Building Privacy into Mobile Location Analytics (MLA) Through *Privacy by Design*

March 2014

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

Nilesh Bansal, Ph.D.
Nick Koudas, Ph.D.
Co-Founders, Aislelabs

Acknowledgements

The authors would like to acknowledge the contributions of Michelle Chibba, Director of Policy and Special Projects, and David Weinkauf, Policy & Information Technology Officer at the Information & Privacy Commissioner's Office, to the development of 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

Building Privacy into Mobile Location Analytics (MLA) Through *Privacy by Design*

TABLE OF CONTENTS

1. Introduction

As the popularity of smartphones and tablet computers continues to rise, more and more creative ways of using these devices are being developed. While apps continue to provide the majority of new functionality, there is a growing industry built upon utilizing, not the advanced computing capability of smart devices, but their increased ability to connect wirelessly to other devices and networks. One technology that has recently created a new use of smart mobile devices by utilizing their increased connectivity is Mobile Location Analytics (MLA).

MLA provides retailers with insights into the in-store behavior of their customers by tracking the number, location, and patterns of smart mobile devices that enter and exit their stores. While this technology provides retailers and customers with many benefits—generally speaking, it allows retailers to adapt more efficiently and effectively to the demands of their customers—it also raises many privacy concerns. In order for MLA to maintain the trust and confidence of consumers while improving retailers' understanding of them, these privacy concerns must be addressed in a manner that simultaneously allows for the generation of effective retail analytics.

Such a positive-sum, "win-win" paradigm, which seeks to meet all legitimate interests and objectives, may be achieved through application of the principles of *Privacy by Design*. By embedding privacy into the design and architecture of MLA systems and their corresponding business practices, *Privacy by Design* allows consumer privacy and retail analytics to co-exist in tandem without diminishing system functionality.

In this paper, we examine the application of *Privacy by Design* to the design and architecture of MLA systems through the work of Toronto-based MLA company Aislelabs. Aislelabs is part of a working group of MLA companies that, together with the Washington D.C.-based think tank Future of Privacy Forum, proactively identified privacy issues inherent in the functioning of MLA technology. The result is a Code of Conduct that sets down effective privacy controls for the use of MLA technology in the industry.[1]

This paper has in total four sections. It begins with a background discussion of MLA and how it works technologically (section 2). Next the paper discusses the unique privacy risks associated with MLA (section 3). Finally, it introduces *Privacy by Design*, discusses Aislelabs' MLA implementation, and shows how it designs in privacy from the outset (section 4).

1 See Appendix A for a discussion of the MLA Code of Conduct.

2. Background on Mobile Location Analytics

The better retailers understand their customers, the better they are able to serve them. To this end, retailers have attempted to measure the flow of consumer traffic throughout their stores through the use of various technologies. For example, over the years retailers have turned to technologies such as infrared motion detection, thermal heat sensors, and, more recently, Anonymous Video Analytics (AVA)[2] in order to understand their customers better and evaluate their own performance in serving them. Many retailers are investing an increasing portion of their IT expenditures in these kinds of retail analytics technologies. A combination of such technologies has been utilized by retail chains, malls, event centers, airports, colleges, and museums around the world to analyze consumer traffic patterns.

In the last year, Mobile Location Analytics (MLA) has emerged as an advanced technology to further the understanding of consumer traffic by way of measuring the number, location, and patterns of individuals within and around a given area. MLA refers to a set of technologies that capture and analyze radio signals, such as Bluetooth[3] and Wi-Fi[4] signals, from nearby mobile devices to generate aggregate reports about consumer behavior for retailers.

Today if you buy a cell phone, tablet, laptop, or other mobile communications device, it is almost certain that it will come enabled with Wi-Fi or Bluetooth connectivity. Wi-Fi and Bluetooth are wireless technologies; they use radio signals that travel at various frequencies to enable devices to communicate wirelessly. Central to Wi-Fi and Bluetooth technologies is the ability to identify the communicating devices while at the same time distinguishing them from other devices. In order to perform this key ability, a unique identifier is assigned by the manufacturer to each physical networking component on a device, including Wi-Fi and Bluetooth interfaces.[5] This unique device identifier is referred to as the Media Access Control (MAC) address and takes the form of six groups of two alphanumeric characters,[6] separated by colons or hyphens. For example, "18:03:73:DE:10:E5" is a valid MAC address. A MAC address uniquely identifies a device's networking interface and is essential for it to communicate across a network.

