User Privacy and Beacons: Proximity Marketing and Privacy, A White Paper on the Future of Responsible Proximity Marketing

By
Alex Bell, CEO and Founder Signal360
and
Tim Bukher, Internet Law and Privacy Expert, Partner at Thompson Bukher LLP

This paper addresses how enterprises should think about consumer privacy in a world where companies are increasingly looking to market to and collect data from users in real-time within physical spaces (a.k.a. "proximity marketing"). We briefly explain aspects of proximity technology as it differentiates from other location-based technologies. We also explain how and why collection of personal information should be used in proximity marketing to achieve marketing goals while avoiding reputation loss to the industry. To that end, we lay out a series of steps that all companies should integrate into their products and agreements to remain transparent with consumers.

Proximity Marketing

While eCommerce has made extraordinary gains over the past ten years, the vast majority of retail in the United States occurs at physical retail locations.[1] Due to the relative ease of integration, eCommerce companies have used a wide array of technical solutions to both track users on their site, analyze their purchases and interests, as well as to market messages that would affect consumer action. The push to extend this data collection and marketing from eCommerce to physical locations has accelerated over the past five years as the penetration of smartphones has increased in the general population. As of today, every sizeable retail corporation is exploring and implementing technology solutions in their retail stores; but with little experience and successful use cases, the pitfalls are plentiful and the results, both positive and negative, will have much higher impact in "brick and mortar" than on the internet.

It is our opinion that the potential privacy concerns for proximity marketing are equal to those of the concerns faced in eCommerce; however, because proximity technology is relatively unknown to the average consumer, as well as its association with the user's physical locations, past and present, means that the potential blowback from consumers could be strong. In the proximity marketing industry, due to inappropriate and intentionally secretive campaigns by certain parties, we have already seen consumer concern and corrective action by government entities.[2] It is incorrect to assume that as an industry we will be able to educate the consumer about the technical specifications of its new system or to assume that this will sufficiently

[1] "US E-Commerce Sales as Percent of Retail Sales: 6.40% for Q2 2014", *YCharts*. YCharts, Inc., 30 Jun. 2014, Web. 16 Oct. 2014. <https://ycharts.com/indicators/ecommerce_sales_as_percent_retail_sales>
[2] "Exclusive: Hundreds Of Devices Hidden Inside New York City Phone Booths," *BuzzFeed*. BuzzFeed, Inc., 6 Oct. 2014. Web. 14 Oct. 2014.

address consumer concerns. Based on our previous experience in the online advertising world, we believe an incomplete technical explanation will only increase the misunderstanding and distrust of the proximity marketing industry. The only solution, as we will lay out, is to be clear about the uses of the technology and to provide clear notice and choice to the consumer.

Proximity marketing is a new area of retail technology which is poised to satisfy two major enterprise requirements: providing data on consumers in a physical location as well as affecting consumer action through marketing with increasing sales. Proximity marketing is the process of delivering content to a user when she is in proximate to a certain physical location.[3] Proximity marketing is primarily different from geomarketing with respect to the level of precision that geomarketing delivers, in terms of content and analytics, based on a user's geographic location such as zip code, neighborhood or even latitude and longitude. For example, a notification sent to a user when the user is within an eighth of a mile of a store's location is a form of geomarketing. On the other hand, proximity marketing uses precision technology which localizes a user down to the meter level. In the proximity marketing case, a notification and message are sent to a user once the user has spent more than two minutes directly in front of the perfume display on the second floor. Another important differentiator between geomarketing and proximity marketing is that the delivery mechanism for proximity marketing is a smartphone application (or "app" for short). Without an app, which has been specifically coded to deliver proximity marketing, there is no ability to gather information nor to deliver marketing or other content.

Technology

A variety of technologies are currently being deployed and tested by enterprises to achieve the precision requirements of proximity marketing. The requirements for the technology are one meter accuracy and passive notification ability (the ability to send a notification or interact with the proximity marketing device when the smartphone application in question is closed). To meet these requirements, a technology must be centered around a transmission mechanism which can deliver data to an app regardless of the app's state. The transmission technologies available are Near Field Communication (NFC) , Bluetooth Low Energy (BLE), WiFi, Audio Communication and Visible Light Communication (VLC.) Of these technologies, only BLE and Audio Communication satisfy the necessary requirements and are being most heavily adopted by retailers (see the Appendix for reasons why the other technologies are not considered Proximity Marketing[4]). Both technologies are usually packaged in devices called "beacons" which house the transmission mechanisms, whether BLE or Audio, and are installed at physical locations.

