement marks a real step forward. Amongst other things, it covers the MAC addresses of wireless devices and the serial numbers and random identifiers of mobile phones and laptops."

[47] Smith, Eric. "iPhone Applications & Privacy Issues: An Analysis of Application Transmission of iPhone Unique Device Identifiers (UDIDs)" (1 October 2010). http://www.pskl.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf

Privacy by Design – Identifying and Avoiding Unintended Uses

The popularity of Wi-Fi networks, in combination with the clear text transmission of identifiers for those networks, creates a ubiquitous infrastructure that may now be used for purposes far different from the original intent.[48] The MAC address and SSID were first developed to ensure the proper functioning of wireless network components; they can now act as geo-location points, enabling location-based services and mobile virtual communities thereby transforming the original intention of the architecture.[49] When designing a technical architecture, the potential for unintended uses should form part of a privacy threat/risk analysis. This is fundamental to the future of computing, where attempts to prevent user tracking are often not seriously pursued.[50]

In 2004, the International Working Group on Data Protection in Telecommunications called on the IEEE, the Wi-Fi Alliance and wireless product vendors "to give data security and privacy matters a high priority in the current and future developments of wireless technology."[51] The Working Group also developed a 'Common Position on Privacy and Location Information in Mobile Communications Services' which was adopted by International Data Protection Commissioners.[52] Among the principles enumerated in the Common Position was the following view: "Precise location information should not normally be generated as a standard feature of the service, but only 'on demand' where it is needed to provide a certain service that requires knowledge of the location of the user's device."[53]

Efforts are underway to define acceptable protocols for the collection, use and disclosure of location data in Internet applications,[54] and efforts specifically in the area of mobile devices are expected to draw on existing protocols defined in this area.[55] There is also great interest by governments to understand current practices regarding the collection, use and disclosure of location data.[56] In addition, there are industry efforts to apply privacy to the mobile applications environment.[57]

[48] For instance, De Montfort University in the United Kingdom is considering the use of their on-campus Wi-Fi networks, in combination with chips in ID cards, to track student attendance. Leicester Mercury, June 6, 2011. "Students' concern over 'Big Brother-style' surveillance" http://www.thisisleicestershire.co.uk/Students-concern-Big-Brother-style-surveillance/story-12718136-detail/story.html

[49] International Working Group on Data Protection in Telecommunications (IWGDPT). *Common Position on privacy and location information in mobile communications services*. (19 November 2004): "The enhanced precision of location information and its availability to parties other than the operators of mobile telecommunications networks create unprecedented threats to the privacy of the users of mobile devices linked to telecommunications networks."

[50] Eric Rescorla. *Can We Have a Usable Internet Without User Trackability?* (5 November 2010). http://www.educatedguesswork.org/iab-privacy.pdf (accessed January 19, 2011).

[51] (IWGDPT). *Working Paper on potential privacy risks associated with wireless networks* (15 April 2004). This paper was adopted at the 35th meeting of International Data Protection Commissioners in Buenos Aires.

[52] (IWGDPT). *Common Position on privacy and location information in mobile communications services*. (19 November 2004).

[53] IWGDPT, *Common Position on privacy and location information in mobile communications services*, Principle 2.

[54] E.g. see Geographic Location/Privacy (geopriv). http://datatracker.ietf.org/wg/geopriv/charter/ (accessed January 19, 2011); Geolocation Working Group http://www.w3.org/2008/geolocation/ (accessed January 19, 2011).

[55] Nick Doty, Deirdre K. Mulligan, and Erik Wilde. *Privacy Issues of the W3C Geolocation API* (2010). UC Berkeley School of Information Report 2010-038. http://escholarship.org/uc/item/0rp834wf (accessed March 31, 2011)., p. 13.

[56] E.g. House of Representatives Committee on Energy and Commerce hearing on *The Collection and Use of Location Information for Commercial Purposes* (24 February 2010).

