BEFORE THE UNITED STATES FEDERAL TRADE COMMISSION

WASHINGTON, DC

COMMENTS OF THE FUTURE OF PRIVACY FORUM	)
RE - SPRING PRIVACY SERIES: MOBILE DEVICE TRACKING, PROJECT NO. P145401	)

I. Introduction

On February 19, 2014, the Federal Trade Commission ("FTC" or "Commission") held a Seminar examining how businesses and other organizations use technologies that detect certain signals emitted by consumers' mobile devices to monitor how consumers move through and around various locations, including airports, malls, public spaces, and retail stores. The Seminar also focused on how organizations use that information, the benefits of those uses, and whether the collection and use of the information raises potential privacy concerns. The FTC has invited public comments on issues related to the Seminar.[1]

The Future of Privacy Forum ("FPF") welcomes the opportunity to provide these Comments to the Commission.[2] Since its founding in 2008, FPF has worked to ensure that privacy is integrated into the development and implementation of new technologies and services, including those involving connected devices, in a manner that allows for innovation. One of our first projects was to promote privacy in the Smart Grid, including by working with Information and Privacy Commissioner of Ontario, Ann Cavoukian, Ph.D., to co-author a white paper on

[1] *Request for Comments and Announcement of FTC Workshop on Spring Privacy Series, Project No. P145401*, FTCPublic.commentworks.com, https://ftcpublic.commentworks.com/ftc/springprivacyworkshop/ (last visited Mar. 19, 2014).

[2] FPF is a Washington, D.C.-based think tank whose mission is to advance privacy for people in practical ways that allow for innovation and responsible use of data. The FPF Advisory Board includes privacy professionals, privacy scholars, and academics. The co-chairs of FPF are Jules Polonetsky, its Executive Director, and Christopher Wolf, who leads the global privacy practice at Hogan Lovells US LLP.

embedding Privacy by Design in the Smart Grid.[3] We are currently working on connected device issues as part of our Connected Cars Project, which seeks to ensure that privacy is protected and data is secured as connected car technologies and services develop. To coincide with the FTC's November 2013 workshop on the Internet of Things, we published a white paper discussing the appropriate framework for the privacy issues raised by the development of connected device ecosystems.[4]

FPF has direct experience working with companies that collect information emitted from consumer's mobile devices in order to learn and share insights about consumers' movements in and around specific locations—a practice that for the purposes of these Comments we refer to as "mobile location services." In October 2013, FPF and companies providing mobile location services released the **Mobile Location Code of Conduct** ("Code"), which promotes privacy in the retail use of mobile location services.[5]

As discussed below, new mobile location services stand to provide substantial benefits to consumers and other stakeholders. Although mobile location services typically involve the collection of information that does not directly identify individuals, and the reports delivered by mobile location service companies typically contain only aggregate information that businesses use to improve customers' shopping experiences, we recognize that mobile location services can raise privacy concerns if responsible practices are not followed. The Code addresses such concerns through the flexible application of the Fair Information Practice Principles ("FIPPs"). The Code also illustrates how FPF's white paper *An Updated Privacy Paradigm for the "Internet of Things"* ("White Paper") can guide the development of privacy frameworks for connected device ecosystems.

---

[3] Future of Privacy Forum & Information and Privacy Commissioner, Ontario, Canada, *Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation* (2009), *available at* http://www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf. Another one of our Smart Grid initiatives was to develop a first-of-its-kind privacy seal program for companies providing consumers with services that rely on energy data. *See* Smart Grid, Future of Privacy Forum, http://www.futureofprivacy.org/issues/smart-grid/ (last visited March 19, 2014).

[4] Christopher Wolf & Jules Polonetsky, An Updated Privacy Paradigm for the "Internet of Things" (2013) [hereinafter FPF White Paper], *available at* http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf.

[5] The main text of these Comments summarizes important elements of the Code. The complete Code is attached as Appendix A.

II. Overview of Technologies Associated with Mobile Location Services

To detect nearby mobile devices, mobile location services simply collect the everyday signals emitted by mobile devices equipped with wireless connectivity. As described in this section and the following, mobile location services are an example of ordinary technologies being put to innovative use. Mobile devices come equipped with various antennae that facilitate wireless connectivity and communications. Connections to terrestrial mobile networks generally rely on LTE, GSM, or CDMA antennae, depending upon the type of network.[6] Wi-Fi antennae facilitate localized connectivity to the Internet or other networks. Bluetooth antennae are used for short-range device-to-device communications (*e.g.*, when smartphones are paired with wireless headsets, vehicle systems, or other smart devices).

Because multiple devices can connect to the same network, devices need to identify themselves. Otherwise, the network would not be able to single out which device is supposed to receive a specific communication. To solve this problem, unique identifiers are assigned to the networking components of mobile devices. When a mobile device transmits information to a network (such as sending an email or uploading a photograph), it broadcasts a unique device identifier so that the network knows where to send any associated response. For example, for GSM and CDMA networks, a Temporary Mobile Subscriber Identity ("TMSI") is a commonly assigned identifier, which consists of a four-octet hexadecimal number.[7] For LTE networks, a Globally Unique Temporary ID ("GUTI"), comprised of 80 bits, is used to identify connected devices. For Wi-Fi and Bluetooth connections, manufacturers assign media access control ("MAC") addresses to Wi-Fi and Bluetooth components.[8] These unique device identifiers by themselves do not reveal the identity of the person who is using the device.

Mobile devices frequently must "probe" their surroundings to discover whether nearby networks are available and to enable devices to connect with those networks. They do so by

[6] GSM, CDMA, and LTE are wireless technology standards that, *inter alia*, facilitate high-speed mobile data transmissions to and from multiple terrestrial network terminals, such as telephone handsets, tablets, vehicles, and other devices.

[7] A hexadecimal number is expressed in base 16 with the numerals 0-9 representing the numbers 0-9 and the letters A-F representing the numbers 10-15.

[8] In standard format, a MAC address is expressed as six groups of two hexadecimal digits. A valid MAC address, for example, would be 00:1C:B3:09:85:15

emitting radio signals, and those signals contain the unique identifiers discussed in the previous paragraph. If a wireless sensor is active and near a mobile device that is emitting a probing signal of the right type (*e.g.*, a Wi-Fi probing signal for a Wi-Fi sensor), the sensor will detect the probing signal and the unique identifier broadcast with it. If the sensor is connected to a system that records when a particular probing signal was detected, the system knows when the mobile device came near that sensor.

Like any electromagnetic wave, the further a probing signal travels before it reaches a sensor, the weaker its signal strength. Wireless sensors can analyze the strength of a probing signal to infer the distance between the sensor and the device emitting the signal with an accuracy of a few meters. If a system is connected to multiple devices that collect probing signals in and around a particular venue, the system can use the information that each sensor collects over time to infer the approximate locations of devices at particular times and devices' movements through and around the venue over time.[9]

It is important to note again that the process described above *does not* involve the use of unique technologies or the collection of contact information, phone logs, text messages, videos, or other information that people store on their phones. Mobile location services collect only the periodic probing signals emitted by devices, which are the same signals that allow devices to detect and connect to wireless networks. In addition, as discussed below, the reports generated by mobile location service companies typically include only aggregate information, so the reports themselves are not likely to raise privacy concerns.

Airports, brick-and-mortar stores, malls, and other businesses and organizations are increasingly working with mobile location service companies to install sensors in and around locations to facilitate mobile location services. Although some mobile location service companies use sensors that detect the LTE, CDMA, or GSM signals used to connect to terrestrial mobile networks,[10] most use sensors that detect Wi-Fi and Bluetooth signals.[11] Those sensors

[9] Another way to determine the locations and movements of mobile devices that is likely familiar to most consumers is through the use of devices' Global Positioning System ("GPS") functionality, a satellite-based navigation system. However, GPS does not function in locations where satellite signals cannot reach. GPS is therefore of limited utility in airports, malls, and other indoor locations. For that reason, we do not further address GPS services in these Comments.

