BEACON TECHNOLOGY AND THE FUTURE/PRESENT STATE OF E-COMMERCE RETAIL SALES

Sophia Martin Schechner[1]

1. OMNICHANNEL RETAILING AND BEACON TECHNOLOGY: A BRIEF INTRODUCTION

On October 14, 2015, Walmart announced its plan to significantly increase its investment in e-commerce activity. The company stated that it will invest an estimated $1.1 billion into

[1] Sophia Schechner is currently an associate (pending admission to the NY bar) at Boyarski Fritz LLP, an entertainment law firm, where she works on a variety of matters, including digital and new technology, intellectual property, and legal research. Sophia earned her BA from Cornell University and her JD from Cardozo. In addition to practicing law, Sophia writes fiction and song lyrics. She would like to thank her parents Carol Martin and Richard Schechner, and her brother Sam Schechner for their love, support and guidance.

e-commerce and digital initiatives to "leverage Walmart's unique supply chain capabilities to lower costs and build deep digital relationships with customers."[2] A *New York Times* article subsequently reported that this announcement served as Walmart's implicit acknowledgment of their struggle to compete with Amazon in attracting online customers.[3] The article noted, "Walmart is hardly the only incumbent bricks-and-mortar chain that is threatened by Amazon and other increasingly sophisticated online retailers [. . .]."[4]

Real world retail merchants have met their match with online stores: "[d]uring the 2013 holiday shopping season, U.S. retailers received approximately half the holiday foot traffic they experienced just three years ago."[5] Declines went from 28.2% in 2011, 16.3% in 2012, and to 14.6% in 2013.[6] The falloff from shopping in brick-and-mortar stores is commonly attributed to the continued growth of online and mobile commerce.[7] Traditional brick-and-mortar retailers are responding by both trying to win back foot traffic sales and compete with online-only retailers. [8] Stores like Walmart are developing marketing

---

[2] *Walmart strategy drives growth and sustainable returns, Plans $20 billion share repurchase program over two years*, WALMART, http://news.walmart.com/news-archive/2015/10/14/walmart-strategy-drives-growth-and-sustainable-returns-plans-20-billion-share-repurchase-program-over-two-years (last visited Dec. 15, 2015).

[3] James B. Stewart, *Walmart Plays Catch-Up with Amazon*, N.Y. TIMES (Oct. 22, 2015), http://www.nytimes.com/2015/10/23/business/walmart-plays-catch-up-with-amazon.html?ref=business.

[4] *Id.*

[5] Brian K. Walker, *Retail in Crisis: These are the Changes in Brick and Mortar Stores Must Make,* FORBES, 1 (Jeremy Bogaisky ed.) (Feb. 12, 2014, 2:30 PM), http://www.forbes.com/sites/jeremybogaisky/2014/02/12/retail-in-crisis-these-are-the-changes-brick-and-mortar-stores-must-make/.

[6] Shelly Banjo & Drew Fitzgerald, *Stores Confront New World of Reduced Shopper Traffic: E-Commerce Not Only Siphons Off Sales, but Changes Shopping Habits,* WALL STREET J. (Jan. 16, 2014, 9:38 PM), http://www.wsj.com/articles/SB10001424052702304419104579325100372435802 ("Traffic to U.S. retailers was hurt during the financial crisis and recession, when job losses soared and shoppers kept a tight grip on their dollars. But nearly five years into the recovery, it appears many of those shoppers may never be coming back. Retailers got only about half the holiday traffic in 2013 and they did just three years earlier, according to ShopperTrak, which uses a network of 60,000 shopper-counting devices to track visits at malls and large retailers across the country.").

[7] Walker, *supra* note 5, at 2 (stating: "Online and mobile commerce continue to grow for both Web-based and traditional retailers. ComScore reported an increase of 10 percent in online spending during the 2013 holiday shopping season, and many retailers are reporting strong growth on their sites.").

[8] *Multi Channel Retailing*, *Multi-Channel Shopper in UK and US*, MULTI

strategies that work both in relation to "shopping-live" and shopping digitally. A large part of this fight to win back sales involves implementing Omnichannel retail mechanisms into their business strategies.[9] Omnichannel refers to the ability of retailers to use various online channels to communicate with customers in addition to, or instead of, traditional brick-and-mortar storefronts.[10]

Thus online stores, mobile stores, app stores and Internet based mass-communication all work together in aiding sales either online or in-store. Omnichannel is driven by the idea that the use of various available channels and customer touchpoints are synchronized in such a way as to "deliver a unified and consistent—albeit contextualized—customer experience."[11] At the vanguard of the shift to Omnichannel marketing are beacons, which have been described as "among the most important new mobile technologies helping real-world merchants win back sales."[12]

Apple, which has been leading in the beacon paradigm with its iBeacon implementation,[13] describes beacons as "the enabling

---

CHANNEL RETAILING, 3 fig., 4 fig., (last visited Apr. 5, 2016), http://www.options-mailorder.co.uk/images/images/Multi%20Channel%20Retailing%20Infographic.jpg (showing why retailers in the U.S. and U.K. must implement Omnichannel market channels through illustrative statistics).

[9] *See* Walker, *supra* note 5, at 2 (discussing the National Retail Federal Conference in New York, and that "omnichannel" was on everyone's lips).

[10] *See* Peter C. Verhoef et al., *From Multi-Channel Retailing to Omni-Channel Retailing Introduction to the Special Issue on Multi-Channel Retailing*, 91 J. OF RETAILING 174, 174 (2015) (Describing the various concerns that accompany the implementation of Omnichannel marketing strategy; the article asserts that retailers must decide "as to whether new channels should be added to the existing channel mix. This decision pertains to traditional brick-and-mortar players, as well as to new online players, who face the question of whether they should be present offline as well. The scope of multi-channel retailing has . . . been broadened by considering issues such as the management of customers across channels and the integration of the retail mix across channels.").

[11] Walker, *supra* note 5, at 2; *See also* Verhoef et al., *supra* note 10, at 178 (Describing a set of studies which analyze the preferable "[r]etail [m]ix across [c]hannels," meaning the assortment of goods a store online-offline as compared to what is available in-store. "Full integration" means offering the same assortments whereas "no integration" means different assortments are offered online and online. The article states: "[a]cross the three experiences, the authors show that online-offline channel integration leads to channel synergies rather than channel cannibalization.").

[12] Cooper Smith, *How beacons—small, low cost gadgets—will influence billions in US retail sales*, BUS. INSIDER (Feb. 9, 2015) http://www.businessinsider.com/beacons-impact-billions-in-reail-sales-2015-2.