[3] "Proximity Marketing." *Wikipedia: The Free Encyclopedia.* Wikimedia Foundation, Inc., 8 Oct. 2013, Web. 14 Oct. 2014.

[4] Appendix A1.

In the most popular and secure variety, the beacons are broadcast devices, they do not have the ability to receive data nor do they have any form of networking in order to transmit information to a server. They are simple devices which transmit encrypted and, ideally, secure identifiers repeatedly. Smartphone applications can include software to receive these broadcasts and decode the beacon identifiers. These identifiers are used to query other sources such as Content Management, Ad Network, Loyalty and other Enterprise systems to deliver a notification or content to a user. Information about the device's reception of the identifiers is transmitted to analytics systems which are used to provide data on consumer usage. It is important to stress that at no point is the beacon performing any tracking or collecting of information. This is very different than other solutions, such as WiFi and Camera tracking, which do, indeed, collect information about the user. In its current implementation, the beacon devices are searched out by smartphone applications and it is the consumer's phone which performs the reception and the transmission of data. This is a very important distinction as it allows for complete **notice and choice** in the application.

In order to receive signals from the beacons, the following permissions are required depending on the transmission mechanism: For Bluetooth Low Energy transmission on iOS, the user must accept the "Use Location" permission for the application and, for Android, the application must have the "pair with bluetooth devices" and "update bluetooth settings" permissions set. For Audio Communication on iOS, the user must accept the "Use Microphone" permission and, on Android, the application must have the "record audio" permissions set[5][6].

Benefit to the Consumer

The benefits of Proximity marketing are not constrained to just the enterprise but extend to the consumer as well. The ability for the smartphone to localize itself with high precision allows for an array of use cases such as wayfinding in a store, product finder, information about nearby products, coupons and deals for bargain hunting consumers, and much more. As we will discuss in the implementation section, it is important that the consumer comes to view proximity marketing as a mutual benefit for herself and the retailer.

Personally Identifiable Information

While the use of Personally Identifiable Information ("PII") is not required for proximity marketing, it should be preferred by both consumers and enterprises. This may sound counter-intuitive but it is important to understand that proximity marketing without PII severely limits the customization that can be applied to the marketing delivered to a consumer. For example, if a sports stadium wants to provide information content to a user, by using PII

[5] "Location and Maps Programming Guide," *Apple*. Apple, Inc., 10 Mar. 2014, Web. 16 Oct. 2014. <https://developer.apple.com/library/ios/documentation/UserExperience/Conceptual/LocationAwarenessPG/Introduction/Introduction.html>

[6] "Bluetooth Low Energy," *Android*. Google, Inc., Web. <https://developer.android.com/guide/topics/connectivity/bluetooth-le.html>

information the stadium can make sure that information notifications about restroom facilities, sponsorship deals, and seat upgrades are only delivered to first-time visitors to the park, and that season ticket holders are delivered content which is relevant to season ticket holders such as clubhouse access or preferred parking. Without using the PII that the team already has access to, the content delivered is unfocused and less effective. Even more so, the delivered content can create intrusive and pestering messaging reminiscent of spam.

How To Do It

Up to this point, we have defined proximity marketing, presented its technical aspects, and discussed the benefits to consumers as well as the improvements that come with using PII. In the next section we will chart out a course of best practices to serve as guidelines for enterprises looking to implement proximity marketing.

Notice and Choice In App

The world of online advertisements has proven that the single most effective way to alleviate user concerns is to provide clear notice and choice.[7] Specifics are always important. To implement effective notice and choice with proximity marketing, considering the relatively young age of the industry, it is in the best interest of the enterprise to provide notice and choice at three levels: install, session, and content [comment]. While, as discussed previously, certain operating system level permissions are required, such permissions are, by themselves, not sufficient.