[10] *See Technology*, Path Intelligence, http://www.pathintelligence.com/technology/ (last visited March 19, 2014).

allow mobile location service companies to collect information about how devices move past and through various locations, including how many devices enter a business after passing by a window display, the number of times that a device has been to a particular location, where most devices travel through the space, what parts of the space are over or under used, what the peak periods of use are, how long devices stay in the space, and other information. Mobile location service companies share insights gleaned from this information with businesses and other organizations, typically by providing aggregate reports.[12] Examples of these reports are attached as Appendix B.

III. The Benefits of Mobile Location Services

Today's mobile location services can provide substantial benefits to consumers. For example, mobile location services can analyze the aggregated data about consumers' locations to learn whether consumers are spending more time waiting in lines than necessary. As a result, companies can use the data to minimize the amount of time that consumers spend in check-out lines, airport security queues, and lines to enter stadiums and entertainment venues by assigning extra staff or opening up additional registers or entry points. In addition, businesses can analyze how consumers move through locations and use that information to design layouts that reduce bottlenecks, make it easier for consumers to find desired goods, and otherwise make visits more enjoyable. Malls, sidewalks, and public spaces can be configured to accommodate more efficiently vehicle, bicycle, and foot traffic. Thus, when mobile location services are used effectively, consumers will spend less time waiting in lines, have an easier time finding what they want, and move more easily through locations.

Businesses also benefit from mobile location services. By understanding how many customers enter a store after passing by a window display, retailers can evaluate the effectiveness of promotions. By monitoring peak traffic periods, they can optimize staffing. Businesses can also determine whether they are designing their locations to make the most effective use of space. And businesses can use mobile location services to learn about the different trends and experiences associated with one-time visitors as opposed to return visitors.

---

[11] *See* Ann Cavoukian, Ph.D., Nilesh Bansal, Ph.D. & Nick Koudas, Ph.D., Building Privacy into Mobile Location Analytics (MLA) Through *Privacy by Design* 2-3 (2014).

[12] *See id.*

Another notable development from mobile location services is that brick-and-mortar businesses can use such services to enhance competition. Until the advent of mobile location services, brick-and-mortar stores were limited in their ability to learn about their customers' shopping habits and how to improve the shopping experience. With mobile location service reports in hand, brick-and-mortar businesses can learn more about how their customers shop, which will help offline businesses provide their customers with the experiences, goods, and services that they want. This can in turn lead to lower prices and better service for consumers as brick-and-mortar stores compete with their offline and online competitors.

IV. The Mobile Location Code of Conduct Addresses the Potential Concerns that Some Have Raised About Mobile Location Services in Retail Environments

A. Concerns raised about mobile location services

At the Seminar, some participants raised concerns about potential privacy risks that could result from new mobile location services. Seminar participants were in general agreement that, because the reports generated by mobile location service companies typically include only aggregate information, the reports themselves are not likely to raise privacy concerns.[13] Instead, the potential privacy concerns raised focused on the fact that mobile location service companies log information about the locations and movements of individual consumers' devices in and around particular venues over time. And that information may be associated with unique and persistent identifiers, like MAC addresses.

However, the MAC address of a device does not itself reveal the identity of a user. It is like the serial number associated with a toaster, television, or other device. We are not aware of any commercially available directory that would allow companies to look up MAC addresses in order to identify users.[14] If a consumer expressly provides personal information along with his or her MAC address, this information could be used to identify the person associated with the

[13] *See* Appendix B.

[14] The latest version of Apple's iOS technically prevents companies from using apps to access MAC addresses. Sarah Perez, *iOS 7 Eliminates MAC Address as Tracking Option, Signaling Final Push Towards Apple's Own Ad Identifier Technology*, TechCrunch (June 14, 2013), http://techcrunch.com/2013/06/14/ios-7-eliminates-mac-address-as-tracking-option-signaling-final-push-towards-apples-own-ad-identifier-technology/.

MAC address.[15] This express linkage, used with permission, could enable useful services. For example, a store could detect the arrival of a customer and immediately deploy an employee to retrieve a product that the customer ordered for pickup.

Some have expressed concerns that consumers' movements in and around venues could reveal information about those consumers' activities that could be used in an adverse manner or shared with insurance companies, credit providers, health insurers, or employment agencies.

Some have also expressed concerns that mobile location services may lack transparency and that consumers may not understand how the associated technologies work. For example, some note that consumers may not be aware that their devices are transmitting probing signals, that those signals contain unique identifiers, or that the signals can be used to record the locations and movements of a device over time. They also note that consumers may not know that they can prevent the transmission of Wi-Fi and Bluetooth probing signals by turning off their Wi-Fi and Bluetooth functionality. And consumers may not know that mobile location service companies collect information to provide insights to businesses and other organizations.

B. How the Code addresses the potential concerns

The Code reflects input from mobile location service companies and is designed to address the potential concerns described above that have been raised about mobile location services. The Code is a flexible document. FPF will monitor the development of technologies and concerns associated with mobile location services and can modify the Code as needed to address any new developments. FPF will look to the FTC and other stakeholders for input as we seek to address new technologies and concerns.

Transparency. To address concerns that consumers may not be aware of or understand retailers' use of mobile location services, the Code requires that participating providers of mobile location services support consumer-education initiatives and encourage the companies using their technologies to conspicuously display signage informing consumers about the use of mobile location services. These notices will include information about where consumers may go to find

[15] The Code requires companies to obtain affirmative consent from consumers prior to linking personal information with a MAC address. Mobile Location Analytics Code of Conduct, III.b. [hereinafter "The Code"] attached as Appendix A and *available at* http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf.

more information about how mobile location services work and the choices consumers have about the collection of information for mobile location services. These and other provisions of the Code will help ensure that consumers understand how mobile location services work, alert consumers when a retailer has engaged a mobile location service company to collect information in a particular venue, and inform consumers about the steps that mobile location service companies take to protect the information they collect.[16]

Choice. To respect consumer choice, the Code provides consumers with the opportunity to opt-out of having their mobile devices' identifiers used to support mobile location services.[17] Recording only the types of devices detected[18] or the number of times that unspecified devices encounter a network would not require choice because that information does not involve the collection of user-specific or individually identifiable information that could lead to the concerns that some have raised.

FPF has launched a centralized website that provides consumers with the ability to opt-out of having participating mobile location service companies use device- or user-specific information for mobile location services.[19] To opt-out, consumers enter the MAC addresses for the devices that they wish to exclude from mobile location services. Once a MAC address is entered, participating companies may use the MAC address only to maintain the device's opt-out status. A screen shot of the beta opt-out page is attached as Appendix C.

The Code also respects consumer choice by requiring participating mobile location service companies to obtain affirmative consent if personal information will be linked to a device identifier (*e.g.*, MAC address) or if a consumer will be contacted based on information collected for mobile location services. "Affirmative consent" is defined in the Code as "an individual's action in response to a clear, meaningful, and prominent notice regarding the collection and use" of the information.[20]

---

[16] *Id.* at I, VII.

[17] *Id.* at III.

[18] Manufacturers often assign MAC addresses in such a way that the addresses reveal their devices' manufacturers and types.

[19] *See Opt Out of Smart Store Tracking*, Smart Store Privacy, https://optout.smartstoreprivacy.org/ (last visited Mar. 19, 2014).

[20] The Code, *supra* note 15, at IX.