[13] Tony Danova, *BEACONS: What They Are, How They Work, and Why*

technology for Apple devices to alert apps or websites (which the user has opted into) when someone approaches or leaves a location."[14] In the retail setting, beacons enable retailers to send consumers timely messages with useful information regarding their products, such as speed checkout processes, personalized offers and where similar products may be found depending on their physical location within or outside of a retail location.[15] Beacons enable in-store retailers to respond to and analyze the ways various channels meld together as customers utilize numerous channels simultaneously.[16]

Already, half of American adults use their mobile devices while inside stores.[17] Shoppers "[f]requently search for information in the store and simultaneously search on their mobile device to get more information about offers and may find more attractive prices."[18] With the advent of beacons, retailers can maximize and exert more control over[19] the way consumers employ the channels available to them, hopefully leading to the eventual complete integration of channels such that the initial notion of a channel disappears.[20] Channel integration involves "understand[ing] the

---

Apple's iBeacon Technology Is Ahead of the Pack, BUS. INSIDER, 1 (Oct. 23, 2014, 10:25 AM), http://www.businessinsider.com/beacons-and-ibeacons-create-a-new-market-2013-12 ("In-store retail and offline payments are in the first wave of beacon applications. Retail outlets are adopting beacons to provide customers with product information, flash sales or deals, and to speed up the checkout process with a completely contactless payments system.").

[14] H.O. Maycotte, *Beacon Technology: The Where, What, Who, How and Why,* FORBES (Sep. 1, 2015 11:00 AM), http://www.forbes.com/sites/homaycotte/2015/09/01/beacon-technology-the-what-who-how-why-and-where/print/.

[15] Danova, *supra* note 13, at 1.

[16] Verhoef et al. *supra* note 10, at 175 ("The opposite of showrooming also occurs, which is now referred to as webrooming, where shoppers seek information online and buy offline. In the past, this was found to be a dominant form of research shopping.").

[17] Danova, *supra* note 13, at 1.

[18] Verhoef et al. *supra* note 10, at 175.

[19] Smith, *supra* note 12, at 2 ("Since beacon-powered apps will collect valuable data on consumers' in-store activity, they could result in highly personalized and targeted offers, which will reinforce the above [loyalty] programs. Once a consumer opens an app in-store, the data on their clicks and location can help retailers target them with offers customized to their location in a store, or based on past in-store shopping behavior.").

[20] Walker, *supra* note 5, at 7 ("Retailers must look at their systems landscape, operational approach and performance metrics, and relentlessly erode the notion of channel. This does not mean that measuring the performance of the website or a specific store is not meaningful. But now we need to focus on the broader benefits and understand the full customer engagement across all touch points in order to optimize the experience. A broader approach requires systems that can serve all interactions and nimbly adapt to new ones. This is the role of

full customer engagement across all touch points in order to optimize the experience."[21] Beacons serve to connect and integrate a shopper's in-store experience with their online shopping experience. In 2015 beacons are expected to "directly influence over $4 billion worth of US retail sales [. . .] at top retailers (.1% of the total), and that number will climb tenfold in 2016."[22]

This paper will first analyze beacons in the context of their use and future potential in Omnichannel retailing. It will go on to describe the various legal implications of beacons in the Omnichannel retail setting.

A. Why Save Brick-and-Mortar Anyway?

In a fast paced economy where technological shifts and innovations commonly erode and destroy previously vibrant industries, why should it matter to consumers whether brick-and-mortar stores continue to compete with online vendors? Beyond the obvious answer that all those who derive their livelihood from the traditional retail industry are invested in its continued success, physical retail also plays an important role in neighborhood and community development.[23] Along with sales tax revenue and job creation, "community vitality itself lies in the balance."[24] Consumption in stores is social event, bringing groups

---

the commerce platform. This is the role of a customer engagement platform. This is the role of a customer engagement platform. This is the role of assortment planning and back office tools, all of which must adapt to this new context.").

[21] *Id.* at 7.

[22] Smith, *supra* note 12, at 1 ("[M]any early adopters who opt in to receive beacon-triggered messages will likely be coupon clippers. Half of beacon-triggered messages sent currently are some form of coupon, according to Shopkick. Mobile coupons are a significant part of this market. Mobile couponing app company RetailMeNot claims that its offers alone influenced $3.5 billion in retail sales in 2013.").

[23] J. Peter Byrne, *The Rebirth of the Neighborhood*, 40 FORDHAM URB. L.J. 1595, 1596 (2013).

[24] Michael N. Widener, *Begone, Euclid!: Leasing Custom and Zoning Provision Engaging Retail Consumer Tastes and Technologies in Thriving Urban Centers*, 35 PACE L. REV. 834, 837 (2015) ("As urban centers become more homogeneous, a product in large part of national brand retailing, the importance of promoting differentiation among urban retail opportunities increases. A thriving town center needs to have a mixture of social, civil, residential and leisure (including retail) opportunities for its citizens, enabling holistic provision within the urban center's space.").

of individuals together in a common activity, contributing to and creating essential continued vigor in urban areas:

> Retailing is what local people, visitors and investors judge the city's core by, declaring it either "vital" or "dead." So, beyond paying and generating taxes, creating employment and serving shoppers, retailing is the face and heart of your community. Investors, office locators, residents, convention organizers, tourists, and shoppers all make their spending decisions based on how alluring a downtown retail area is.[25]

Ensuring that physical retailers remain competitive has large implications for the livelihood of neighborhoods and cities alike.[26] Because physical retail competes so heavily with online shopping, in-store retail vendors must recognize that many individuals choosing to shop in-store are often seeking both a sense of community and a sensory experience that will provide a reprieve from the doldrums of daily life.[27] Thus, although "every retail shopping experience cannot resonate with consumers like a live music concert, physical retailers know that a sensory-deadening encounter is one a consumer will act to avoid repeating."[28] Beacons could potentially revive in-store shopping experiences through providing an additional sensory stimulus that helps connect consumers' online shopping activity, and their online activity in general, with their in-store experiences.[29] From the retailer's vantage point, beacons have the potential to provide

---

[25] *Id.* at 881–82.

[26] *Id.*

[27] *Id.* at 842–43 (The author, asking readers to think back to their "most intense retail shopping experience" describes their own shopping episode at the Queen Victoria Market in London, a large outdoor market. Widener states: "[i]nteractivity between merchants and shoppers is intensely animated and fascinating to behold at close range. There is no anticipating who or what you encounter within the stalls of the market and on its adjoining streets from one visit to the next. The human energy level, heightened by the richness of sensory experiences and coupled with the novelty of unfamiliar goods and fellow-travelers, is palpable and vast. While every retail shopping experience cannot resonate with consumers like a live music concert, physical retailers know that a sensory-deadening encounter is one a consumer will act to avoid repeating.").

[28] *Id.* at 843.