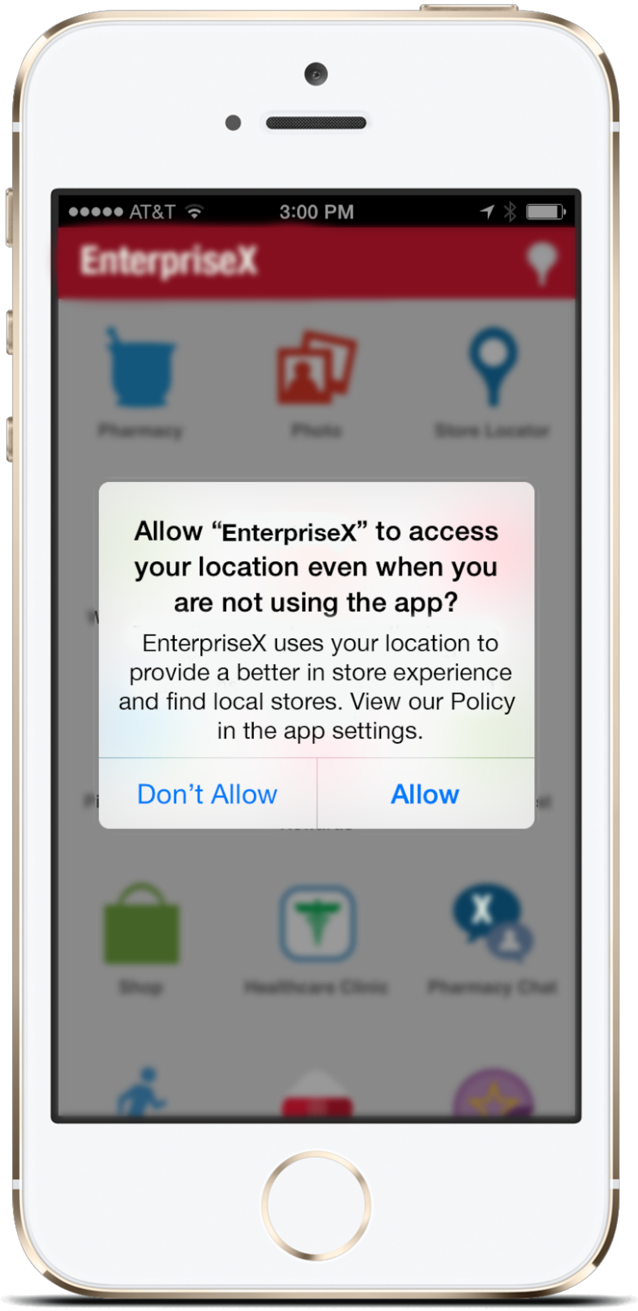
Upon installation, the application should inform the user of the intended use of operating system resources for proximity marketing. The user should have a clear opt-in that requires her consent. In addition there should be a session-level permission which governs the use of proximity marketing for the entirety of the user's current session. It is important that the user be able to decide for a single visit that they are no longer interested in receiving messaging -- this might not extend beyond that particular visit.

For iOS applications, it is our recommendation to provide information in the operating system level notifications which explain the application's use. We believe that a separate additional opt-in for proximity marketing is not necessary and provides a poor user experience as it adds yet another popup upon installation. See below for an example of opt-in for location services, notifications, as well as the optional, but not recommended, separate proximity marketing prompt.

[7] "Consumer Data Privacy in a Networked World," *Whitehouse.gov*. U.S. Gov., 23 Feb. 2012, Web. 16 Oct. 2014. <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>

For Android applications, it is our recommendation to provide a separate prompt asking the user to opt-in. We make this recommendation because the Android operating system permissions are listed in the specification for the app in the Google Playstore, and downloading the app serves as acceptance. We believe this default approach is poor because it does not allow an application to request permission but allows a user to selectively enable or disable it at the operating system level. In order to be more transparent with the consumer, we therefore recommend a separate prompt. We have found that because the operating system prompts for location services, and other information sharing mechanisms, are not displayed as they are in iOS, the additional proximity marketing prompt is not onerous to the user.