[57] Privacy Design Guidelines for Mobile Application Development, GSMA. http://www.gsmworld.com/our-work/public-policy/mobile_privacy.htm

In taking these steps, it is clear that it is essential to infuse privacy as a value into protocols for location-based technology in the wireless mobile ecosystem. Numerous examples exist in other fields demonstrating that privacy can be embedded right into the architecture of various technologies and systems.[58] The incentive to adhere to the higher standard of *Privacy by Design* is to avoid having to add privacy requirements at a later date, when it will be far more expensive and less effective to do so. If systems are built without respect for user privacy, and adhere to only the most basic requirements, companies may suffer when their systems are compromised or when a large base of customers reacts negatively. No company *in any industry* wants to learn about privacy problems on the front page of a major newspaper, and no company wants to jeopardize a customer relationship due to a lack of trust.

Privacy by Design is a concept developed back in the '90s, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.[59] It 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. 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 7 Foundational Principles of *Privacy by Design*: 1) Proactive not Reactive; Preventative not Remedial; 2) Privacy as the Default Setting; 3) Privacy Embedded in the Design; 4) Full Functionality – Positive-Sum, not Zero-Sum; 5) End-to-End Security – Full Lifecycle Protection; 6) Visibility and Transparency – Keep it Open; 7) Respect for User Privacy – Keep it User-Centric.

In the case of MAC addresses and Wi-Fi Positioning Systems, creative thinking must be employed to find ways of embedding privacy directly into the architecture. Jacques Bus, the former Head of Unit for the European Commission's Information and Communication Technologies (ICT) Research Programme, states, "Technology solutions, like developing Wi-Fi protocols that appropriately randomize MAC addresses and also protect other personal data, are also needed urgently to enable development of trustworthy solutions that are competitive and methods should be sought to standardize such results quickly."[60]

There are many players in the mobile space who have a contributing role to ensuring end-to-end privacy, whether it is the device manufacturer, the operating system and platform developer, network providers, application developers, data processors and even users themselves.[61] Working with the broader research community, location aggregators and location-based technology and application developers should research and implement alternatives that protect the privacy of individuals, and provide individuals with a choice in whether their devices can be used in the creation and updating WPS architecture.

[58] See the following book: Information and Privacy Commissioner, Ontario. *Privacy by Design … Take the Challenge*. http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf

[59] Dr. Ann Cavoukian, *Privacy by Design*.(January 2009) http://www.ipc.on.ca/images/Resources/privacybydesign.pdf

[60] *Trusting Mobile Technology*. http://www.identityblog.com/?p=1147 (accessed January 19, 2011); See also Tang et al, p. 5: "If a WiFi-based application is continuously making queries of the form '*I can see access point 00-0C-F1-5C-04-A8, what is my location*?', then it is continuously disclosing the person's location. In Place Lab, this is addressed by the local storage of a database mapping WiFi access points to GPS coordinates. An application can therefore infer its location by checking this local database, without sending a query to a server."

[61] ASU Privacy by Design Research Lab and Information and Privacy Commissioner, Ontario Canada. *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users*. http://www.ipc.on.ca/images/Resources/pbd-asu-mobile.pdf

The linking of information is a major concern when combining MAC address, IP address and location information, and combing this information with other details about individuals. However, a *Privacy by Design* approach seeks to prevent such associations from being possible in the first place.[62] Research already performed to protect, shield and minimize location data should be reviewed (e.g. location fuzzing or obfuscation, ambient notices, two-way communication for privacy notices and consent, user-generated identifiers, substitution of MAC addresses, cloaking, changing identifiers in mix zones, etc).[63]

By taking a *Privacy by Design* approach, WPS architects will ensure that they apply sufficient protections to ensure the future viability of invested resources. In particular, transparency and visibility are imperative. Location aggregators must be transparent about what they are collecting and the purposes for collecting, using, and matching data with other data. The individual must also be provided with granularity of choice regarding all of the practices regarding the provision of MAC address and SSID for location-based services. There is some concern that it may not be presented as an option to users wanting location-based service whether to participate in WPS crowdsourcing, or that such updating could occur when location services are not being requested.[64] For example, it should be clear whether one's device's ID is being "fingerprinted."