[29] *Could Beacons Push People off the Couch and to the Store?* EMARKETER (July 25, 2014), http://www.emarketer.com/Article/Could-Beacons-Push-People-off-Couch-Store/1011046 ("No one is seriously declaring the death of the retail store, but improving the in-store experience is top of mind for many- and mobile can be a catalyst. 'Brick-and-mortar businesses need to come up with much more compelling reasons for consumers to get off the couch and actually show up to the store,' said Schulyer Brown, vice president of marketing at beacon provider Nomi. 'And mobile apps powered by microlocation marketing, I think, is a key component to make that a compelling argument.'").

important and previously inaccessible data that could be used to cut costs and generate more sales.[30]

2. BEACON TECHNOLOGY: HOW EXACTLY DOES IT WORK?

Retailers are beginning to utilize a beacon referred to as a Bluetooth Low Energy (BLE) beacon. This beacon "uses short range radio waves with less power consumption for the communicating devices than previous Bluetooth technology."[31] The beacon works through two BLE specifications: a peripheral device and a central device.[32] The central device, which most commonly is a mobile phone (top mobile device operating systems all support BLE, including, Android, iOS and Windows), receives information from the peripheral device, which is typically a low-powered device built to send data.[33] The data that peripheral devices send is most commonly a beacon advertisement affixed with a unique identifier.[34] In the retail setting, this unique identifier is connected with both a shopper's mobile app (for example, their Walmart app) and various beacons inside a store.[35] Beacons situated throughout the store use different "minor" values in order to identify where inside a particular store a consumer is, while "major" values are used to identify which store location a consumer is shopping in.[36] The different minor and major values vary depending on store location and individual store layout, but an individual company's unique identifier

---

[30] *Federal Trade Commission* (F.T.C.), *Comments of the Future Privacy Forum,* F.T.C., 5 (2014), https://www.ftc.gov/system/files/documents/public_comments/2014/03/00018-89123.pdf [hereinafter F.T.C. *Comments*] ("Businesses [. . .] 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 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.").

[31] Carl L. Huth, *A Privacy Primer on Beacon Technology*, 18 J. INTERNET L. 21 (2015).

[32] *Id.*

[33] *Id.*

[34] *What is iBeacon?,* BEACON SANDWICH, 1, http://www.beaconsandwich.com/what-is-ibeacon.html (last visited Apr. 11, 2016).

[35] *Id.* at 2.

[36] *Id.* at 1–2.

remains the same.[37]

Consumers would experience beacons as such: outside a Walmart Location A, shopper's Walmart app receives a beacon signal identifying that the costumer is close to that Walmart location (this is demarcated from Walmart Locations A, B, C etc. by each store location's different major value). Once inside the store, beacons placed in different locations, for example at the cosmetics section of the store or at the clothing section, would each be configured to send different minor values to the Walmart app, alerting it that the shopper is looking at cosmetics or clothing. The information broadcast by each beacon allows the app to know how close or far a mobile device is from a product and subsequently perform actions such as send the device owner an alert.[38] As such, beacons only send out data, but beacon-powered apps are able to collect consumer data once the customer opens the app in-store.[39] Beacons detect a user's phone once that individual has approached a retail location. They subsequently send alerts to the mobile phone user containing information about sales, promotions or other marketing material. These alerts are only viewable if the phone user has downloaded a beacon enabling mobile application.

Beacons are a valuable tool not only for communicating information to customers as they shop in a traditional retail setting, but also for collecting highly personalized information on an individual's shopping behavior and in-store activity.[40] Akin to how cookies enable online stores to track an individual's online shopping habits without having them ever effectuate a purchase, beacons may also track an individual's in-store shopping behavior without them ever effectuating a purchase. As such, beacons allow companies to collect information regarding:

> [H]ow 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,

---

[37] *Id.* at 1.

[38] *Id.* at 3.

[39] *See* Smith, *supra* note 12, at 1–2 (explaining that "[s]ince beacon-powered apps will collect valuable data on consumers' in-store activity, they could result in highly personalized and targeted offers, which will reinforce the above programs. Once a consumer opens an app in-store, the data on their clicks and location can help retailers target them with offers customized to their location in a store, or based on past in-store shopping behavior.").

[40] *Id.* at 1–2.

> what parts of the space are over and under used, what the peak periods of use are, how long devices stay in the space, and other information.[41]

The questions is, are consumers ready to share this kind of information with retailers through enabling beacon technology on their phones? One study suggests that "56% of customers overall are not comfortable sharing their location in-store with retailers. Even with an offer or discount, 41% are still reluctant."[42]

Consumer privacy concerns loom large for retail companies investing in beacon technology. This is especially significant in relation to beacon-enabled applications that have the means to collect data regarding retail consumers. Utilizing these applications is what presents the most significant privacy concerns to consumers and retailers alike.[43]

3. PRIVACY CONCERNS BEHIND BEACON TECHNOLOGY

The forces that prevent individuals from disclosing personal information to online services are referred to in the tech world as "friction."[44] Individual friction, which to most online businesses represents lost opportunity, is countered by so-called "frictionless sharing" that discloses individuals' activities automatically, without asking for their permission prior to each disclosure.[45] For example, "[M]ainstream news websites . . . offer 'social reading' applications ('apps') in Facebook. After a one-time authorization,

---

[41] F.T.C. *Comments*, *supra* note 30, at 5; *See also* Huth, *supra* note 31, at 22 (stating that in addition, retailers may collect other data about the shopper, such as their age and gender.).

[42] Mark Walsh, *Getting Privacy Right is Key to Beacon Deployment,* MOBILE MARKETING DAILY (Aug. 12, 2014, 12:15 PM), http://www.mediapost.com/publications/article/231883/getting-privacy-right-is-key-to-beacon-deployment.html.

[43] *See* Huth, *supra* note 31, at 22 ("[U]nder most common uses, the beacon itself is passive, and does not collect any information. The predominant consideration from a privacy perspective when engaging with beacon technology is the application development.").

[44] William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 15 (2013) ("To many in Silicon Valley [. . .] the word 'friction' [. . .] mean[s]: [. . .] the forces that impede individuals from disclosing personal information when they use online services, particularly social networks such as Facebook. As more businesses turn to social media as a source of promotion and eventually revenue, this kind of friction represents lost opportunity."), http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1509&context=uclf.

[45] *Id.*

these apps send routine messages through Facebook to users' friends identifying articles the users view."[46]

Technology in mobile phones "does enable truly frictionless collection and disclosure of information [such as one's location] in many situations,"[47] but such frictionless sharing has received substantial pushback and criticism from consumers who consider this form of sharing to be an unacceptable invasion of privacy.[48] Indeed, one nationwide survey showed that 57% of all app users either declined to initially install an app, or have uninstalled an app, due to concerns about sharing their personal information.[49] Central to overcoming consumer friction in the context of beacon enabling apps is providing consumers with notice as to when a company is collecting data, transparency as to how this data is used, and subsequently obtaining consumer consent.[50]

The importance of notice, transparency and consent in the utilization of beacon technology was made clear by a 2014 incident whereby Titan, an advertising company "which owns the right to sell ads in thousands of phone booth kiosk advertising displays"[51] installed hundreds of beacons in pay phone booths around Manhattan.[52] A *BuzzFeed News* article exposed the

---

[46] *Id.* at 16.