Preventing Harm to Consumers. The Code also includes several provisions to address the concerns raised by some about the possibility that information collected for mobile location services could facilitate the creation of individually identifiable location histories that could be used for purposes adverse to consumer interests. First, the Code prohibits participating companies from using information collected in an adverse manner for employment eligibility, promotion, or retention; credit eligibility; eligibility for health care treatment; or insurance eligibility, pricing, or terms.[21] Under the Code, participating companies may collect consumers' personal information (*e.g.*, names, physical addresses, or email addresses) or unique device identifiers (*e.g.*, MAC addresses) only if consumers affirmatively consent or if the information is promptly de-identified or de-personalized.[22] The same restrictions hold if participating companies wish to link data to a unique device identifier.[23]

The Code also reflects that technical anonymization measures alone cannot guarantee that data can never be re-identified.[24] Therefore, in addition to technical anonymization measures, the Code requires participating companies to rely on administrative safeguards, including publicly committing to not re-identify the data and prohibiting downstream recipients from attempting re-identification.[25] The Code requires participating companies to maintain data retention policies.[26] And participating companies that disclose information broadcast by consumers' mobile devices (*i.e.*, the probing signals) to unaffiliated third parties may do so only if those parties are contractually required to comply with the Code when using the information.[27]

---

[21] *Id.* at IV.

[22] *Id.* at II. The Code defines "de-identified" data as that which "is not reasonably used to infer information about a particular consumer, computer or other device." *Id.* at IX. "De-personalized" data is "that which is not reasonably used to infer information about a particular individual, but that may be associated with a particular computer or device." *Id.*

[23] *Id.* at II.

[24] *See generally* Yianni Lagos & Jules Polonetsky, *Public vs. Nonpublic Data: The Benefits of Administrative Control*, 66 Stan. L. Rev. Online 103 (2013), *available at* http://www.stanfordlawreview.org/online/privacy-and-big-data/public-vs-nonpublic-data.

[25] The Code, *supra* note 15, at IX.

[26] *Id.* at VI.

[27] *Id.* at V.

Together, these provisions reduce the risk that information collected for mobile location services will be used in a manner adverse to consumers' interests.

V. The Code Is an Example of How a Use-Based Framework Can Promote Privacy for Connected Device Ecosystems

As mentioned above, to coincide with the FTC's workshop examining the privacy and security issues associated with the Internet of Things, FPF released the White Paper discussing how flexible, use-based standards that implement the FIPPs in non-traditional ways may be needed to promote privacy for connected, smart technologies.[28] The FIPPs are designed to serve as high-level guidelines for the processing of information.[29] Although traditional implementations of the FIPPs—such as the presentation of detailed privacy policies prior to the collection of information—have served well in many contexts, there is widespread agreement that connected, smart technologies will sometimes present challenges for traditional methods of implementing the FIPPs.[30] The Code is an excellent example of how the use-based privacy framework proposed in the White Paper can be used to promote privacy in the world of connected devices by implementing the FIPPs in a "use-based manner" that focuses on the context in which specific types of data are used.

Using anonymized data minimizes privacy impacts.[31] When appropriate anonymization practices that take advantage of technological measures and administrative

---

[28] FPF White Paper, *supra* note 4.

[29] OECD, OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data 13-14 (2013), *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf; The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 11-19, 21 (2012).

[30] *See* Opening Remarks of FTC Chairwoman Edith Ramirez, The Internet of Things: Privacy and Security in a Connected World, at 4 (Nov. 19, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/opening-remarks-ftc-chairwoman-edith-ramirez-federal-trade-commission-internet-things-privacy/131119iotremarks.pdf; Remarks of Commissioner Maureen K. Ohlhausen, Consumer Electronics Show, Promoting an Internet of Inclusion: More Things AND More People, at 3 (Jan. 8, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/promoting-internet-inclusion-more-things-more-people/140107ces-iot.pdf; Remarks by Commissioner Julie Brill, FTC, Keynote Address, Proskauer on Privacy, at 2 (Oct. 19, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/remarks-commissioner-julie-brill/101019proskauerspeech.pdf; FPF White Paper, *supra* note 4, at 3-7.

[31] FPF White Paper, *supra* note 4, at 7-9.

safeguards are used, privacy risks are minimal. As discussed in FPF's comments submitted following the FTC's Workshop on the Internet of Things, the use of anonymized data is one way to implement the FIPP of Data Minimization.[32] The Code promotes the use of anonymized data by allowing mobile location services to be free of the requirement to provide notice if data collected is not unique to a device or user and individual information is not retained. When data is unique to a device, but not an individual user, the Code requires participating companies to take reasonable measures to prevent identification, publicly commit to not identifying data, and require unaffiliated recipients of the data to not use the data to identify individuals.

Consider the context in which personally identifiable information or other information that raises potential and reasonable privacy concerns is collected.[33] When organizations use information in a manner that respects the context in which the information was collected, those uses should be permitted. This is one way to implement the FIPP of Use Limitation.[34] If reasonable consumers expect a given use of information, that use should be allowed because it does not implicate reasonable privacy concerns. The Code reflects the principle of respecting the context of collection in the following ways:

- The Code does not restrict participating companies from using information to manage, operate, or test a Wi-Fi network.[35] Reasonable consumers would expect that companies would use probing signals or transmissions sent over a Wi-Fi network to be used in these ways.
- The Code does not restrict participating companies from using information to address security, fraud, legal compliance, or threats to the safety, property, or rights of individuals.[36] Although some consumers may not expect that probing signals could be used for these purposes, such uses deliver substantial benefits and would likely be embraced by consumers.

---

[32] Future of Privacy Forum, Comments of the Future of Privacy Forum, RE: Internet of Things, Project No. P135405, 7 (Jan. 10, 2014) [hereinafter Internet of Things Comments], *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/2014/01/00013-88250.pdf.

[33] FPF White Paper, *supra* note 4, at 9.

[34] Internet of Things Comments, *supra* note 32, at 7.

[35] The Code, *supra* note 15, at VIII.a.

[36] *Id.* at VIII.b.

- The Code does not limit employer-employee use of mobile location services because such use should be addressed in the context of the employer-employee relationship[37]—not in a framework designed to address consumer concerns.

Be transparent about data use.[38] Organizations can implement the FIPP of Notice by transparently disclosing their data practices. The Notice and Consumer Education Principles of the Code help ensure that consumers understand and are aware of the use of mobile location services. As discussed in our White Paper, the level of transparency required of organizations should be tailored to the nature of the information collected and the purposes for which it will be used. The Code reflects this principle by not requiring in-store notices if participating companies do not collect information in a form that uniquely identifies individuals or devices.[39]

Develop Codes of Conduct.[40] Self-regulatory codes of conduct are an effective means to promote accountability and privacy in the development of new technologies and services. Self-regulatory frameworks, such as the Code, allow for flexible implementation and can be modified to address developing concerns. When self-regulatory frameworks require participating companies to make public commitments about how information will be collected, used, shared, and retained, the FTC has in the past used its Section 5 authority to enforce those frameworks. The Code illustrates how companies can work together to establish enforceable codes of conduct that promote privacy and offer reasonable consumer choice.

VII. Analytics and Privacy Requirements

In many other frameworks and codes of conduct, the use of data for analytics does not generally warrant the implementation of privacy requirements such as enhanced notices or consumer choice.[41] We have supported this view, as the use of analytics data does not ordinarily call for measures as robust as those required by the Code. However, the Code recognizes the potential sensitivity of location data that is collected over time and linked to a device identifier

[37] *Id.* at VIII.c.

[38] FPF White Paper, *supra* note 4, at 10.

[39] The Code, *supra* note 15, at I.b.

[40] FPF White Paper, *supra* note 4, at 11.

[41] *E.g.*, FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 38-39, 53 (2012); Network Advertising Initiative, 2013 NAI Code of Conduct 6 (2013), *available at* http://www.networkadvertising.org/2013_Principles.pdf.

and therefore mandates additional privacy measures, even when the data is generally provided to clients in aggregated form.

VIII. Conclusion

FPF appreciates the opportunity to engage with the Commission on mobile location services and looks forward to further engagement with the Commission, mobile location service companies, retailers, and other stakeholders working to promote consumer privacy and innovation. Mobile location services are one example of the innovative technologies and services that mobile technologies and the Internet of Things can offer. The companies participating in the Code recognize that consumer trust and engagement are vital to the development of mobile location services. And they further recognize that consumers will not engage if their privacy interests are not promoted.