Any device that is enabled with Wi-Fi or Bluetooth connectivity has such a MAC address—one for each wireless interface installed. For example, smartphones, personal fitness devices, and many wearable computing devices are enabled with wireless connectivity and thus have their own MAC addresses. How this relates to MLA technology is that when the Wi-Fi or Bluetooth connectivity of these devices is turned on, periodically these devices will "probe" to discover nearby wireless services to connect to. Any wireless sensor "listening" to these probes can initiate the connection protocol sequence for device connectivity. Such probes for wireless

2 AVA technology scans real-time feeds from video cameras utilizing pattern detection algorithms to identify shoppers anonymously for the purpose of creating aggregate reports. See http://www.ipc.on.ca/images/Resources/AVAwhite6.pdf.

3 http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1203598

4 http://dl.acm.org/citation.cfm?id=1067170.1067193

5 See IEEE Standards Association. *Guidelines for Use of EUI*. Retrieved from http://standards.ieee.org/develop/regauth/tut/eui.pdf.

6 More specifically, the characters used in MAC addresses are hexadecimal digits, which are base-16 numbers represented by the values 0–9 and A–F.

services contain the device's MAC address in order to enable communication. Each probe also includes a signal strength that can be used to infer the distance between the sensor and the device with accuracy within a few meters. Thus, by listening to probes for wireless services, MLA sensors are able to collect the MAC addresses and signal strengths of nearby smart mobile devices and so determine the number, location, and patterns of customers within and around a given area.

The ability to sense the MAC address and associated signal strength of any nearby device with Wi-Fi or Bluetooth turned on has been reported in the past in several research publications.[7,8] In these works, the researchers utilize the MAC address of a device to determine its location inside a building to assist the person carrying the device to navigate indoors or for numerous other innovative applications. This field has attracted the attention of the research community for more than fifteen years.

By combining and analyzing the MAC addresses and signal strengths of nearby smart mobile devices, MLA is able to enhance retail metrics by generating aggregate reports on window conversion, walking paths, heat maps depicting busy areas, repeat visits, sequential visits, dwell times, sales intercepts, product interaction, queue wait times, zone traffic counts, dwell-to-traffic ratios, personnel location, employee to customer ratio, and public safety. Inclusion of these metrics allows for a better understanding of consumers' in-store behavior, enabling stakeholders to optimize their processes and provide a better overall shopping experience. For example, using MLA a retailer would be able to optimize store layout, measure key metrics before and after the rollout of different sales campaigns, and minimize checkout times.

The data collected and processed by MLA technologies focuses on consumer traffic within and around individual stores or retailers. However, it is important to note that when multiple stores or retailers use the same MLA provider, their datasets may be combined to produce additional, cross-store insights on consumer traffic. For example, if the same MLA provider is used by a coffee bar, vegetarian restaurant, and gym, the coffee bar owner might learn that a number of customers appear to frequent vegetarian restaurants and the gym. As such, the owner could begin to offer healthy menu items as a way of increasing sales and improving customers' experience.[9]

7 M. Youssef and A. Agrawala. (2005). "The Horus WLAN location Determination System," Proc. ACM Mobisys.

8 P. Bahl and V. Padmanabhan. (2000). "RADAR: An In Building RF-based User Location and tracking System," IEEE Infocom.

9 See A. Ligaya. (February 2, 2014). "'It's creepy': Location based marketing is following you, whether you like it or not." *National Post*. Retrieved from http://business.financialpost.com/2014/02/01/its-creepy-location-based-marketing-is-following-you-whether-you-like-it-or-not/?__lsa=78b7-20d5.

3. Privacy Risks of Mobile Location Analytics

In the context of MLA, 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. Although there may be jurisdictional differences, personal information (also known as personally identifiable information, or PII) may be defined as 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.