[47] *Id.* at 52.

[48] *Id.* at 17. ("[M]any implementations of frictionless architecture have gone too far, potentially invading privacy and drowning useful information in a tide of meaningless spam.").

[49] *Federal Trade Commission* (F.T.C.), *Mobile Privacy Disclosures,: Building Trust Through Transparency*, F.T.C., 3 (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (hereinafter F.T.C., *Mobile Privacy*) (explaining that "[s]imilarly, in a 2011 survey of U.S. smartphone users, less than one-third of survey respondents reported feeling in control of their personal information on their mobile devices.").

[50] *See* Jules Polonetsky, *Trust, transparency best in-store deal for shoppers with mobile phones,* RETAILING TODAY, 1–2 (May 19, 2014), http://www.retailingtoday.com/article/trust-transparency-best-store-deal-shoppers-mobile-phones (explaining that "[i]t's not a surprise that the deployment of [. . .] [beacon] technologies has led to critical media stories about surprised shoppers who express annoyance when told that they are secretly having their phones tracked. To respond to these concerns, the Future of Privacy Forum partnered with Senator Charles Schumer to create a Mobile Location Code of Conduct for venues using location analytics.").

[51] Joseph Bernstein & Jeremy Singer-Vine, *New York City Kills Hidden Phone Booth Devices*, BUZZFEED NEWS, 2 (Oct. 6, 2014, 1:14 PM) http://www.buzzfeed.com/josephbernstein/new-york-city-to-advertising-contractor-take-down-secretly-i#.buaBLeLRw.

[52] *Id.* at 1.

existence of these beacons, noting that although the beacons were installed with "the blessing of a city agency"[53] there was no "public notice, consultation, or approval."[54] The subsequent outcry from New Yorkers and news outlets alike led to the beacons near immediate removal.[55] A representative for New York City Comptroller, Scott M. Stringer, told *BuzzFeed News* that "New Yorkers deserve to know that their private information is being protected and the Comptroller's office will be keeping a close eye on any agreement that comes before us to ensure that the process to award this contract was done with full transparency."[56]

The ambiguity surrounding how Titan's phone booth beacons were being used, coupled with the beacon's secret installation, and the subsequent lack of consent from the public caused much friction.[57] Retailers wishing to utilize beacon technology must acknowledge that transparency in privacy practices could be a means for competition where "[c]ompanies that are able to demonstrate to consumers clear and consistent transparency in collection and use of personal information can be more competitive and, consequently, more profitable."[58]

There is a wealth of information regarding best practices for retail companies wishing to utilize beacon technology. In 2012, the Federal Communications Commission (FCC) identified consumer's key privacy concerns and best practices in regards to location based services on mobile devices (LBS), producing a report meant to "facilitate increased adoption of these services and their attendant economic benefits. . . ."[59]

---

[53] Joseph Bernstein et al., *Exclusive: Hundreds of Devices Hidden Inside New York City Phone Booths*, BUZZFEED NEWS, 2 (Oct. 26, 2014, 2:00 AM), http://www.buzzfeed.com/josephbernstein/exclusive-hundreds-of-devices-hidden-inside-new-york-city-ph#.lb4woeqw7.

[54] *Id.*

[55] Bernstein & Singer-Vine, *supra* note 51, at 1–2.

[56] *Id.* at 2.

[57] Joseph Bernstein et al., *supra* note 53, at 2–3.

[58] *Federal Communications Commission Record* (FCC Rcd), *Location Based Services: An Overview of Opportunities and Other Considerations*, WIRELESS TELECOMMUNICATIONS BUREAU, 23 (2012) http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0530/DOC-314283A1.pdf [hereinafter FCC *Overview*].

[59] *Id.* at 19 ("[A]s the [location based services on mobile phones] industry continues to develop, companies remain mindful of the associated privacy challenges. A 2009 survey of LBS users conducted by Carnegie Mellon University found that in general, consumers believe that the privacy risks of sharing their location outweigh the potential benefits of the services. Thus, to

4. BEST PRACTICES AND BEACON TECHNOLOGY

A. Best Practices for Location Based Services

Firstly, the FCC identifies notice and transparency as key aspects of companies' approach to privacy.[60] Given the limited screen space that mobile phones have, it is difficult to post extensive privacy policies on a mobile app. As such, one survey cited by the FCC had found that in 2010 only 66% of mobile applications using LBS had privacy policies in place that would inform users as to how their personal information was being utilized.[61]

Retailers wishing to utilize beacon technology through mobile applications should aim to build trust with their consumers through transparent notice, which the FCC identifies as indispensible for creating and maintaining customer relationships.[62] Some recurring elements of common privacy notices include:

[C]ategories of personal information collected and how that information will be used; opportunities and mechanisms for consumers to make choices regarding these uses, including opt-in or opt-out mechanisms for effectuating their choices; third-party access and sharing of personal information; and data minimization and data security practices.[63]

By providing consumers with transparent notice, a consumer is able to assess whether or not they consent to the company's terms of use. If, subsequent to obtaining initial consent, a user's information will be used in a new or materially different purpose than that for which the original consent was provided, then companies "must provide users with further notice and obtain consent to the new or other use."[64]

---

facilitate increased adoption of these services and their attendant economic benefits, companies must address key privacy issues associated with [location based services]."). *Id.* at 18–19.

[60] *Id.* at 19.

[61] *Id.* at 20.

[62] *Id.* at 23 ("Transparency in privacy practices also has become a source of competition. Companies that are able to demonstrate to consumers clear and consistent transparency in collection and use of personal information can be more competitive and, consequently, more profitable. The trust that is built between companies and their customers around transparency in privacy has become an essential precondition for building and maintaining productive customer relationships."). *Id.*

[63] *Id.* at 19.

[64] *Best Practices and Guidelines for Location-Based Services,* CTIA: THE

The FCC next identifies meaningful consumer choice in regards to "the collection and use of their personal information"[65] as a salient concern surrounding the use of LBS (location-based services). Specifically, the FCC discusses whether choice should take the form of opt-out or opt-in for the utilization of consumer location information.[66] One 2010 survey cited in the report found that "the vast majority of respondents say that search engines and online social networking sites should not be able to share their physical location with other companies before they have given specific authorization."[67] Thus both Microsoft and Google do not collect or use location information from mobile devices without first obtaining opt-in consent.[68]

Notice, transparency, and meaningful consumer consent are all inextricably tied to the issue of third party access to personal information, which the FCC states is central to the privacy debate surrounding LBS.[69] Indeed, "[o]nce an app has access to a user's data, there are usually no rules governing its disclosure and no controls available to consumers to regain control of it. For the most part, once data leaves the phone, it is effectively 'in the wild.'"[70] Thus companies providing LBS have tried to address third party access both by encouraging app developers to include privacy protections in the creation of their product[71] and by

---

WIRELESS ASS'N, 3 (2010) http://www.ctia.org/policy-initiatives/voluntary-guide lines/best-practices-and-guidelines-for-location-based-services.