Respectfully submitted,

/s/ Jules Polonetsky
Jules Polonetsky
Co-Chair and Director

/s/ Christopher Wolf
Christopher Wolf
Founder and Co-Chair

FUTURE OF PRIVACY FORUM
919 18th Street NW
Washington, DC 200036

March 19, 2014

Appendix A
Mobile Location Analytics
Code of Conduct

Preamble

Mobile Location Analytics (MLA) provides technological solutions for Retailers by developing aggregate reports used to reduce waiting times at check-out, to optimize store layouts and to understand consumer shopping patterns. The reports are generated by recognizing the Wi-Fi or Bluetooth MAC addresses of cellphones as they interact with store Wi-Fi networks.

Given the potential benefits that Mobile Location Analytics may provide to businesses and consumers, it is important that these practices are subject to privacy controls and are used responsibly to improve the consumer shopping experience. This Code puts such data protection standards in place by requiring transparency and choice for Mobile Location Analytics.

Who Is Covered

This Code is intended to provide an enforceable, self-regulatory framework for the services provided in the US to Retailers by Mobile Location Analytics ("MLA") Companies.

I. Principle One: Notice

MLA Companies shall provide consumers with privacy notices that are clear, short, and standardized to enable comprehension and comparison of privacy practices.

a. MLA Company Privacy Notice

MLA Companies 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 steps shall include proposing standard or model contract language, providing companies with model language for in-store signage, developing a standardized symbol or icon to be included with such signage, and using other reasonable efforts to promote the use of in-store signage where MLA technology is used. Such signage shall provide information about how consumers can find additional information and exercise choice. Such signage shall also include a standardized symbol intended to help alert consumers to the use of MLA and other technologies. This Code does not intend to restrict notice to physical signage only. As other forms of just-in-time notice become feasible, this Code may be updated to reflect that these notice techniques also satisfy this requirement.

The following model language, in combination with a standardized symbol, satisfies the in-store notice requirement: "To learn about use of customer location and your choices, visit "www.smartstoreprivacy.com."

MLA Companies shall provide a detailed privacy notice at their websites which describes the information they collect and use and the services they provide. This notice should be separate

from and in addition to a notice describing information collected by the MLA Company's website itself. This detailed notice shall include the following information:

- Information collected by the MLA service;
- Steps taken to protect, de-identify, or de-personalize any tracking identifiers collected and statement of commitment not to re-identify data;
- A data retention statement;
- Information about data sharing, including law enforcement access;
- Description of whether data is provided to clients in individual or aggregate form;
- Disclosure about appending additional data to any unique user profile;
- How consumers can exercise any choices required by this Code;
- A method that consumers can use to contact the MLA Company with privacy questions; and
- A consumer-friendly description of how the technology works or a link to such information on the MLA Company site or at a Central Industry Site.

b. Exceptions to Principle One

Notice does not have to be provided when (1) the information logged is not unique to an individual device or user, or (2) it is promptly aggregated so as not to be unique to a device or user, and individual information is not retained.

For example, simply logging device types encountered does not require notice, nor does counting the total number of times unspecified mobile devices have been detected by a network. If a company only provides aggregated data to clients but still collects and retains device-level information, this exception will not apply and notice must be provided.

MLA Companies relying on this exception shall describe the steps taken to aggregate such data.

II. Principle Two: Limited Collection

Unless covered by the Exceptions in this Code, MLA Companies 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. In the provision of MLA services, MLA Companies shall not collect personal information or unique device information, unless it is promptly de-identified or de-personalized, or unless the consumer has provided affirmative consent. MLA Companies that collect MAC addresses or other unique device identifiers shall ensure this information meets the definition of De-personalized data as set forth in this Code, unless they obtain Affirmative Consent or other Exceptions apply.

If MLA Companies append data or add third party data to a user's profile that includes a device identifier or a hashed device identifier, they shall disclose such practices in their privacy notice. Any process used to link data to a unique device identifier, shall employ methodologies that maintain the data's de-identified or de-personalized status, unless a consumer has provided Affirmative Consent to the use of MLA Data.

III. Principle Three: Choice

MLA Companies shall provide consumers with the ability to decline to have their mobile devices used to provide retail analytics services. Information about how to exercise this choice shall be provided in a MLA Company Website privacy notice.

MLA Companies shall provide a link to the Central Industry Site which provides the Central Opt-Out. The MLA Company Website privacy notice may also provide a MLA Company specific opt-out.

a. Exceptions to Principle 3

Choice does not have to be provided when the information logged is not unique to an individual device or user, or it is immediately aggregated so as not to be unique to a device or user, and individual information is not retained.

For example, simply logging device types encountered does not require choice, nor does counting the total number of times unspecified mobile devices have been detected by a network. Logging the total number of unique devices detected requires choice because it necessitates recording device-level information in order to distinguish new devices from previously detected ones.

When a consumer exercises an opt-out choice, the MLA Company will no longer associate information with a unique mobile device identifier and will only use the identifier in order to maintain the device's opt-out status. Informing consumers that turning off their mobile devices, or turning off Wi-Fi or Bluetooth, are not considered by themselves to be choice options that qualify as an opt-out when required by this Code. This Code seeks to be technologically neutral and does not dictate a particular opt-out method in order to encourage new and effective methods to offer choice. However, any method of opt-out choice provided in order to satisfy this Code must allow a consumer to maintain full use of mobile device features.[1]

b. Affirmative Consent

A consumer's Affirmative Consent shall be required in the following circumstances:

1) Personal information will be linked to a mobile device identifier; or

2) A consumer will be contacted based on MLA information.

IV. Principle Four: Limitation on Collection and Use

[1] We note that some devices do not provide consumers the ability to view the device's MAC address and thus at this time it is not feasible to provide those consumers with a choice option. In the future, it may be possible to provide a method for such MAC addresses to be collected by an opt-out mechanism.

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.

V. Principle Five: Onward Transfer

MLA Companies that provide MLA Data to unaffiliated third parties shall contractually provide that third party use of MLA Data must be consistent with the Principles of this Code.

VI. Principle Six: Limited Retention

MLA Companies shall set internal policies for data retention and deletion of unique device data. MLA Companies shall set forth a data retention policy in their privacy notice.

VII. Principle Seven: Consumer Education

a. Central Industry Site

MLA Companies shall participate in an industry-provided, consumer-focused website that presents information about how MLA services work and how information is collected and used by MLA Companies. Such a site shall be easy to access on mobile devices and shall include information about how to exercise choice. MLA Companies shall link to this site from their privacy notices. The Central Industry Site shall also provide the Central Opt-Out.

b. Standardized Symbol

MLA Companies shall develop a standard symbol that is intended to convey to consumers the concept of MLA services. Such symbol shall be used on the central industry site, on MLA Company websites, and on education materials and communications.

c. Education

MLA Companies shall participate in education efforts to help inform consumers about the use of MLA services.

VIII. Exceptions to the Principles

a. Operational Exclusion

Data that is collected for the purpose of managing or operating a Wi-Fi network, or for analysis used to test the operation of that network, is not subject to the restrictions in this Code.

b. Security Exclusion

Nothing in this Code shall be construed to limit the collection or use of data for security, fraud or legal compliance, or to protect the safety, property, or other rights of a company or its employees or customers.

c. Employee Exclusion

This Code does not limit an employer's right to use MLA Data within the context of an employer-employee relationship.

d. Affirmative Consent Exception

A MLA Company, Retailer or other entity that has obtained an Affirmative Consent that describes collection, use or sharing of MLA information is not subject to the limitations in this Code for that consumer.

IX. Definitions

Central Opt-Out – the Central Opt-Out shall provide consumers with an opt-out that is effective across all participating MLA Companies.

MLA Data – information broadcast by consumer mobile devices.

MLA Company – a non-Retailer entity that uses local sensors to collect information broadcast by consumer mobile devices for the purpose of providing analytics, market research, or other similar services.