Since MAC addresses were designed to be persistent and unique over the lifetime of a Wi-Fi or Bluetooth-enabled device, in the case of MLA, they identify devices that are closely associated with individuals—not only smart phones, but personal fitness and wearable computing devices. 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.[10] The issue is that, while not personal information *per se*, a MAC address can nonetheless act as a powerful unique identifier that can bring together disparate pieces of personal information about an individual. When combined with the fact that MLA technology tracks the location and movements of Wi-Fi and Bluetooth-enabled devices, this ability of MAC addresses to accumulate disparate pieces of information contributes to the public's concern that "somebody out there knows something about me"—the Big Brother scenario, leading to increased suspicion and distrust on the part of consumers.

More specifically, as more and more information about an individual is collected and processed by an automated system, an increasingly detailed "picture" of that individual's life may be created. As a result, intimate details about an individual's life may be determined or inferred that he or she did not wish to share or disclose with others. The kinds of information collected and processed by MLA technologies—frequency and times of visits, walking paths, dwell times—may be used in this manner to glean information about an individual's lifestyle or habits. For example, whether an individual is employed, has children, prefers certain brands over others, celebrates certain religious holidays, etc.—may be inferred from an individual's in-store behavior and used to form a detailed portrait of that individual's life. Without proper safeguards in place, such profiling may occur and be used without the consent of the individual for purposes other than retail analytics, such as marketing. For example, if an MLA provider offers free Internet access through its Wi-Fi sensors and makes as a condition of that service the provision of an email address, it could send the individual personalized ads based on her shopping profile. Furthermore, once such information about an individual is collected and stored, the potential is there for it to be copied and shared with third parties without the knowledge or consent of the individual. This is especially true of digital information, which, in contrast to its analog counterpart, can be transported instantaneously "at the click of a button."

10 See A. Cavoukian, K. Cameron. (June 2011). "Wi-Fi Positioning Systems: Beware of Unintended Consequences." Retrieved from http://www.ipc.on.ca/images/Resources/wi-fi.pdf.

Such sharing of MLA information opens up the possibility of it becoming linked to, or commingled with, other sets of information about the same individual, thereby increasing the amount and scope of information available for processing about that individual. This increase may not only result in further profiling of an individual but a reduction in overall data quality. Since the commingling of datasets often disassociates the information from the original context in which it was collected, there is a tendency when linking together naturally disparate datasets for the quality of the data to suffer.[11]

In order for different datasets about an individual to be joined together, they must both be able to identify the individual usually through a common or shared identifier. In the case of MLA, the need for such an identifier would most likely be fulfilled by the MAC address of the individual's smart device. However, if an individual uses an application that publicly broadcasts his or her location and identity or online "handle"—for example, Foursquare or Twitter with location services enabled—it is also possible for this identifying information to be linked to an MLA dataset based on the existence of a shared location. For example, by cross referencing Tweets that have location information and MLA datasets, it would be possible to link together MAC addresses and Twitter IDs, thereby increasing the personal identifiability of the data involved.

11 See D. Solove. (January 2006). "A Taxonomy of Privacy." University of Pennsylvania Law Review, Vol. 154, No. 3, pp. 507–508.

4. Building Privacy into Mobile Location Analytics

4.1 Privacy by Design

Privacy by Design (*PbD*) is an internationally recognized[12] framework developed in the mid-nineties 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. Ongoing advancements in, coupled with the widespread use of, information and communications technologies have led to dramatic increases in the collection, use, disclosure, and retention of information about individuals. 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 future.

The objectives of *PbD*—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
2. Privacy as the *Default Setting*
3. Privacy *Embedded* into 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*[13]