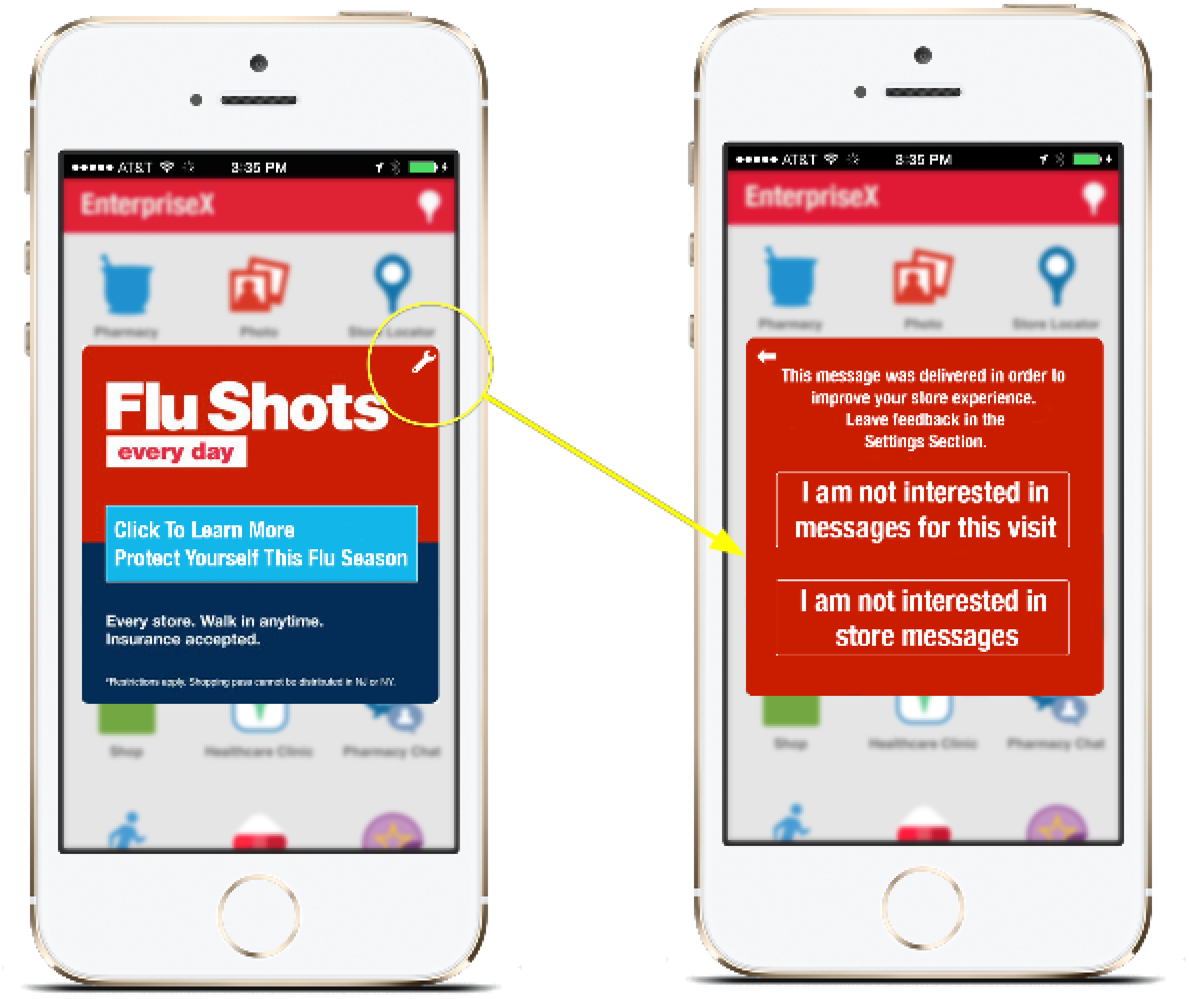
For additional operating systems, such as Windows Phone, it is our recommendation to follow the Android permission mechanisms.



Allow “EnterpriseX” to access your location even when you are not using the app?

EnterpriseX uses your location to provide a better in store experience and find local stores. View our Policy in the app settings.

iOS Operating System Prompt


AT&T
3:35 PM
EnterpriseX
Pharmacy
Photo
Store Locator
Flu Shots
every day
Click To Learn More
Protect Yourself This Flu Season
Every store. Walk in anytime.
Insurance accepted.
*Restrictions apply. Shopping pass cannot be distributed in NJ or NY.
Shop
Healthcare Clinic
Pharmacy Chat
I am not interested in messages for this visit
I am not interested in store messages

This message was delivered in order to improve your store experience. Leave feedback in the Settings Section.

iOS and Android Message and Session Notice & Choice

Privacy Policy

We recommend employing separate privacy policy documentation (a “Privacy Policy”) for proximity marketing-enabled smartphone applications from the standard online content mechanisms discussed above. While there will most likely be similarities between the two, we suggest a separate Privacy Policy in order to specify the differences in how PII is used. Below is an example of the relevant items we suggest should be included or addressed in addition to standard mobile privacy policies.[8]

[8] “Model Privacy Policy for Mobile Application,” *MMAGlobal*. Mobile Marketing Association, Inc., 15 Dec. 2011, Web. 16 Oct. 2014.<http://www.mmaglobal.com/whitepaper-request?filename=MMA_Mobile_Application_Privacy_Policy_15Dec2011PC_Update_FINAL.pdf>

1. The Privacy Policy should be separately accessible before and after installation. Specifically, applications should provide users with an option to review the Privacy Policy at any time post-installation.