The use of location-based applications that rely in whole or in part on WPS is still in nascent stages, making it the perfect time to incorporate *Privacy by Design* – before these issues create large-scale consumer concern. Now is the critical time for *Privacy by Design* to be applied. Failing to be transparent is unacceptable to users, and requires careful thought in collecting Wi-Fi access point data, whether through war driving, or from individuals' mobile devices requesting location-based services.[65] In no case should the MAC address of end-user devices be collected or recorded without the consent of the owner of such devices.[66]

[62] For example, research in the area of IPv6 is attempting to ensure privacy of IP address through a proxy-like method of assigning addresses. See Privacy Extensions for Stateless Address Autoconfiguration in IPv6. *RFC 4941*. http://tools.ietf.org/html/rfc4941. Note, this method could technically be used for IPv4 as well. See, for example, this international research project focused on mobile communities: Privacy and Identity Management for Community Services (PICOS). "The objective of the project is to advance the state of the art in technologies that provide privacy enhanced identity and trust management features…". http://www.picos-project.eu (accessed May 31, 2011).

[63] Aura et al.; Karen P. Tang, Pedram Keyani, James Fogarty, and Jason I. Hong. *Putting People in their Place: An Anonymous and Privacy-Sensitive Approach to Collecting Sensed Data in Location-Based Applications*. Conference on Human Factors in Computing Systems (CHI 2006). Montreal, Quebec; Marco Gruteser and Dirk Grunwald. *Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis* (2003). Proceedings of the AMC International Workshop on Wireless Mobile Applications and Services on WLAN (WMASH 2003), p. 46-55; Marco Gruteser and Dirk Grunwald. *A Methodological Assessment of Location Privacy Risks in Wireless Hotspot Networks*. In, *Lecture Notes in Computer Science*, 2004, Volume 2802/2004, p. 113-142; Qi He, Dapeng Wu, Pradeep Khosla. *The Quest for Personal Control over Mobile Location Privacy* (2004). *IEEE Communications Magazine*, p. 135: "An ideal way to remedy this is to replace the MAC address with the authorized-anonymous-ID. ID collision should not be a serious problem in this case and can be prevented in many ways, for instance, by adding a time stamp."; Marco Gruteser and Dirk Grunwald. *Anonymous Use of Location-Based Services through Spatial and Temporal Cloaking* (2003). Proceedings of the ACM Conference on Mobile Systems, Applications, and Services (MobiSys 2003), p. 31-42.; Tao Jiang, Helen J. Wang, Yih-Chun Hu. *Preserving Location Privacy in Wireless LANs* (2007). MobiSys'07, Proceedings of the 5th international conference on Mobile systems, applications and services. *San Juan, Puerto Rico*; R Shokri, J Freudiger, J-P Hubaux. *A Unified Framework for Location Privacy* (2010). EPFL-Report-148708. http://infoscience.epfl.ch/record/148708 (accessed January 25, 2011); Geopriv Internet Draft Informal. *A Process for Obscuring Location* (2010). http://tools.ietf.org/pdf/draft-thomson-geopriv-location-obscuring-01.pdf (accessed January 19, 2011); Alastair R Beresford and Frank Stajano. *Location Privacy in Pervasive Computing* (2003). PERVASIVEcomputing (January – March), p. 46-55.

[64] T Krazit. *Google mobile apps collect Wi-Fi location data*. CNET news http://news.cnet.com/8301-30684_3-20009223-265.html (29 June 2010).

[65] Office of the Privacy Commissioner of Canada (OPC). *Preliminary Letter of Findings*. http://www.priv.gc.ca/media/nr-c/2010/let_101019_e.cfm (accessed January 20, 2011), at 18, at 48.

[66] *Press Release*. Dutch Data Protection Authority. "Dutch DPA issues several administrative orders against Google." (19 April 2011).