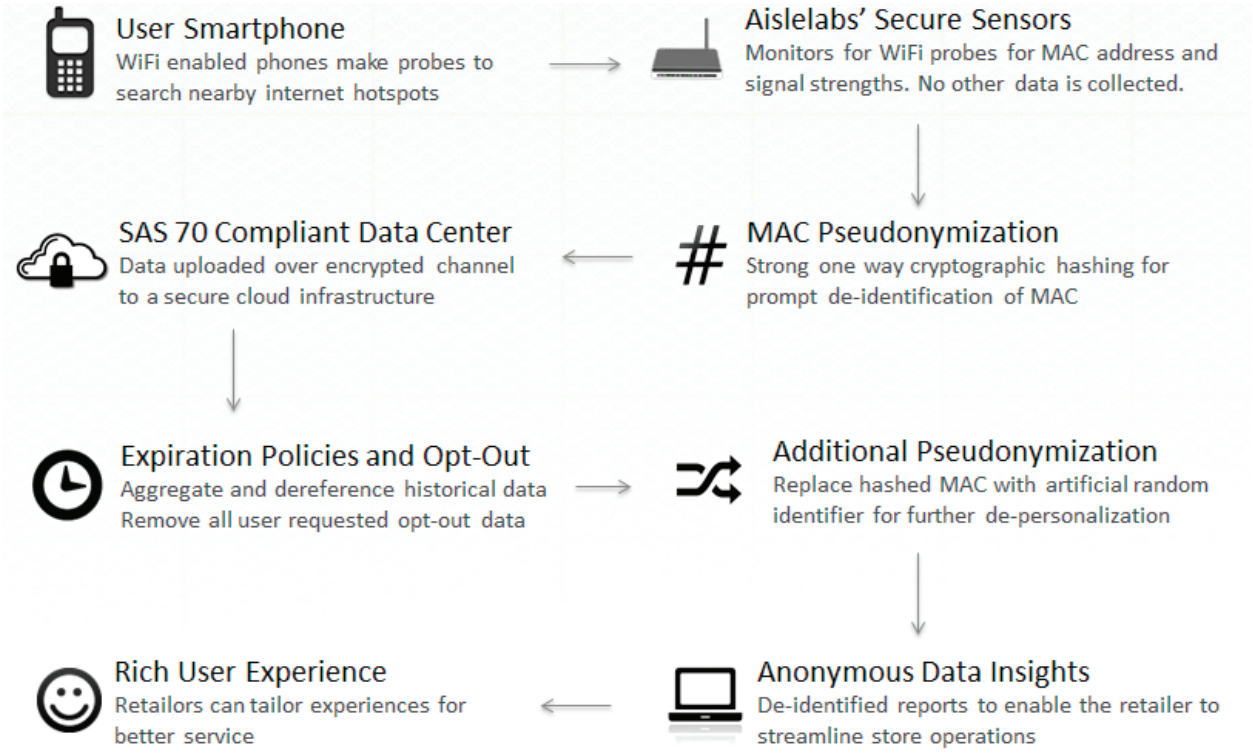
Given the necessity of establishing user trust in order to gain public acceptance of its technologies, the MLA industry must think *Privacy by Design* as new products are developed, marketed, and deployed. In the next sections, we will discuss the particular MLA technology developed by Toronto-based company Aislelabs and show how its privacy-protective solution was motivated by an overall desire to design in privacy from the outset.

12 See International Conference of Data Protection and Privacy Commissioners, Jerusalem, Israel. (October 27–29, 2010), "Resolution on Privacy by Design." Retrieved from http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26502/ResolutiononPrivacybyDesign.pdf; U.S. Federal Trade Commission. (2012). *Protecting Consumer Privacy in an Era of Rapid Change*. Retrieved from http://www.ftc.gov/os/2012/03/120326privacyreport.pdf; European Commission. (2012). "General Data Protection Regulation." Retrieved from http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

13 See A. Cavoukian. (2011). "Privacy by Design. The 7 Foundational Principles." Retrieved from http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

4.2 Aislelabs' MLA Technology

The diagram below shows the data collection and the report creation process, as implemented by Aislelabs. The diagram has eight steps, as listed below:



1. User smartphones and other devices emit probes for all nearby wireless services.

2. Secure Wi-Fi and Bluetooth sensors obtain the device MAC address and signal strength. These sensors are unable to detect other information, such as the phone number, email address, or other personal communication data. None of the data collected is stored on the sensor and all data is processed and encrypted in-memory. Network firewalls and other appropriate security measures are implemented to prevent any unauthorized access to the sensors.