Retailer – an entity that maintains a commercial location where it offers goods or services for sale to consumers and that is engaging an unaffiliated MLA Company to collect/analyze MLA data on its behalf.

De-personalized Data – data that is not reasonably used to infer information about a particular consumer, but that may be associated with a particular computer or device. Data is treated as depersonalized if a MLA company:

(1) takes measures to ensure that the data cannot reasonably be linked to an individual (for instance, hashing a MAC address or deleting personally identifiable fields);

(2) publicly commits to maintain the data as de-personalized; and

(3) contractually prohibits downstream recipients from attempting to use the data to identify a particular individual.

De-identified Data – data that is not reasonably used to infer information about or otherwise be linked to a particular consumer, computer, or other device. Measures such as aggregating data, adding noise to data, or statistical sampling are considered to be measures that de-identify data under this Code if a MLA Company:

(1) takes reasonable measures to ensure that the data is de-identified;

(2) publicly commits not to try to re-identify the data; and

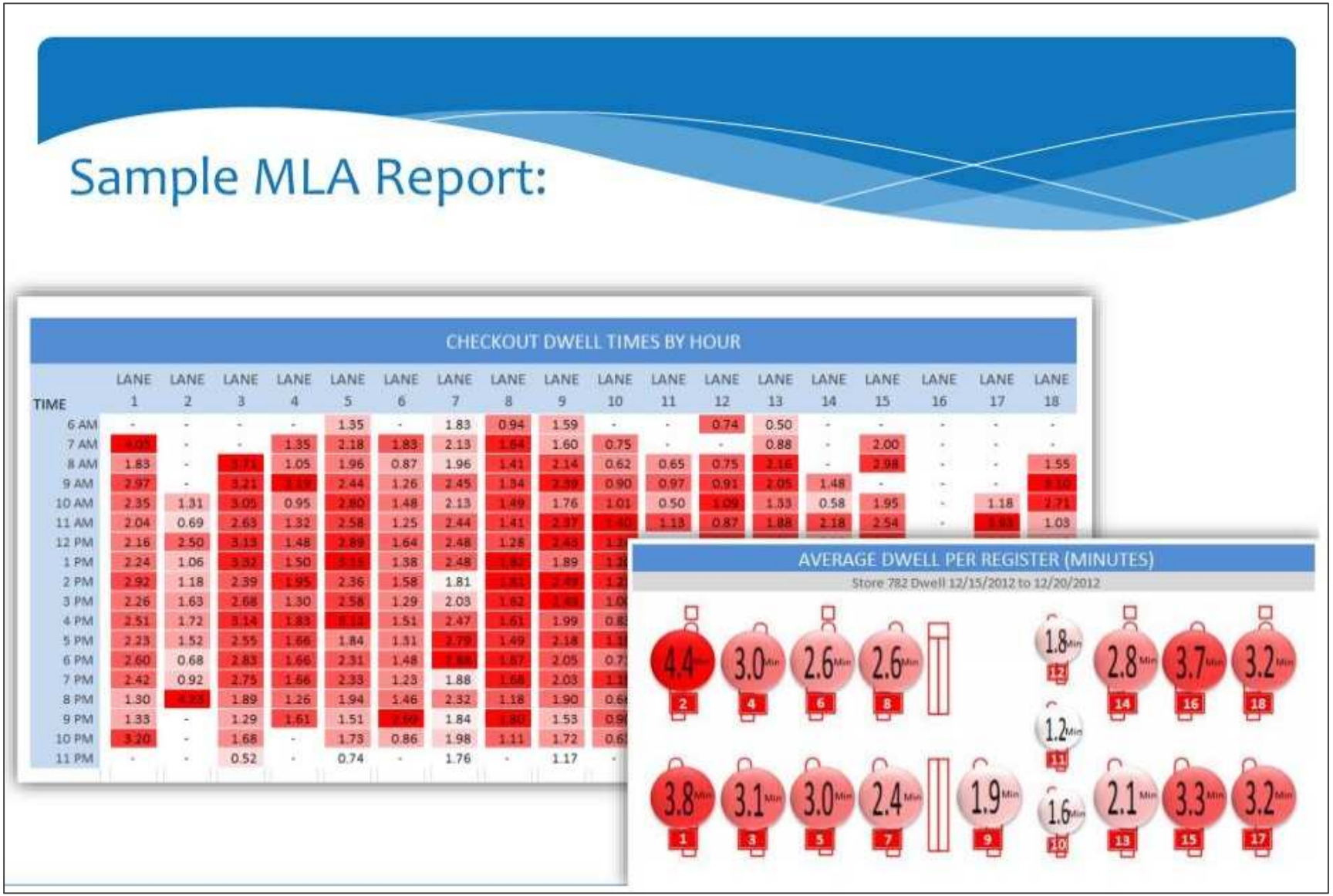
(3) contractually prohibits downstream recipients from trying to re-identify the data.

Unaffiliated Third Party – a company that is not controlled by, under the control of, or under common control of another entity.

Affirmative Consent – an individual's action in response to a clear, meaningful, and prominent notice regarding the collection and use of MLA Data.

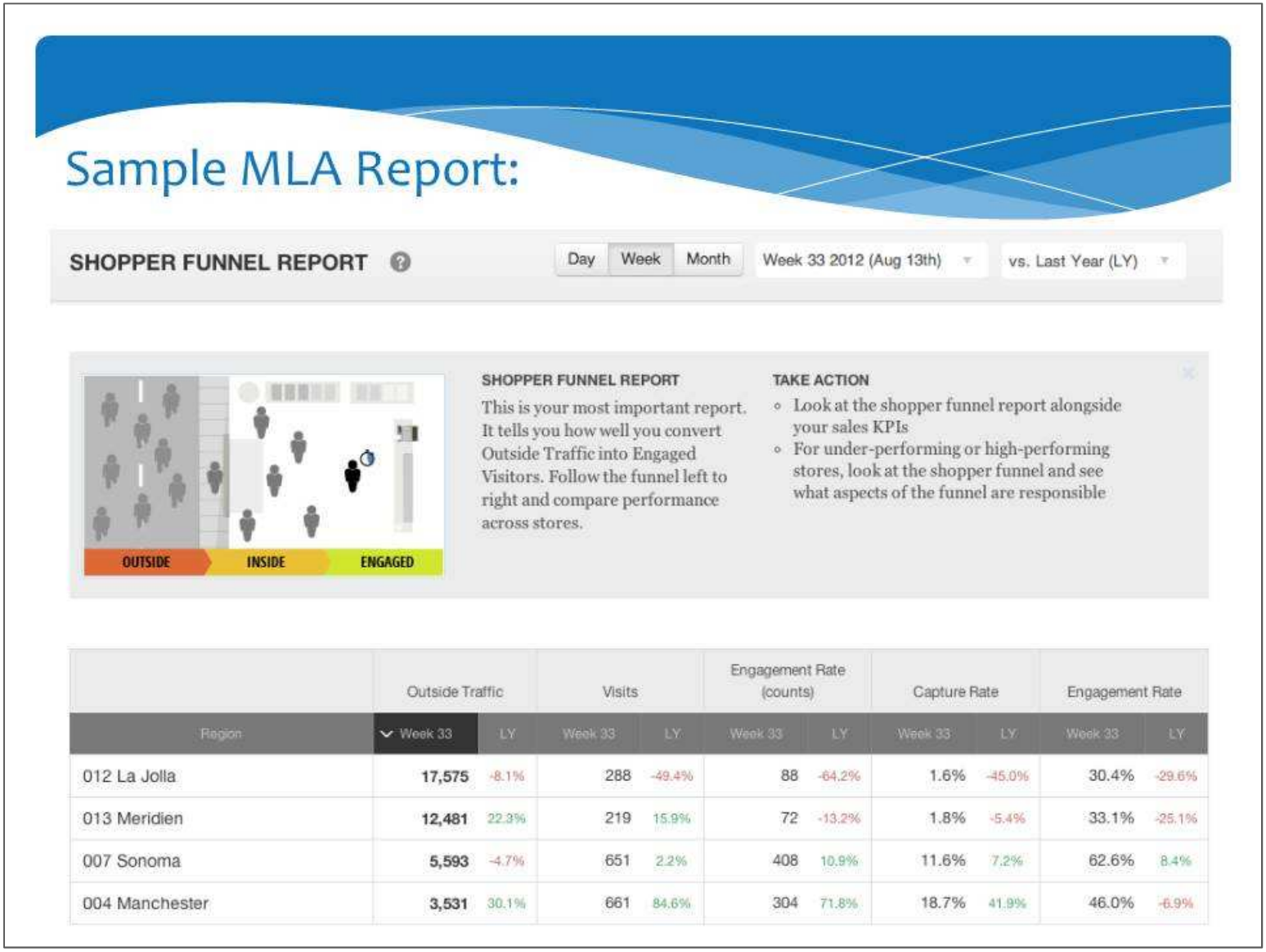
Personal Information – data considered personal information under this Code shall include personal identifiers such as name, address, email, and IMSI.

