Sacrificing Privacy for Convenience: The Need for Stricter FTC Regulations in an Age of Smartphone Surveillance

Ashton McKinnon

Follow this and additional works at: https://digitalcommons.pepperdine.edu/naalj

Part of the Administrative Law Commons, Consumer Protection Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation
Available at: https://digitalcommons.pepperdine.edu/naalj/vol34/iss2/6

This Comment is brought to you for free and open access by the School of Law at Pepperdine Digital Commons. It has been accepted for inclusion in Journal of the National Association of Administrative Law Judiciary by an authorized editor of Pepperdine Digital Commons. For more information, please contact Katrina.Gallardo@pepperdine.edu, anna.speth@pepperdine.edu.
Sacrificing Privacy for Convenience: The Need for Stricter FTC Regulations in an Age of Smartphone Surveillance

By Ashton McKinnon*

TABLE OF CONTENTS

I. INTRODUCTION ................................................................. 486
II. THE SMARTPHONE ............................................................ 488
III. APPS ............................................................................. 492
IV. CONSUMER REASONABLE EXPECTATION TO PRIVACY .......... 498
   A. Privacy Under Katz ...................................................... 498
   B. Technology Advances and the Supreme Court After Katz—
      Smith v. Maryland ............................................................. 500
      1. When Civil Behavior is Subject to Criminal Context .... 501
   C. What’s New? In re HTC America, Inc. ........................... 504
      1. The Claims of the FTC .................................................. 507
      2. Implications of the HTC Settlement ......................... 508
   D. The Sneaky Path: Path Inc.’s Social Networking App .... 509
V. REGULATION INITIATIVES .................................................. 511
   A. Mobile Device Privacy Act Proposal ............................ 511
   B. Senator Al Franken’s Location Privacy Bill .................... 513
      1. The Location Privacy Protection Bill ........................... 513
      2. Supreme Court Uncertainty Still Remains ................ 516
   C. The FTC’s Privacy Agenda for 2014 .............................. 517
      1. Data Transparency .................................................... 518
      2. Mobile Technologies and Connected Devices ......... 518
      3. Sensitive Data Involving Children, Health Information, and Financial Data ........................................... 519
VI. THE PLEA FOR REFORM .................................................... 519
A. Smartphones Are Computers Too: A Suggestion for Proper Regulatory Oversight ........................................................... 520
B. The Internet of Things .......................................................... 521
C. Not for Nothing: The FTC’s Efforts Toward Reform .......... 522
   1. The FTC’s Suggestions for Mobile Platforms .................. 523
   2. The FTC’s Suggestions for App Developers .................... 524
   3. The FTC’s Suggestions for Advertising Networks and Other Third Parties ........................................................... 525

VII. CONCLUSION ............................................................................ 526
I. INTRODUCTION

Part of the Federal Trade Commission’s (FTC) mission is to prevent business practices that are unfair to consumers and to enhance informed consumer choice. Paired with maintaining the balance to keep a competitive economic market and legitimate business practices, the goals of the FTC with respect to the consumer seem to fall secondary on the priority scale regarding the popular, and arguably necessary, uses and distribution of the smartphone. Privacy concerns are nothing new in today’s society, and the increase in the variety of devices that keep us connected is only going to continue to exacerbate these concerns.

---

2 See id.
One of the most challenging aspects of this issue lies in the dichotomy between privacy and convenience. Many of the same technologies that threaten consumer privacy are also the critical technologies that provide consumer convenience. This comment aims to focus on the most frequently used connector that consumers treasure not only for convenience but also as a lifelong necessity—the smartphone.

The majority of the population craves a data-driven, highly-networked present and future reality, and although some companies engaged in online commerce are already involved in the adoption of self-regulation methods, it is time for the FTC to step in and prioritize the consumer at the same level and degree in which it supports the competitive market. The FTC needs to enforce federally mandated guidelines that will allow the consumer to use technology without the technology using the consumer.