Conclusion

The area of location privacy, involving an individual's ability to control who, when, how, and what granularity of personally identifiable location data is made available to others, is well established in the literature. However, additional discussion is required in this area where the individual's mobile device becomes an unknowing active contributor to the location architecture. In assessing the design of WPS architecture and location-based applications, the issues canvassed in this paper should be seriously considered, such as the concern for re-identification of location data, the sensitive nature of location information, the physical safety of individuals, and onward disclosure without the user's knowledge, or worse – contrary to his or her privacy preferences. Lengthy "take-it-or-leave-it" privacy policies are not consistent with the options researched to incorporate the decision-making ability of individuals using location-based services.[67] Efforts to fingerprint devices and associate them with individuals by combining information from other sources without the individual's consent are fundamentally inconsistent with privacy practices. Privacy is predicated on providing users with personal control along with openness and transparency associated with one's practices, which demonstrates respect for the user, and builds greater trust.

In situations where static, unique identifiers already exist, significant care must be shown in the use of those identifiers. The primary example of this is biometrics, such as fingerprints, facial recognition, iris scans, and similar physiological or behavioural characteristics of individuals. The unchecked use of biometrics for identification or verification of individuals could lead to numerous privacy concerns – the linkage of databases, expanded surveillance, and function creep, to name only a few. Again, to an even greater extent than the MAC address, a person's biometric is unique and unchangeable. The IPC has written extensively regarding the use of Biometric Encryption in those situations in which the use of biometric identifiers is appropriate.[68]

Thus, as with all technologies affecting privacy, it is clear that options exist and must be pursued to ensure that individuals are permitted to maintain their privacy while using WPS. Regardless of what requirements exist in the form of standards or laws, incorporating a *Privacy by Design* approach will ensure that the highest standard of privacy will be met. Incorporating a doubly-enabling Privacy by Design methodology into the treatment of mobile device identifiers, such as MAC address and SSID, WPS location aggregators, application developers, and advertisers can ensure greater protection of user privacy, while meeting consumer demand for location-based technologies and services – the ultimate win-win scenario.

[67] E.g. Geographic Location/Privacy (geopriv). *RFC 3693*. http://datatracker.ietf.org/doc/rfc3693/ (accessed January 19, 2011).

[68] By way of introduction, see http://www.ipc.on.ca/images/resources/bio-encryp.pdf

A final note of caution based on what we frequently encounter in the field of privacy: What may at first appear to be the "easy way out" may not in fact be so beneficial in the long term. However, when you begin by proactively embedding privacy, as you build a technological architecture or application, the rewards are numerous. The cost of bolting on privacy protections down the road when the system is already built, will be far more expensive and far less effective. *Privacy by Design* as a methodology was unanimously recognized and supported by the International Assembly of Data Protection and Privacy Commissioners, and is a recommended approach in major U.S. and European regulatory efforts.[69] *Privacy by Design* has now been made the International Standard for privacy, and should be considered for adoption from the outset, for a doubly-enabling, psotive-sum outcome.

[69] E.g. see Peter Hustinx, European Data Protection Supervisor. *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy.* (18 March 2010): "[T]he Opinion discusses the need to provide for the principle of 'privacy by design' into the data protection legal framework in at least two different ways. First, by incorporating it as a general, binding principle and, second, by incorporating it in particular ICT areas, presenting specific data protection/privacy risks which may be mitigated through adequate technical architecture and design," at 6; Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers* (2010): "Privacy by Design: Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services," p. 41.

Appendix A: *Privacy by Design*: The 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 Setting***

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 Security — ***Full 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 — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. ***Visibility*** and ***Transparency* — Keep it *Open***

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 — Keep it ***User-Centric***

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.

Appendix B: Overview of Major Positioning Systems

There are three broad categories of positioning systems: satellite vehicle-based (SV-based) positioning systems; systems operated by cellular communication network operators (‘cellular network-based positioning systems’); and systems based on wireless network technology such as Wi-Fi and Bluetooth.