[65] FCC *Overview*, *supra* note 58, at 23.

[66] *Id.* at 19.

[67] *Id.* at 24 (quoting Memorandum from Zogby International to Common Sense Media (2010), http://www.privacylives.com/wp-content/uploads/2010/10/ Final-CSM-adults-topline-8-24-10-Updated-EMBARGO.pdf.).

[68] *See id.* (discussing the issue companies face of whether consumer choice should opt-out or opt-in for location information).

[69] *See generally id.* ("[T]here appears to be a developing consensus in the LBS industry that opt-in is appropriate for such sensitive information.").

[70] *Before the Senate Judiciary Comm., Subcomm. on Privacy, Tech., and the Law: Hearing on "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy,"* 2 (2011) (statement of Justin Brookman, Dir., Consumer Privacy, Ctr. for Democracy & Technology), https://cdt.org/files/ pdfs/20110510_mobile_privacy.pdf (Data which has left one's phone "may be retained long after the moment of collection, and often long after the original service has been provided. App developers, advertisers, ad networks and platforms, analytics companies, and any number of other downstream players can share, sell, or unpredictably use data far into the future.").

[71] *See generally About the Application Data Privacy Project*, FUTURE OF PRIVACY FORUM, http://www.applicationprivacy.org/about/ (last visited Apr. 10, 2016) (which aims to help app developers create a responsible way to collect and use sensitive user data).

alerting users when an application is accessing the mobile device's GPS location.[72] Companies like AT&T have gone so far as to "require[] third party application developers that sell their applications through AT&T to have a privacy policy and to comply with the both CITA and AT&T guidelines for LBS privacy."[73]

Being that beacons are app-enabled technology, the privacy practices of a retailers' app is central to building consumer trust. A 2013 Federal Trade Commission report entitled "Mobile Privacy Disclosures: Building Trust Through Transparency" suggests that an application programming interface (API) provide just-in-time disclosures, meaning disclosures occurring immediately prior to the collection of geolocation data, so that consumers will be provided with relevant information regarding a company's privacy policy.[74]

Finally, data security, meaning "the technical, physical, and administrative safeguards that have been put in place to protect personal information primarily from the risks of unauthorized disclosure or access"[75] must be central to a company's privacy policy. Data security is tied to data minimization, which "refers to the idea that a company will only retain personal information it actually needs and only for the amount of time that it is needed."[76] Through data minimization, LBS utilizers are able to provide more robust data security to their users.

By addressing consumer's central privacy concerns, company's utilizing LBS can hopefully "evolve[] to meet [their] fullest potential while protecting the legitimate interests of consumers in safeguarding their personally identifiable information."[77] This is particularly important for the successful utilization of beacon technology in the retail setting, which for many consumers still feels like an invasion of privacy.[78] In the words of one consumer utilizing a Shopkick beacon marketing app inside Best Buy,

---

[72] *See* FCC *Overview*, *supra* note 58, at 20.

[73] *Id.* at 29.

[74] F.T.C., *Mobile Privacy*, *supra* note 49, at 3.

[75] FCC *Overview*, *supra* note 58, at 30 (citing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 17, para.1).

[76] *Id.*

[77] *Id.* at 2.

[78] *See* Mae Anderson, *Shopping beacons: Big help or Big Brother?*, NORTHWESTER MEDIA 1 (Dec. 4, 2014, 5:09 PM) http://www.thenorthwestern.com/story/money/2014/12/04/shopping-beacons-big-help-big-brother/19915883/.

"[t]he experience was great but also a little unnerving in the sense that the store knew who I was and that I was present in their location. It felt a little Big Brother-like."[79]

New York Senator Chuck Schumer has attempted to address and ameliorate consumer ambivalence specifically regarding retail beacon technology. In October of 2013, Schumer wrote a letter to the Federal Trade Commission (FTC) stating that:

> Geophysical location data about a person is obviously highly sensitive; however, retailers are collecting this information anonymously without consent. I would ask that the Federal Trade Commission investigate and clarify that it is an unfair or deceptive trade practice to fail to notify shoppers that their movements are being tracked in a store or to give them an opportunity to opt out of this type of tracking before it begins. As these technologies become more widespread, it is imperative that we protect our consumers from unknowingly giving information they do not desire.[80]

Subsequently Schumer, along with the Future of Privacy Forum (FPF), introduced the Mobile Location Analytics Code of Conduct[81] (MLA), meant to "provide an enforceable, self-regulatory framework for the services provided in the US to Retailers by Mobile Location Analytics ('MLA') Companies."[82]

While companies that have signed onto the MLA are not household names, they "power a big chunk of the back-end technologies that let marketers precisely geolocate customers in

---

[79] *Id.*

[80] Press Release, Schumer Reveals; Stores are Tracking Shoppers Movements Through Their Cell Phones With Rapidly Increasing Frequency, and Testing Ever More Invasive Technologies; Calls for FTC to Require Mandatory Opt-Out Opportunity Before Retailers are Allowed to Track Shoppers Movements, CHARLES E. SCHUMER, U.S. STATE SENATOR FOR N.Y. (July 30, 2013), http://www.schumer.senate.gov/newsroom/press-releases/schumer-reveals-stores-are-tracking-shoppers-movements-through-their-cell-phones-with-rapidly-increasing-frequency-and-testing-ever-more-invasive-technologies-calls-for-ftc-to-require-mandatory-opt-out-opportunity-before-retailers-are-allowed-to-track-shoppers-movements.

[81] *See Mobile Location Analytics Code of Conduct*, FUTURE OF PRIVACY FORUM (2013), http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf [hereinafter *Mobile Analytics Code*].