3. The MAC address is promptly pseudonymized. This is achieved through the use of the cryptographic hashing technique SHA256.[14] This hashing technique is recommended for use by the Government of Canada Policy for the Protection of Classified Information up to level SECRET.[15]

4. The secure sensor transfers the collected information to a data center equipped with strong industry standard network and physical security

14 C. Parr, J. Pelzl. (2011). *Understanding Cryptography, A Textbook for Students and Practitioners*, Springer.

15 Government of Canada Policy for the Protection of Classified Information Using Suite B Algorithms. Retrieved from http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb40a-eng.html.

measures. All data transfer takes place over strong 256-bit SSL encrypted channel. The encryption ensures safety of the data while in transit.

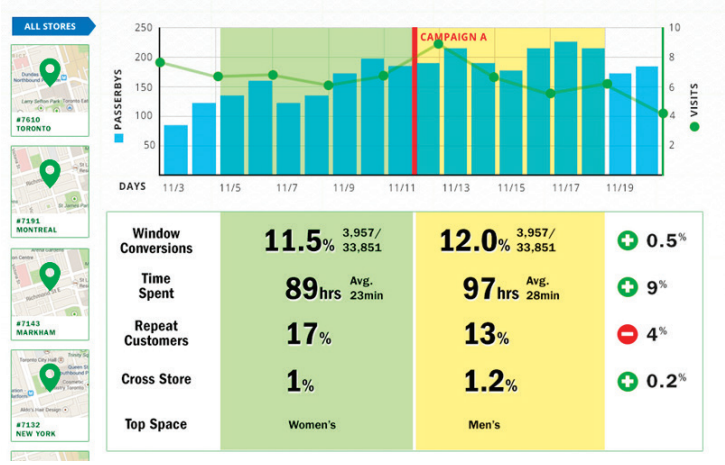
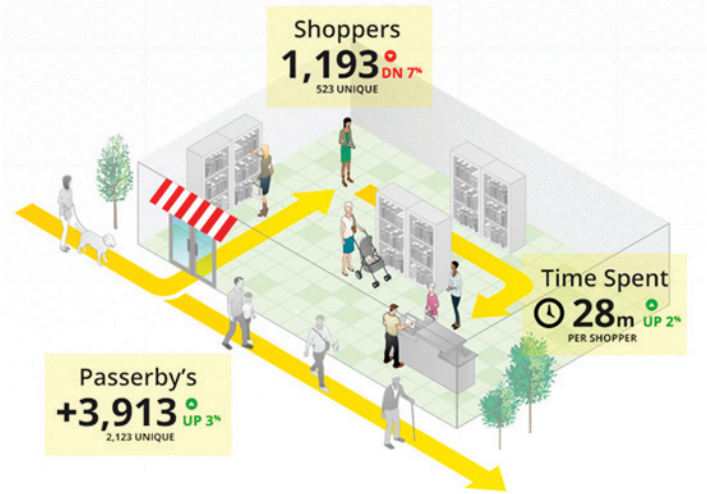
5. Collected data is checked against a list of opt-out users. Users may choose not to participate in Aislelabs MLA analytics by entering the MAC addresses of their smart mobile devices at Aislelabs' opt-out page (http://www.aislelabs.com/privacy/). Information from devices that have opted out is discarded. Further, the expiration policy is checked to ensure no data is retained for a period longer than the one stated in Aislelabs' privacy policy.

6. Aislelabs further secures collected pseudonymous identifiers (hashed MAC addresses) by randomization. In this step, each hashed unique identifier is replaced with a random artificial identifier such that the MAC address for an individual's device cannot be obtained from the value stored. This provides an additional layer of de-personalization over the already privacy-protective implementation in Step 3. Outside of Aislelabs' MLA system, the resulting random identifier cannot be linked to the original MAC address in any way.

7. Aggregated anonymous reports are created based on the collected data. These reports include statistics about the number of shoppers, repeat customers, window conversion, time spent in store, top walking paths, and heat maps for frequented spaces. No personally identifiable information is disclosed to the retailer. All this is delivered to the retailer via web-based dashboards where all information transfer is encrypted. Sample screenshots from some of these reports, as displayed by the Aislelabs dashboard, are provided in the table below.

8. Using the insights learned from MLA reports, the retailer better understands the return on investment for different decisions, thus leading to operational efficiencies, cost reductions, better services, and a richer experience for shoppers.