Appendix B
Sample Reports



Reports showing check-out wait times per hour and average check-out wait times over a certain period.

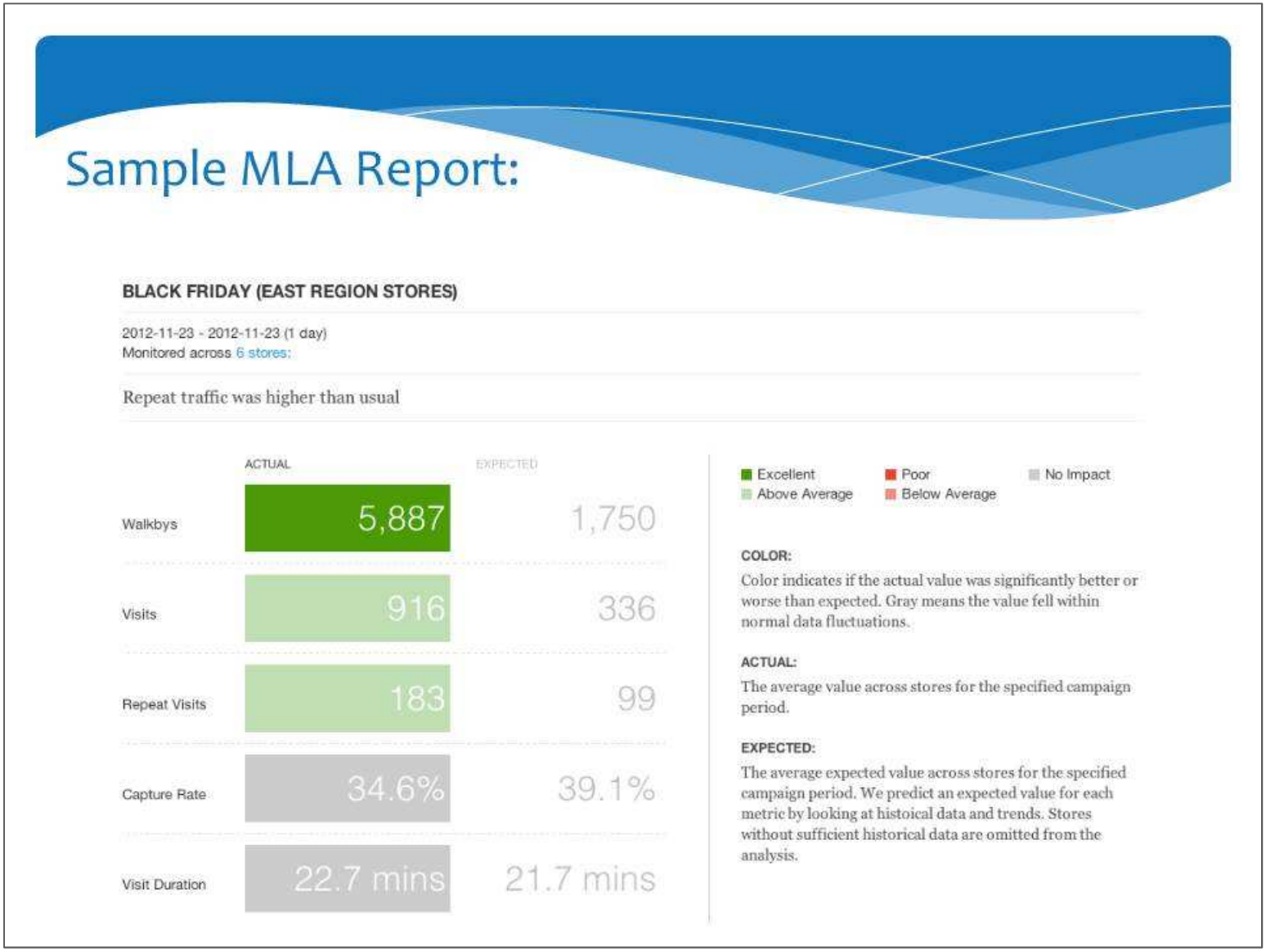
Appendix B
Sample Reports



	Outside Traffic		Visits		Engagement Rate (counts)		Capture Rate		Engagement Rate	
Region	Week 33	LY	Week 33	LY	Week 33	LY	Week 33	LY	Week 33	LY
012 La Jolla	17,575	-8.1%	288	-49.4%	88	-64.2%	1.6%	-45.0%	30.4%	-29.6%
013 Meridien	12,481	22.3%	219	15.9%	72	-13.2%	1.8%	-5.4%	33.1%	-25.1%
007 Sonoma	5,593	-4.7%	651	2.2%	408	10.9%	11.6%	7.2%	62.6%	8.4%
004 Manchester	3,531	30.1%	661	84.6%	304	71.8%	18.7%	41.9%	46.0%	-6.9%