[82] *Mobile Analytics Code*, *supra* note 81. at 1; LEVENT DEMIR ET AL., ANALYSING THE PRIVACY POLICIES OF WI-FI TRACKERS 5 (Rocquencourt, Inria 2014) (Companies that are part of the FPF's MLA working group include: Aislelabs, Euclid, eyeQ, iInside, Measurance, Mexia, Radius Networks, Solomo, and Turnstyle.).

stores."[83] The ultimate goal of the MLA is to enable the successful use of beacon technology through the creation of consumer trust.[84]

(I) Mobile Location Analytics Code of Conduct

The MLA identifies many of the same important privacy concerns and best practices illuminated by the FCC's LBS report such as transparency and choice.[85] Specifically, the MLA's central principles are: (1) notice, taking the form of in-store signage informing consumers of the use and collection of MLA data[86] with a link to a more detailed privacy notice posted online; (2) limited collection, meaning that MLA companies shall promptly de-identify and de-personalize consumer and device information, unless the consumer has otherwise given affirmative consent; (3) choice, allowing for consumers "to decline to have their mobile devices used to provide retail analytics services,"; (4) limitation on collection and usage; (5) onward transfer, such that MLA companies will contractually provide that unaffiliated third parties must also comply with the MLA Code of Conduct; (6) limited retention of consumer data, which is to be covered in a company's privacy notice; and (7) consumer education, taking the form of a website explaining MLA services, a standardized symbol meant to "convey to consumers the concept of MLA services"[87], and education efforts meant to inform consumers about MLA services.[88]

The MLA Code of Conduct attempts to aid retailers using beacon technology to balance both "properly gather[ing] and employ[ing] analytics for their primary purpose"[89] while also

---

[83] Doug Thompson, *The Future of iBeacons: A Code of Conduct (for the NSA?)*, BEEKN (Oct. 22, 2013), http://beekn.net/2013/10/ibeacons-code-of-conduct/.

[84] *See, e.g.*, *Most Shoppers Disapprove Of In-Store Tracking*, RETAIL TOUCHPOINTS (May 19, 2014, 5:55 AM) http://www.retailtouchpoints.com/topics/-experience/most-shoppers-disapprove-of-in-store-tracking (discussing shopper disapproval of tracking devices as nearly 81% of consumers "said they do not trust retailers will keep personal information secure").

[85] *Mobile Analytics Code, supra* note 81, at 1.

[86] *Id.*

[87] *Id.* at 2–3.

[88] *See id.* at 1–6 (discussing the education efforts and numbered principles that are in place to inform consumers about MLA services).

[89] Jim Riesenbach, *Understanding the Mobile Location Analytics Code of Conduct*, RETAIL CONSUMER EXPERIENCE (last visited Apr. 16, 2016)

"remain[ing] committed to ensuring the privacy of their customers."[90] Beyond building consumer trust and eliminating consumer friction, precise geolocation data is considered sensitive personal information, and the dissemination of this data has potential to cause great harm.[91] Geolocation data could be used to "help build profiles about consumers without their knowledge or consent, or it could be accessed by cybercriminals, hackers or through surreptitious means such as 'stalking apps.'"[92] As such, it is imperative that retailers utilizing beacons carefully consider their privacy policies and practices.

(II) Privacy in the Courts

i. Private Litigants

The importance of adequate consumer consent in the context of beacon technology is again highlighted by the fact that consent has "been successfully deployed [as a defense] to claims mounted against data collectors under both tort theories and violations of the Electronic Communications Privacy Act (ECPA)."[93] The ECPA, a federal statute passed in 1986, remains the central piece of federal legislation addressing consumer data privacy, although many consider the statute to be "woefully inadequate and antiquated."[94]

Section II of the ECPA, entitled the federal Stored Communications Act (SCA), makes it a punishable offense to "(1) intentionally access[] without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed[] an authorization to access that facility[.]"[95]The statute provides exceptions for conduct that is

http://www.retailcustomerexperience.com/articles/understanding-the-mobile-location-analytics-code-of-conduct/.

[90] *Id.*

[91] Press Release, Fed. Trade Comm'n, FTC Testifies on Geolocation Privacy (June 4, 2014) https://www.ftc.gov/news-events/press-releases/2014/06/ftc-testifies-geolocation-privacy.

[92] *Id.*

[93] Peter Segrist, *How the Rise of Big Data and Predictive Analytics Are Changing the Attorney's Duty of Competence,* 16 N.C. J. L. & TECH. 527, 577 (2015).

[94] *See* 18 U.S.C. § 2701 (2002) (discussing the unlawful access to stored communications statute); *See* Segrist *supra* note 93, at 581.

[95] 18 U.S.C. § 2701(a) (2002).

authorized "(1) by the person or entity providing a wire or electronic communication service; (2) by a user of that service with respect to a communication of or intended for that user. . . ."[96]

The Wiretap Act, also contained within the ECPA, provides that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity"[97] held responsible. Private litigants using the ECPA to either recover monetary damages or enjoin data collection practices in the private sector have been largely unsuccessful in addressing data collection from cellphone usage.[98]

a. In re iPhone Application Litigation

In *In re iPhone Application Litigation*[99], a nationwide class of plaintiffs brought suit against Apple, Google, and other Mobile Industry Defendants for alleged violations of both federal and state law, including the SCA and the Wiretap Act.[100] The plaintiffs' central injury was that the iOS devices they bought were overvalued or that they did not operate as represented due to certain privacy deficiencies.[101] These claims "all required plaintiffs to allege one key fact: *that they relied on Apple's privacy representations, and reliance on these representations caused the injury in question*."[102] The plaintiffs' were divided into two separate putative classes: the iDevice Class and the Geolocation Class.[103]

---

[96] 18 U.S.C. § 2701(c) (2002).

[97] 18 U.S.C. § 2520 (a) (2002).

[98] Segrist, *supra* note 93, at 589.

[99] *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1040 (E.D. Cal. 2012).

[100] *Id.* at 1048–49.

[101] Venkat Balasubramani, *Privacy Plaintiffs Lose Because They Didn't Rely on Apple's Privacy Representations – In re iPhone App Litigation*, TECH. & MARKETING L. BLOG (Dec. 2, 2013), http://blog.ericgoldman.org/archives/2013/12/privacy-plaintiffs-lose-because-they-didnt-rely-on-apples-privacy-representations-in-re-iphone-app-litigation.htm ("Ultimately, this case devolved into claims that Apple misrepresented into products by plaintiffs who claimed that they didn't get what they paid for.").

[102] *Id.*

[103] *In re* iPhone Application Litig., 844 F. Supp. 2d at 1049–50.

(1) iDevice Plaintiffs and Geolocation Plaintiffs

The claims of the iDevice Plaintiffs and the Geolocation plaintiffs are addressed together by the Court because many of their claims overlap.[104] The iDevice Plaintiffs claimed that, "Defendants violated their privacy rights by unlawfully allowing third party applications ('apps') that run on the iDevices to collect and make use of, for commercial purposes, personal information without user consent or knowledge."[105] Plaintiffs stated that Apple makes free Apple-Approved Apps downloadable through its App Store, and that when users download and install these Apps, the Defendants' software obtains information about the device users without their consent, subsequently transmitting it to the Mobile Industry Defendants.[106] The information collected includes "[p]laintiffs' addresses and current whereabouts[.]"[107]

The Geolocation Plaintiffs claimed that subsequent to Apple's release of their iOS 4 operating system "Apple began intentionally collecting Plaintiff's precise geographic location and storing that information on the iDevice [. . .]." [There should be a footnote here] Furthermore, the plaintiffs alleged that although Apple claimed that one could turn off this feature and prevent Apple from collecting their geolocation data, in fact Apple continued to store and monitor information about Plaintiffs location even after the feature was turned off.[108] This, they asserted, was in violation of Section II of the ECPA which, as above stated, creates a private right of action against one who "intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system. . . ."[109]

The Geolocation Plaintiffs also claimed that Apple violated the Wiretap Act which provides a private right of action against anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" *or* one who uses or

---

[104] *Id.* at 1051–52.