Table 1: Examples of Aislelabs' Aggregate Insights

	Campaign Comparison shows the key metrics across stores before and after the rollout of different campaigns, helping the retailer to understand the return on investment.
	Shopper Window Conversion shows what fraction of consumers walked in the store and the amount of time spent inside on average.
	Heat maps and walking paths show the most frequented spaces in the store, helping the retailer to optimize the store layout for better access.

From the above process, the following architectural elements and functional results stand out as key *Privacy by Design* characteristics of Aislelabs' solution.

4.2.1 MAC Address Pseudonymization

The privacy risks of MLA stem from the unique, persistent character of MAC addresses, which makes possible the singling-out and tracking of individuals by way of their smart mobile devices. However, the consumer should not have to take any action to ensure that his or her personal information is not collected or subsequently abused. Hence, as a starting point, when collecting MAC addresses, Aislelabs' MLA technology promptly pseudonymizes them using a strong cryptographic one-way hash function such as SHA-256. Pseudonymizing MAC addresses allows MLA technology to distinguish between individuals, and thereby calculate metrics on repeat customers, while adding measures to protect those customers' privacy.

4.2.2 Randomization Tables

MAC address pseudonymization helps to protect the privacy of individuals. However, while one-way hash algorithms prevent the hashed values they create from being *reversed* back into their original form, they still maintain a *forward* relationship between original and hashed values. In certain scenarios, this relationship may be used to rediscover the MAC address of a hashed value, thereby re-identifying the individual's device to which it corresponds. For example, if retailer A shares its pseudonymized dataset with retailer B, it would be possible for B to discover the MAC addresses of customers who shop at both A and B by collecting the MAC addresses of its customers, hashing them with the same algorithm as retailer A, and then comparing the hashed values against the shared pseudonymized dataset. This would require B to hold on to MAC addresses of its customers and not discard them upon applying the hash function. In addition, there is also the possibility of B performing a brute-force or dictionary attack on A's entire pseudonymized dataset by calculating the hashed values of *all* possible MAC addresses—of which there are only 2^{48} or 281,474,976,710,656—and performing a reverse lookup on the values in A's dataset.[16]

While it is possible to prevent such rediscovery of MAC addresses through contractual provisions that prohibit downstream recipients of pseudonymized datasets from attempting to use the data to identify a particular individual,[17] Aislelabs implements a technological solution to this problem. By replacing each hashed identifier with a random artificial identifier, an *additional* layer of de-personalization may be added to the system. This randomization would prevent any downstream recipient of the dataset from rediscovering the MAC address of a value in it, since, once randomized, the values in the dataset bear *no* relation to the MAC address. For the same reason, this would also prevent the values in the dataset from being susceptible to dictionary or brute-force attacks. Thus, by embedding an additional layer of de-personalization into the design and architecture

16 See P. Higgins, L. Tien. (October 27, 2013). "Mobile Tracking Code of Conduct Falls Short of Protecting Consumers." Retrieved from https://www.eff.org/deeplinks/2013/10/mobile-tracking-code-conduct-falls-short-protecting-consumers.

17 This is, for example, the approach taken by the MLA Code of Conduct.

of its MLA systems, Aislelabs is able to prevent the rediscovery of MAC addresses either by comparing their hashed values to shared pseudonymized datasets or dictionary or brute-force attacks. The use of a salt[18] while hashing would also prevent the rediscovery of MAC addresses.

4.2.3 Empowering Stakeholders and Consumers

Retailers play an important role in bridging the gap between production and consumption, and as a result retail transactions contribute significantly to the economy—for example, $165B annually in Ontario.[19] Inevitably the retail sector affects other industries and the national economy as a whole, through its innovation in critical areas, including key performance indicator (KPI) measurement, customer relationship management (CRM), e–commerce, and supply chain mandates. In Canada, the retail sector has outpaced the overall economy in multifactor productivity growth primarily led by investments in information and communications and technology (ICT) greater than both the Canadian manufacturing sector and the U.S. retail sector in terms of dollars invested in ICT per GDP.[20] The ability to access and utilize strategic information in decision-making enables retailers to focus on initiatives that deliver a strong return on investment. Consequently, Canadian retail employment has grown 2.4 percent per year from 2002 to 2009 while employing 2.0 million people, or 11.9 percent of the total working population in 2009.[21] The case of Canada shows how innovation in the retail sector is benefiting Canadian consumers by streamlining the shopping experience, providing more options, better customer service and cost reductions as a result of operational efficiencies.