SV-based positioning systems (e.g. Global Positioning System, Galileo Satellite Systems) involve a minimum of three satellites triangulating the location of the mobile device. SV-positioning is highly precise and relatively low cost since SV-positioning is increasingly embedded in devices as a feature. The drawbacks to SV-positioning are that it requires a high level of power consumption, and has a weak signal inside buildings.[70] However, there are advancements in assisted SV-positioning (e.g. assisted GPS) which make use of networks to speed up identification of location.[71]

Cellular network-based positioning systems like Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) provide positioning methods such as, for example, cell tower calculation, Cell of Origin positioning (COO) (also called ‘Cell Identity’ or ‘Cell ID’), time difference of arrival positioning (TDOA), angle of arrival positioning (AOA), and enhanced observed time difference positioning (E-OTD).

For cell tower calculations, cellular based network architecture is divided into cells within a geographic area. These cells can be meters or kilometres large, and are serviced by Base Transceiver Stations (BTS) antenna where each cell is serviced by one antenna. The location of these antennas is housed in GSM and UMTS location databases.[72] In order to provide mobile communication service and to bill customers, the location of the mobile device must be known at all times.[73]

COO involves the user’s location being determined by locating the base station that the user’s mobile device is connected to.[74] TDOA is possible when three base stations measure the time it takes to receive a signal from a user’s mobile device, and the distance between the base stations and the device.[75] E-OTD adds a level of accuracy by estimating how far antennas are located based on time intervals between signal arrival times to the mobile device.[76] AOA calculates the angle of the user’s mobile device by looking at the direction of radio signals based on information received on an antenna array.[77]

Wi-Fi based positioning systems have become useful as a geolocation tool in urban areas where GPS signals can be weaker, or where the use of GPS puts too much strain on the device’s battery. The

[70] *FIDIS, D11.2: Mobility and LBS*, p. 22.

[71] *FIDIS, D11.2: Mobility and LBS*, p. 22.

[72] C Renso, S Puntoni, E Frentzos, A Mazzoni, B Moelans, N Pelekis, and F Pini. *Wireless Network Data Sources: Tracking and Synthesizing Trajectories*. In *Mobility, Data Mining and Privacy. Geographic Knowledge Discovery*, ed. T Gianotti and F Pedreschi. Heidelberg: Springer Verlag, 2008. p. 75.

[73] Nouwt, p. 377.

[74] FIDIS, *D11.2: Mobility and LBS*, p. 24; Renso et al, p. 76.

[75] FIDIS, *D11.2: Mobility and LBS*, p. 25.

[76] Renso et al, p. 77; FIDIS, *D11.2: Mobility and LBS*, p. 26.

[77] FIDIS, *D11.2: Mobility and LBS*, p. 25.

systems measure the distance of the wireless device to nearby Wi-Fi access points MAC addresses and SSIDs.[78] A query is sent from the device to a database, including a list of detected nearby MAC addresses and the database replies with the location of the device based on matching Wi-Fi points geo-tagged in its database.[79] Bluetooth may also be tracked and positioned indoors, however limited range and density make this less practical, whereas Wi-Fi access points are more commonly present in urban areas.[80]

Different kinds of location technologies can be used simultaneously to provide a more accurate location. For example, for handsets in the U.S., and in the case of emergency calls, GPS data can be sent to cell carriers if the handset is configured to do so.[81]

[78] Nouwt, p. 381.

[79] Testimony of J Morris before the *Committee on Energy and Commerce*, U.S. House of Representatives (24 February 2010), p. 4.

[80] Renso et al, p. 82; Nouwt, p. 381.

[81] Morris, *Testimony*, p. 4.

About the Authors

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner,

Ontario, Canada

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. Her concept of *Privacy by Design* seeks to proactively embed privacy into the design specifications of information technology and accountable business practices, thereby achieving the strongest protection possible. In October, 2010, data regulators from around the world unanimously passed a landmark Resolution recognizing *Privacy by Design* as an essential component of fundamental privacy protection. This was followed by the U.S. Federal Trade Commission's inclusion of *Privacy by Design* as one of its three recommended practices for protecting online privacy – a major validation of its significance.

Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is strongly protected, not only in Canada, but around the world. She has been involved in numerous international committees focused on privacy, security, technology and business, and endeavours to focus on strengthening consumer confidence and trust in emerging technology applications.

Dr. Cavoukian serves as the Chair of the Identity, Privacy and Security Institute at the University of Toronto, Canada. She is also a member of several Boards including, the European Biometrics Forum, Future of Privacy Forum, RIM Council, and has been conferred as a Distinguished Fellow of the Ponemon Institute. She was named by *Intelligent Utility Magazine* as one of the "Top 11 Movers and Shakers for the Global Smart Grid industry for 2011," and has been honoured with the prestigious *Kristian Beckman Award* for her pioneering work on *Privacy by Design* and privacy protection in modern international environments.

Kim Cameron

Identity Architect

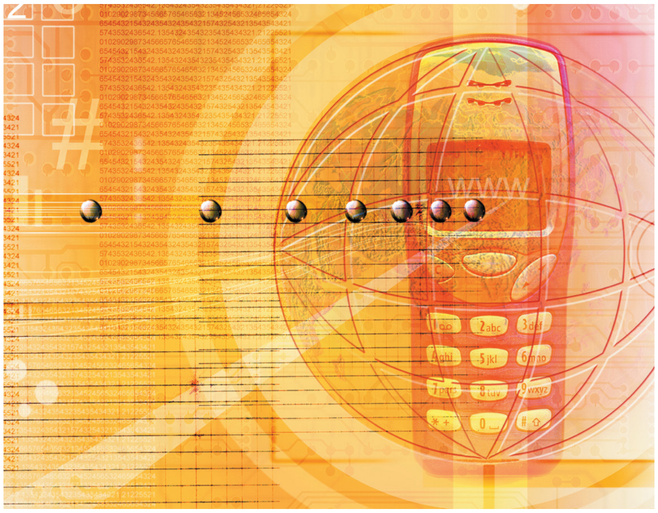
Kim Cameron is a leading expert in digital identity. The author of the influential Laws of Identity, he serves as an advisor on identity architecture and issues.

Kim began his career in the software industry as a founder of the ZOOMIT Corporation. As VP of Technology he led ZOOMIT's development of email, networking, directory and security products. He invented and built the first Metadirectory. Microsoft bought the ZOOMIT Corporation in 1999 and Kim joined Microsoft, playing a leading role in the evolution of Active Directory and Microsoft Metadirectory Services (now Forefront Identity Manager).

In 2005 he was appointed Chief Architect of Identity in the Identity and Access Division at Microsoft, where he championed the emergence of a privacy enhancing Identity Metasystem reaching across technologies, industries, vendors, continents and cultures. He led the emergence of claims based architecture, embodied in Federation Services, CardSpace and Microsoft's other Identity Metasystem products and initiatives. He was appointed Microsoft Distinguished Engineer in 2009, finally resigning his role as Chief Architect of Identity in 2011.

Kim grew up in Canada, attending King's College at Dalhousie University and l'Université de Montréal. He served on RISEPTIS, the high-level European Union advisory body providing vision and guidance on security and trust in the Information Society. He has won a number of industry awards, including Digital Identity World's Innovation Award (2005), Network Computing's Top 25 Technology Drivers Award (1996) and MVP (Most Valuable Player) Award (2005), Network World's 50 Most Powerful People in Networking (2005), Microsoft's Trustworthy Computing Privacy Award (2007) and Silicon.com's Agenda Setters 2007. In 2010 King's College recognized his work on digital identity by awarding him an honorary Doctor of Civil Law degree.

Kim blogs at www.identityblog.com



Information and Privacy Commissioner
Ontario, Canada
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca
Telephone: 416-326-3333
Fax: 416-325-9195

The information contained herein is subject to change without notice. The authors shall not be liable for technical or editorial errors or omissions contained herein.

June 2011

Information & Privacy
Commissioner of Ontario