[105] *Id*. at 1049.

[106] *Id.* at 1049–50.

[107] *Id*. at 1050 (Also, "the unique device identifier ('UDID') assigned to the iDevice; the user's gender, age, zip code and time zone; and app-specific information such as which functions Plaintiff performed on the app.").

[108] *Id.*

[109] 18 U.S.C. § 2701(a)(2) (2002).

tries to use an intercepted communication that was collected in violation of the Wiretap Act. Plaintiffs claim that Apple collected their "precise geolocation data"[110] and used that data in order to "develop an expansive database of information about the geographic location of cellular towers and wireless networks throughout the United States[,]" to Apple's benefit[111] and in violation of the Act.

In response to the Plaintiff's SCA claim, the Court held that Plaintiffs had failed to state a claim under the statute because "their iOS devices do not constitute 'facilit[ies] through which an electronic communication service is provided.'"[112] Initially, the Court was faced with deciding, "whether an individual's computer, laptop, or mobile device fits the statutory definition of a 'facility through which an electronic communication service is provided.'"[113] Uncontested examples of facilities through which electronic communication services are provided under the SCA include: the computer systems of email providers, an Internet service provider or a bulletin board system. [114]

In determining that mobile devices do not constitute facilities through which electronic communication services are provided, the Court looked at the holding of *Crowley v. CyberSource Corp*[115] a 2001 California District Court decision, where plaintiffs similarly argued that their private computers should be held to be facilities under the meaning of the SCA.[116] In that case, the Court reasoned that private computers do not fall within this definition because adopting this construction of the statute "would render other parts of the [SCA] illogical."[117] For example, following this construction would mean that a under another part of the SCA a service provider could grant third party access to one's home computer (the "facility").[118] A similar result would follow if the Court determined that Plaintiff's mobile phones were facilities under the Act.

---

[110] *In re iPhone Application*, 844 F. Supp. 2d at 1050, 1061 (also citing to 18 U.S.C § 2511(1)(a)).

[111] *Id.* at 1050.

[112] *Id.* at 1058.

[113] *Id.* at 1057.

[114] *Id.*

[115] *Crowley v. CyberSource Corp.,* 166 F. Supp. 2d 1263, 1263 (N.D. Cal. 2001).

[116] *In re iPhone Application*, 844 F. Supp. 2d at 1058.

[117] *Id.*

[118] *Id*.

In response to the Geolocation Plaintiff's Wiretap Act claims, the Court states that "intercept" under the Wiretap Act means to acquire "the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[119] The Court held that Plaintiff's geolocation data does not constitute "content" under the Act, which is limited to information that the "user intended to communicate, such as the words spoken in a phone call."[120] Because the geolocation information that Plaintiff's claim Apple collects illegally is "automatically generated by the communication but that does not comprise the substance, purport, or meaning of that communication"[121] it is thus not within the purview of the Act.

The *In Re iPhone Application Litigation* demonstrates the substantial roadblocks that private litigants face when challenging the unauthorized collection and retention of geolocation data through mobile phones.[122] Private litigation is not the only means of regulating mobile industry players. The FTC may also bring actions against companies for violating their own privacy policies.[123]

ii. Federal Trade Commission (FTC) Action

The FTC, "an independent U.S. law enforcement agency charged with [among other things] protecting consumers"[124] attempts to defend consumer rights in regards to privacy. The FTC states that "[w]hen companies tell consumers they will safeguard their personal information the FTC . . . [ensures that these] companies live up to [their] promises."[125] This includes

---

[119] 18 U.S.C. § 2510(4).

[120] *In re iPhone Application* 844 F. Supp. 2d at 1061 (citing the Ninth Circuit's decision in *United States v. Reed*, where the Court held "that data automatically generated about a telephone call, such as the call's time of origination and its duration, do not constitute 'content' for purposes of the Wiretap Act's sealing provisions because such data 'contains no "information concerning the substance, purport, or meaning of [the] communication." ' ").

[121] *Id.* at 1062.

[122] *See generally id.* at 1058.

[123] *Federal Trade Commission* (F.T.C.), *Federal Trade Commission 2014 Privacy and Data Security Update,* F.T.C. (last visited April 18, 2016), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf [hereinafter: F.T.C., *Security Update*]

[124] *Id.*

[125] *Federal Trade Commission* (F.T.C.), *Enforcing Privacy Promises,* F.T.C.

ensuring that any consumer data collected through applications is accurately reflected to consumers in a company's privacy policies.[126]

> The FTC's enforcement power in this field is endowed to them in Section 5 of the FTC Act, which prohibits unfair or deceptive practices in the marketplace.[127] Specifically, the act states that "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful"[128] and that The Commission may commence a civil action to recover a civil penalty in a district court of the United States against any person, partnership, or corporation which violates any rule under this chapter respecting unfair or deceptive acts or practices . . . with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule.[129]

In total, the FTC has brought more than 40 general privacy lawsuits.[130]

One recent example of an FTC action aimed at protecting consumers from having their data collected in a way that was not disclosed to them is their action against the Android App, called The Brightest Flashlight.[131] This app is characterized by the FTC as "one of the most popular free apps on the Android marketplace."[132] In its complaint, the FTC states that when the app is running on a user's mobile phone, it "also transmits, or allows the transmission of, data from the mobile device to various

---

(last visited April 23, 2016), https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises [hereinafter F.T.C., *Enforcing Privacy*]

126 *Id.*

127 *Id.*

128 15 U.S.C. § 45 (Westlaw through 2013).

129 *Id.*

130 F.T.C., *Security Update, supra* note 123, at 14 ("The FTC has brought enforcement actions addressing a wide range of privacy issues, including spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile. These matters include over 130 spam and spyware cases and more than 40 general privacy lawsuits.").

131 Nicole Vincent Fleming, *Sharing Your Location . . . In a Flash, Federal Trade Commission*, F.T.C. (Dec. 5, 2013), http://www.consumer.ftc.gov/blog/sharing-your-location-flash (Since February 2011, "people have downloaded the Brightest Flashlight app to more than 50 million Android devices – making it one of the most popular free apps on the Android marketplace. According to the FTC, most of these users probably didn't realize that anytime they launched the app, it collected and broadcasted their locations and device IDs to advertising networks and other third parties.").