2. The Privacy Policy should identify each specific type of PII (e.g., location data, content access, unique identifier, etc.) that will be collected by the application.

3. The Privacy Policy should specify, with reasonable detail, what purpose each type of PII will serve. It is no longer an industry “best practice,” nor can we endorse a PII Use clause that merely states that, “PII is collected to better deliver our services to the user.” Instead, a best practice example would state that, “Location data is collected in order for the application to provide the user with location-specific content [relevant to the core services meant to be provided by the application].”

4. The Privacy Policy should specify the specific third parties with whom PII would be shares and the specific reasons for such sharing. Again, it is no longer an industry “best practice,” nor can we endorse a PII Sharing clause that merely states that, “PII is shared with certain third party services to better the user experience.” Instead, a best practice example would state that, “PII is shared with [Specific Vendors X, Y and Z, and only Specific Vendors X, Y, and Z] to [e.g., provide analytics on specific user interaction which will be used to provide feedback for application improvement, or better targeted content.]”

The obvious question with respect to point 4 above is why a user would choose to continue using an application that admits to collecting PII for the purposes of “better targeted content” (which essentially means better advertising). The answer is “notice and choice” (see discussion above). In truth, most modern users no longer have a knee jerk reaction against any and all forms of PII collection or targeted advertising.[9]

Instead, modern users want to be provided with notice of how their PII will be used and a choice as to whether or not they want their PII used in that manner. Suggested best practices to convince users to choose in favor of limited PII collection and even sharing would include providing users with notice not only of those types of PII that will be collected and how they will be used and shared, but also the specific types of PII that will not be collected or the ways in which they would not be used or shared. Such simple considerations could maximize the retention of even the most privacy suspicious users, not to mention prevent additional suspicion or backlash against proximity marketing technology.

[9] “Right To Be Forgotten: Do users even care?” *Search Engine Land.* Third Door Media, Inc., 16 Jul. 2014, Web. 16 Oct. 2014. <http://searchengineland.com/right-forgotten-users-even-care-196464>

User Feedback

Our final suggestion is to provide a feedback mechanism in the application which is specifically tailored to proximity marketing. In our experience, it is better to allow users to directly comment on the experience from within the app. This would allow the enterprise an opportunity to address user concerns without engendering a poor user experience or leading to potentially misleading and damaging reviews on the relevant applications stores.

Conclusion

As members of the nascent proximity marketing industry it is incumbent upon ourselves to understand the long-term repercussions of how we, as an industry, present and interact with the general public. In this paper we have laid out the basics of proximity marketing and guidelines on how to implement notice and choice as it relates to proximity. It is our recommendation that all enterprises which engage in proximity marketing clearly provide notice and choice at all levels of the consumer interaction as well as provide clear opt-in installation and privacy policy documentation for the smartphone application.

Appendix

A1. Technology Included in the Definition of Proximity Marketing

To be included as a technology capable of proximity marketing, the capabilities must include the following:

- One meter accuracy
- Passive notification ability (the ability to send a notification or interact with the device when the app in question is closed.)
    - Specifically this must be possible on the vast majority of device types which means iOS and Android systems

The foregoing requirements are formed based on the use cases specified by enterprise retailers. While the passive notification ability can be argued, in our experience based on consumer action, a mechanism which is active and requires continued user action is not classified as proximity marketing and should be included in active technologies such as short codes, QR codes, and urls.

Based on these requirements the only current technologies which meet this requirement are:

- Bluetooth Low Energy
- Audio Communication

The following technologies are not included for the following reasons:

WiFi:

- Accuracy possible although difficult without substantial capital expense
- iOS prevents identifiable sniffing of MAC addresses of users from the WiFi router side
- iOS also prevents an application from scanning and reading a list of available SSIDs or identifiable WiFi hotspots

Near Field Communication (NFC):

- Accuracy debatable as the range is severely constrained
- iOS doesn't allow an application to access the NFC chipset
- Passive notification not possible, this is a active technology

Visible Light Communication (VLC):

- Never deployed at scale
- Access to cameras and light sensors not allowed if app is not in foreground, this prevents passive notification