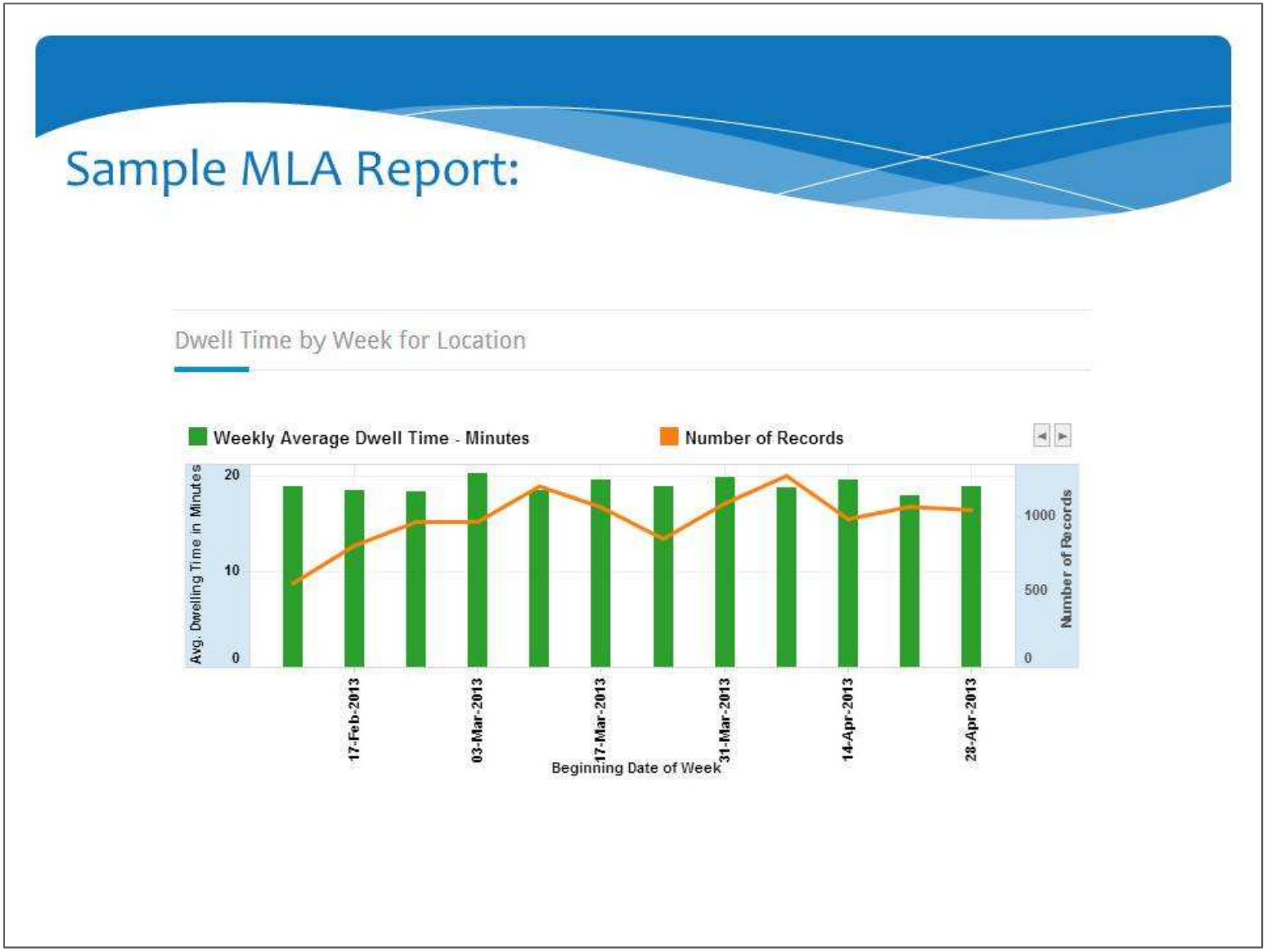
Report showing the conversion rate of outside traffic to engaged visitors.

Appendix B
Sample Reports



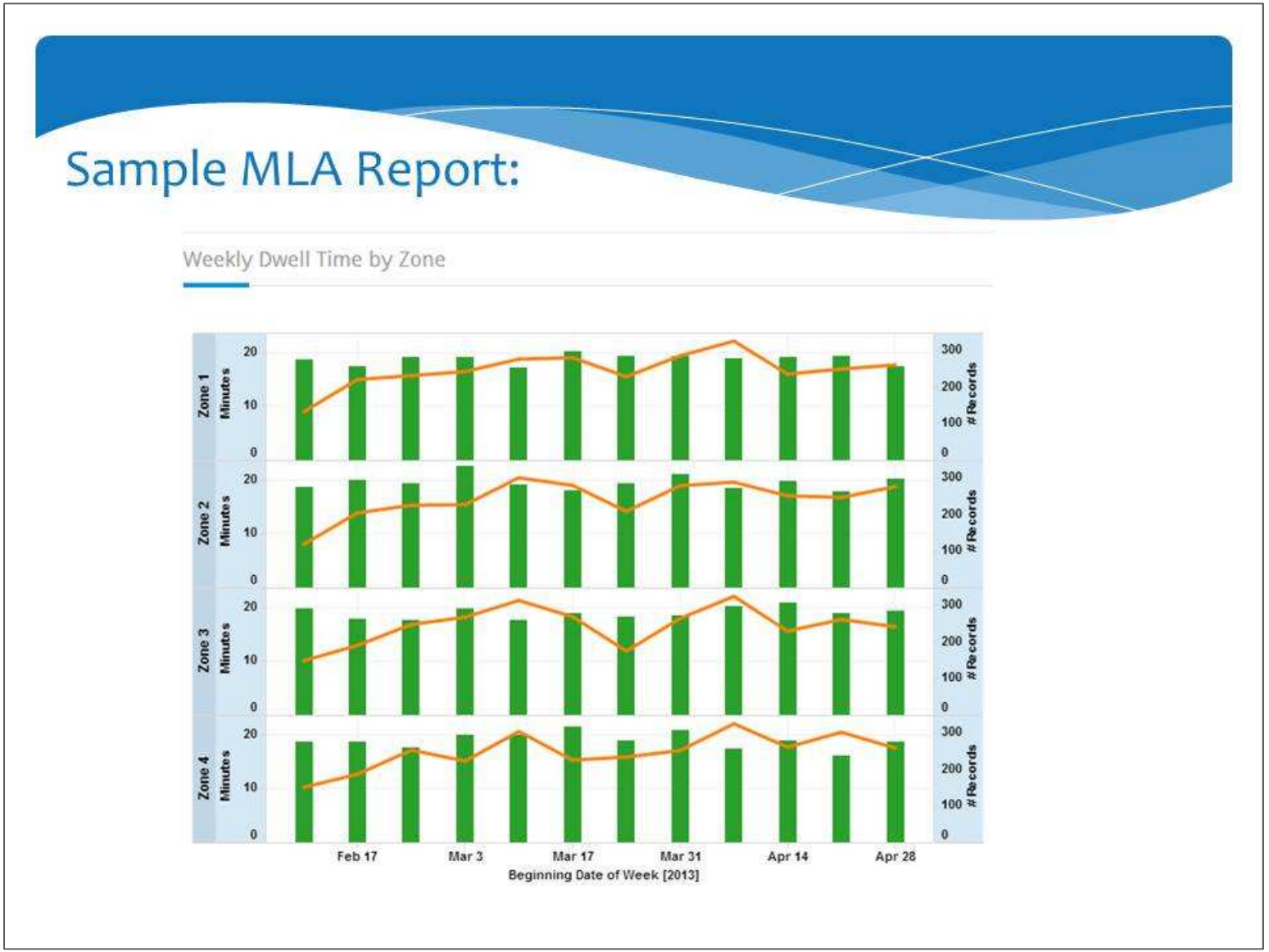
Report showing number of walkbys, visits, repeat visits, visit durations, and visitors captured on a particular day.