132 *Id.*

third parties, including advertising networks."[133] The types of data transmitted include, among other things, the device's precise geolocation along with persistent device identifiers that can be used to track a user's location over time."[134] Android phones do give notice to consumers regarding what sensitive data and functionality an app has access too, such as geolocation and the capacity to take photos with a device's camera, the app fails to "explain whether the application shares any information with third parties."[135] The app itself, through its promotion pages, fails to mention the collection or use of consumer data at all.[136]

The app's privacy policy, which is quoted in the complaint, states that:

> Goldenshores Technologies and its subsidiaries and agents may collect, maintain, process and use diagnostic, technical and related information, including but not limited to information about your computer, system and application software, and peripherals, that is gathered periodically to facilitate the provision of software updates, product support and other services to you (if any) related to the Goldenshores Technologies Software, and to verify compliance with the terms of the License. Goldenshores Technologies may use this information, as long as it is in a form that does not personally identify you, to improve our products or to provide services or technologies to you.[137]

This policy fails to inform those who download the app that whatever data they transmit, including device identifiers, is repeatedly disclosed to third parties, which include various advertising networks.[138] Being that "[t]hese facts would be material to users in their decision to install the application [. . .] [t]he failure to disclose, or adequately disclose, these facts, in light of the representation made, was, and is, a deceptive practice."[139] In addition, while the app gives users the impression that they have the ability to opt out of the terms of the Brightest Flashlight App, including those terms which address data

---

[133] Complaint at 2, In the Matter of Goldenshores Technologies, LLC et al., (F.T.C. 2013) (No. C-4446) https://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.* at 4.

[138] *Id.* at 3.

[139] Complaint at 4–5, In the Matter of Goldenshores Technologies, LLC et al., (F.T.C. 2013) (No. C-4446) https://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf

collection, this is not in fact the case.[140] The app "transmits, or causes the transmission of, device data as soon as the consumer launches the application and before they have chosen to accept or refuse the terms of [the app]."[141]

The complaint resulted in an order by the FTC mandating that Brightest Flashlight shall not misrepresent: "(A) The extent to which Covered Information is collected, used, disclosed, or shared; and (B) The extent to which users may exercise control over the collection, use, disclosure, or sharing of Covered Information collected from or about them, their computers or devices or their online activities."[142] In addition, the FTC ordered that the company may not use geolocation data without prominently displaying the following disclosures immediately before the initial collection or transmission of such data: "(1) That such application collects, transmits, or allows the transmission of, geolocation information; (2) How geolocation information may be used; (3) Why such application is accessing geolocation information; and (4) The identity or specific categories of third parties that receive geolocation information directly or indirectly from such application[.][143] Subsequently the application must obtain affirmative consent from the user.[144]

While FTC action does provide mobile phone users with some protection against the unauthorized collection of their data, more is still needed. As previously stated, the FTC's enforcement power is applicable only against those defendants who violate their own privacy policies.[145] Legislation by Congress mandating that mobile application's coverage, use and collection of user's data be initially disclosed through these privacy policies would further protect consumers.

iii. Congress's Legislation

The Application Privacy, Protection, and Security (APPS) Act was introduced in the House during May of 2013 and is still awaiting a vote.[146] The bill directs mobile phone application

---

[140] *Id.* at 4.

[141] *Id.* at 5.

[142] Decision and Order at 3, In the Matter of Goldenshores Technologies LLC et al., (F.T.C. March 13, 2014) (No. C-4446).

[143] *Id.* at 4.

[144] *Id.*

[145] F.T.C., *Enforcing Privacy, supra* note 125.

[146] *See* Application Privacy, Protection, and Security Act of 2013, H.R. 1913, 113th Cong. (proposed May 9, 2013), https://www.congress.gov/bill/113th-

developers to notify users as to personal data that the application is about to collect and obtain the user's consent regarding "the terms and conditions governing the collection, use, storage, and sharing of such personal data."[147] The bill specifically excludes any personal data, referred to as "'de-identified data' . . . that cannot reasonably be used to identify or infer information about, or otherwise be linked to, a particular individual or mobile device[.]",[148] The bill directs app directors to provide users with a way to withdraw their consent and delete any user data on their servers, if the user should so desire after withdrawing their consent.[149] Finally, it requires that app developers "take reasonable and appropriate measures to prevent unauthorized access to personal and de-identified data[.]"[150]

If ever passed, the APPS Act would be the first federal law specifically aimed at regulating mobile applications.[151] Enforceability remains an obstacle for such a law, given the number of applications on the market, and that "mandatory notices and disclosures - even when provided - may not effectively communicate information that is sufficiently detailed to protect consumers."[152] Despite this, providing app users with the right under federal law to request for an app to stop collecting and delete any previously collected their personally identifiable data would be a positive step for consumer privacy, as currently "it is almost impossible to withdraw consent or protect one's data from developers."[153] The initial step in creating a consumer right to privacy in their personally identifiable data is to further educate consumers as to exactly what data they are sharing. The next step is to educate app developers in what steps they can take to

---

congress/house-bill/1913 (providing for greater transparency in and user control over the treatment of data collected by mobile applications and to enhance the security of such data); *see also* Katherine Gnadinger, Comment, *The Apps Act: Regulation of Mobile Application Privacy*, 17 SMU SCI. & TECH. L. Rev. 415, 417 (2014) (urging mobile application platforms and developers to create regulations and standards for collecting private information and informing consumers about this collection).

147 H.R. 1913, *supra* note 146.

148 *Id.*

149 *Id.*

150 *Id.*

151 *See* Gnadinger, *supra* note 146, at 417 (stating that "as the first federal law focused specifically on mobile applications, [the APPs Act] can set a precedent for mobile privacy laws in the United States.").

152 *Id.* at 418.

153 *Id*. at 437.

obtain consumer trust, mainly through meaningful notice and consent, along with limiting the amount of personally identifiable data an app may collect.

5. CONCLUSION

Beacon technology can potentially play an important role in retailer's omnichannel marketing strategies aimed at revitalizing in in-store sales. The successful implementation of in-store retail beacons requires that accompanying mobile applications gain user's trust. If beacon enabling mobile applications can gain user's trust in relation to privacy concerns and become a tool that consumers are willing to use in order to enhance their shopping experience, then beacons have the potential to help stimulate in-store shopping. An application that gives the sense of following users through stores has the unique challenge of acquiring information and reformulating the information for users in ways that produce spending without making the user feel they are being shadowed by a force that is guiding their hand. The "Big Brother" potential for beacons is a unique challenge because beacon-enabling applications are designed both to be useful to shoppers and generate specific consumer behavior. Strategizing the benefits of beacon technology in the context of a live shopping experience is the challenge beacons ultimately faces.