Aislelabs' MLA technology empowers stakeholders with knowledge that enables them to optimize certain aspects of their business. Such optimizations lead to efficiencies that directly impact consumers. For example:

- Knowing the number of visitors to a store at any point in time and the aggregate time spent enables retailers to optimize their staffing. Such optimization leads to better customer service, such as reduced waiting times, more people to answer questions in store, leading to a better shopping experience.
- Knowledge of aggregate walking paths and heat maps inside the store helps retailers optimize the store layouts. This helps customers find easily what they are typically searching for and provide easy access to merchandise in the store, directly benefiting customers.
- By obtaining a detailed understanding on the performance and return on investment (ROI) of their marketing campaigns, retailers can employ the science of big data in their future investments. This helps them utilize their capital spend more efficiently and leads to better business that could result in benefits to the overall economy.

18 http://en.wikipedia.org/wiki/Salt_%28cryptography%29

19 http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/trad17a-eng.htm

20 Industry Canada, *State of Retail: The Canadian Report 2010,* http://www.ic.gc.ca/eic/site/retra-comde.nsf/eng/h_qn00281.html?Open&pv=1

21 Statistics Canada. CANSIM, 2010.

- Insights into aggregate frequency of customer visits helps retailers understand and reason about customer loyalty. As a result this will spawn consumer-friendly programs to boost loyalty and offer better services and pricing to consumers.

These examples show how both retailers and consumers benefit from the results of MLA technology—a positive-sum "win-win" outcome in its own right. However, when combined with the fact that this benefit does not come at the expense of individuals' privacy, but rather individuals' privacy may be protected at the same time without diminishing system functionality, this positive-sum outcome becomes a "win-win-*win*." Consumers benefit from not only better services and prices but by the fact that their privacy is protected throughout the system by appropriate measures being proactively embedded into its design and architecture.

4.2.4 Security of Data at Rest and in Transit

A system is only as secure as its weakest module. Recognizing this, all parts of Aislelabs' MLA IT and business systems are developed with strong security provisions from day one. All sensors have network firewalls and strong de-identification algorithms. The data centers supporting the cloud infrastructure are secure both physically and via the network. Data storage and transfer of sensitive information employ military-grade encryption technologies like AES128 and TLS. Policy controls for limited employee access are enforced to prohibit unauthorized access. Business processes are designed to complement the security in IT systems and protect any sensitive information.

4.2.5 Notice to Users

Trust is not possible without an open and transparent operation to inform all stakeholders regarding the business practice or technology involved. As a result, Aislelabs provides complete visibility in its processes by publishing its privacy policy on its website and including a contact helpline for privacy matters. In addition, if non-aggregated data is stored for a given retailer, Aislelabs installs conspicuous signage notifying the retailer's customers of the use of MLA technology, with links to its privacy policy.

4.2.6 Persistent Opt-Out

At its core, respecting the user means that, when designing or deploying an information system, the individual's privacy rights and interests are accommodated right from the outset. User-centricity means putting the interests, needs, and expectations of people first, not those of the organization or its staff. This is key to delivering the next generation of retail experience because empowering people to play active roles in the management of their personal data helps to mitigate abuses and misuses. To this end, Aislelabs provides an opt-out site that allows individuals to choose not to have their retail traffic data included in any anonymous analytics.

5. Conclusion

When it comes to the new retail analytics technology of MLA, one could raise the "slippery slope" argument; namely, that what poses no privacy risk as it now applies could change as technologies evolve. Through its collection and analysis of MAC addresses and signal strengths, MLA technology could, in theory, tailor marketing to the shopping patterns or other characteristics of recognized individuals. As this paper discusses, however, MLA need not be designed to do any of that.

A deployment of MLA technology that follows the 7 Foundational Principles of *Privacy by Design* provides sufficient safeguards to protect against the misuse of any personal information while allowing for effective retail analytics. Consumers can reap the benefits of this technology as retailers make more informed decisions to serve them. At the same time, consumers can rest assured that their privacy is protected through pseudonymization, randomization, and de-identification of the MAC addresses of their smart mobile devices.