Appendix B
Sample Reports



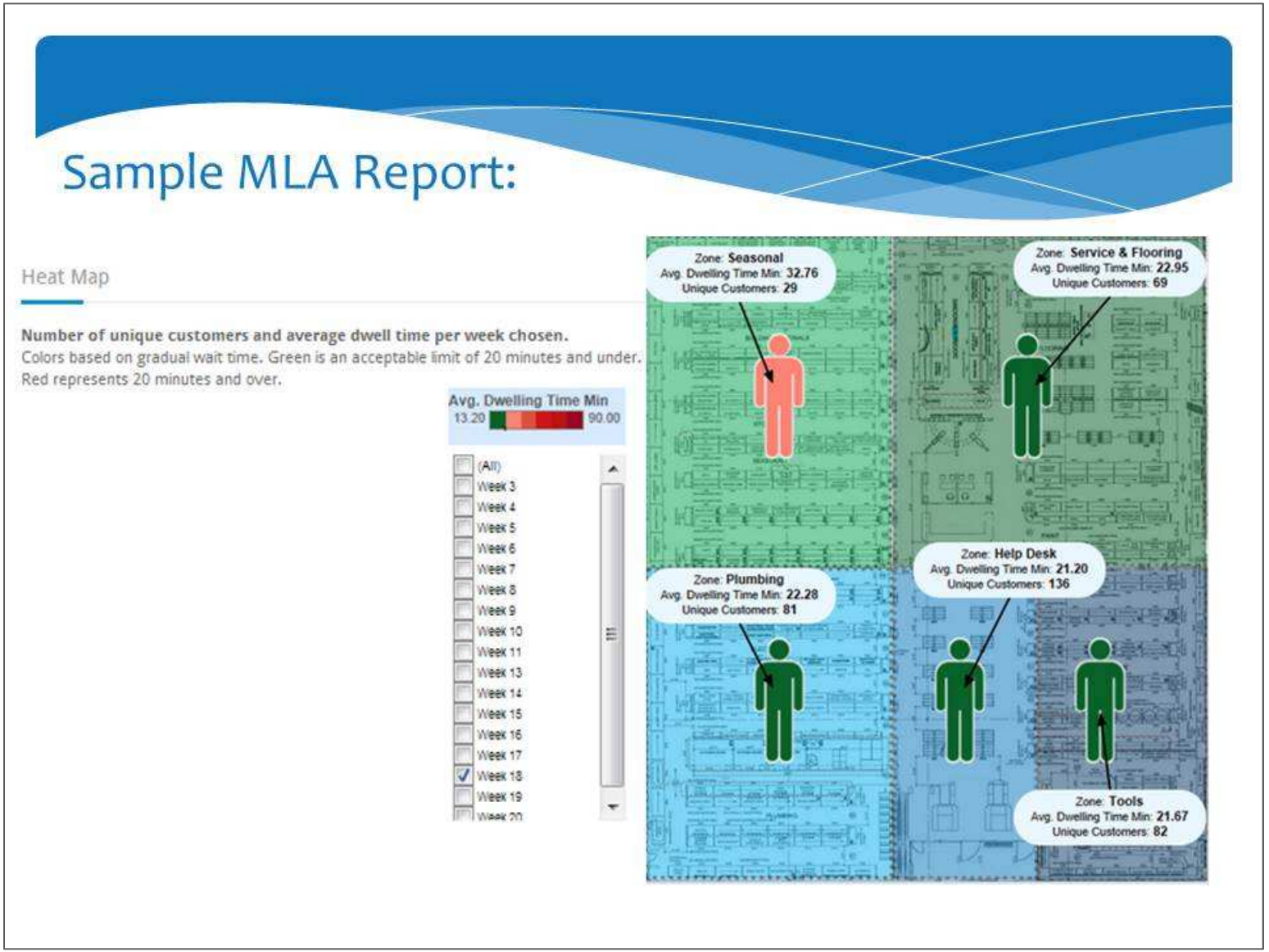
Report showing average dwell time and number of customers for 12 one-week periods.

Appendix B
Sample Reports



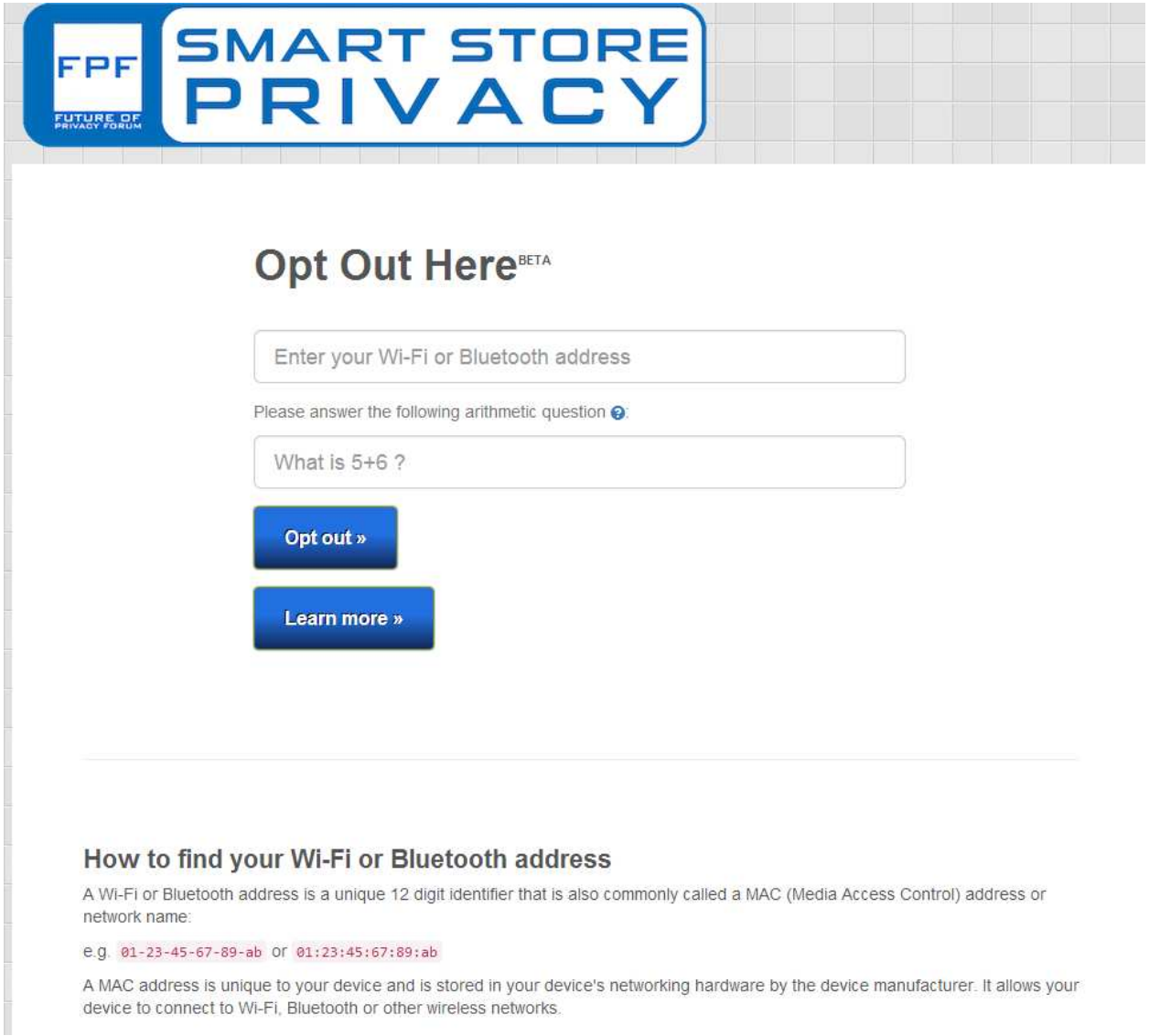
Report showing average dwell time and number of visitors in particular zones for 12 one-week periods.

Appendix B
Sample Reports



Report showing number of unique customers and dwell times in particular zones in a particular week.

Appendix C
Opt-Out Website



Appendix C
Opt-Out Website

Smart Phones and Tablets

Apple iPad, iPhone or iPod Touch

- Go to **Settings > General > About.**
- The Wi-Fi MAC is displayed in the field labeled "**Wi-Fi Address**" and the Bluetooth MAC is labeled "**Bluetooth.**"

Tip: Once you've found your MAC address, double-tap it to select it. Then, tap copy. Tap again in the opt-out field to paste.

Android Phone or Tablet

- Go to **Menu > Settings > Wireless & Networks.**
- Check the box marked **Wi-Fi** to ensure that wireless is turned on.
- Go to **Back > About Phone** or **About Tablet > Hardware Information.**
- The Wi-Fi MAC and the Bluetooth MAC are displayed here.

Blackberry Phone or Tablet

Wi-Fi Address for OS 4.5-5.0:

- Go to **Options > Status.**
- The Wi-Fi MAC is located in the field labeled "**WLAN MAC.**"

Wi-Fi Address for OS 6.0-7.1:

- Go to **Setup > Options > Device > Device and Status Information.**
- The Wi-Fi MAC is located in the field labeled "**WLAN MAC.**"

Bluetooth Address for all OS:

- Go to **Connections >Bluetooth > Properties.**
- The Bluetooth MAC is located here.

Appendix C
Opt-Out Website

Windows Phone or Tablet

Wi-Fi Address:

- Make sure your Wi-Fi is enabled.
- Go to **Start > Settings > Connections > Wireless LAN > Advanced.**
- The MAC address is displayed in the "**MAC**" field.

Bluetooth Address:

- Go to **Start > Settings > Connections > Bluetooth > Accessibility.**
- The Bluetooth MAC is listed as "**Address.**"