Proactive efforts that not only recognize but also protect privacy are essential for MLA developers and users. Using the principles of *Privacy by Design*, in conjunction with MLA Code of Conduct, places vendors in the best position to build and evolve MLA technology. Build with *Privacy by Design* in mind and gain a competitive advantage—your customers will thank you!

Appendix A: MLA Code of Conduct

Consumer trust in any new technology is of paramount importance, as the ultimate aim is to provide a rich shopping experience to build a healthy relationship between the retailer and the consumer. Any technology must first consider the interests of consumers to succeed in the long term. Recognizing this, several MLA vendors, including Aislelabs, participate in an industry consortium, organized by the Future of Privacy Forum,[22] that has proactively put forth an MLA Code of Conduct for the implementation and deployment of this new technology.

The Code of Conduct is available online[23] and sets out necessary guidelines for protecting consumer interests and privacy while enabling the next generation of retail operations. The Code lays out the following principles: (1) Notice; (2) Limited Collection; (3) Choice; (4) Limitation on Collection and Use; (5) Onward Transfer; (6) Limited Retention; and (7) Consumer Education. Specifically, the code states:

- MLA vendors shall take reasonable steps to require that companies using their technology display, in a conspicuous location, signage that informs consumers about the collection and use of MLA data at that location. Such signage shall provide information about how consumers can find additional information and exercise the choice of opting-out completely should they wish to do so.
- MLA vendors shall provide a detailed privacy notice on their websites describing the information they collect and use and the services they provide.
- MLA vendors shall not collect personal information or unique device information, unless it is promptly de-identified or de-personalized, or unless the user has provided affirmative consent. Collected MAC addresses should be de-personalized such that the data cannot reasonably be linked to an individual by use of techniques such as cryptographic one-way hashing.
- MLA vendors who collect location information from mobile devices for the purpose of providing location analytics shall limit the data collected for analysis to information needed to provide analytics services.
- MLA vendors that provide data to third parties shall contractually prohibit those parties from attempting to use the data to identify an individual.
- MLA vendors shall provide consumers with the ability to decline to have their mobile devices anonymously included in retail analytics services. Users have the ability to opt-out completely by visiting a central industry website (http://smartstoreprivacy.org/).
- MLA data shall not be collected or used in an adverse manner for the following purposes: employment eligibility, promotion, or retention; credit eligibility; health care treatment eligibility; and insurance eligibility, pricing, or terms.
- MLA vendors shall not retain the collected information indefinitely. All vendors shall set internal policies for data retention and deletion of unique device data.

22 http://www.futureofprivacy.org

23 http://www.futureofprivacy.org/issues/smart-stores/

Overview of Organizations

Office of the Information and Privacy Commissioner of Ontario (IPC)

The role of the Information and Privacy Commissioner of Ontario, Canada, is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The IPC acts independently of government to uphold and promote open government and the protection of personal privacy. Under the three *Acts*, the Information and Privacy Commissioner: resolves access to information appeals and complaints when government or health-care practitioners and organizations refuse to grant requests for access or correction; investigates complaints with respect to personal information held by government or health-care practitioners and organizations; conducts research into access and privacy issues; comments on proposed government legislation and programs; and educates the public about Ontario's access and privacy laws. More at: www.ipc.on.ca and www.privacybydesign.ca.

Aislelabs

Aislelabs is a technology company assisting retailers to increase sales through the power of big data analytics. We help our clients understand customer traffic patterns and behavior inside and outside their physical stores in ways never before possible. This deeper understanding empowers our suite of products to deliver highly personalized omni-channel marketing tailored to in-store customers. Aislelabs' technology transforms retail locations to smart stores, resulting in effective marketing, increased sales, and better customer satisfaction. We serve retail chains, shopping malls, boutique retailers, restaurants & cafes, event venues and public spaces of all sizes.

Office of the Information and Privacy Commissioner, Ontario, Canada
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

Aislelabs
33 Lombard Street
Suite 3604
Toronto, Ontario
Canada M5C 3H8
Telephone: 647-557-3510
Fax: 647-557-3511
E-mail: privacy@aislelabs.com
Website: www.aislelabs.com

Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

March 2014