Part II of this comment focuses on the type of information that can be collected by various companies, service providers, and agencies from an individual’s smartphone, and the intentions of these collectors behind use of this information.4

Part III evaluates how applications (apps) contribute to this scheme, and, specifically, apps’ recordkeeping role in direct marketing, advertising initiatives, and user location tracking.5

Part IV reiterates a consumer’s reasonable expectation of privacy under *Katz v. United States*,6 its developing application to technological changes, and delves further into the two most recent cases brought by the FTC: *HTC America, Inc.*7 and *United States v. Path, Inc.*8

Part V discusses the various actors that are currently engaged in implementation of regulation strategies in an effort to balance the

---

4 See discussion infra Part II.
5 See discussion infra Part III.
need for government intervention against excessive government control.9

Part VI concludes by suggesting that there is an urgent need for the FTC to implement concrete regulations to clearly identify and protect impermissible accessible data from consumer smartphones.10

II. THE SMARTPHONE

Ask your neighbors, friends, siblings, or business partners if they own a smartphone and the likely response will be, “Sure, yeah, I’ve got an iPhone.” While Apple Inc.’s iPhone may be the most widely recognized smartphone among today’s consumers, it may come as a shock that it is actually the number two smartphone provider in the industry overall.11 As of July 2013, Samsung was the top smartphone provider dominating the market share at 30.4% and carrying the lead in unit shipments—over 72 million worldwide.12 Apple Inc. claimed the second leading spot, but rather at a distance to Samsung.13 Apple Inc. fills the market share worldwide at a mere 13.1% with unit shipments over 31 million worldwide.14 According to a 2013 Pew Internet Report, 91% of the American adult population owns a cell phone, and of that 91%, 55% of these adults would classify their cell phone as a smartphone.15 This unremarkable majority figure may seem insignificant in reference to privacy reform; however, it is important to note that this percentage only applies to the adult population. What happens when we consider the line of middle school students seen waiting for the school bus on a commute to work? It is likely that an overwhelming majority of

9 See discussion infra Part V.
10 See discussion infra Part VI.
12 Id.
13 Id.
14 Id.
those students are all staring at those illuminated screens of addicting entertainment, revealing an instant text message, Facebook notification, Words With Friends invite, etc.

What is more revealing than the “tweens” not factored into user statistics—although very much part of the equation—is that service providers can and are obtaining information from tween users as much as that of the adult population. At the bare minimum, service providers can collect the following:

- Incoming and outgoing calls: the phone numbers you call, the numbers that you receive calls from, and the duration of the call;
- Incoming and outgoing text messages: the phone numbers you send texts to and receive texts from;
- How often you check your e-mail or access the Internet; [and]

---

16 Words With Friends is a mobile game accessible to both Android and iOS smartphone users through an app database. See About, ZYNAGWITHFRIENDS, www.zyngawithfriends.com/en/about (last visited Jan. 13, 2015). Players of the game exchange turns forming words horizontally or vertically on the board to try to score as many points as possible for each word. See Words With Friends: Rulebook, available at http://www.zyngawithfriends.com/wordswithfriends/support/WWF_Rulebook.html (last visited Jan. 13, 2015) The popular game was developed by Newtoy, a Texas-based mobile game company that was founded in 2008 by brothers Paul and David Bettner. See About, supra. In December 2010, Zynga acquired Newtoy and expanded the mobile game concept to include games such as Scramble With Friends, Hanging With Friends, and Chess With Friends. Id.

17 The term “tween” refers to a specific marketing demographic that is defined as in-between the age of a child and the age of a teen. See Tween Definition, DICTIONARY.COM, http://dictionary.reference.com/browse/tween?s=t (last visited Jan. 5, 2015). It is a popularly coined and frequently used term in the media market due to its reference to the state in which a former child is experimenting with common teenage rebellious acts and thus tend to be conformist. See generally Sharon Jayson, It’s Cooler Than Ever To Be A Tween, But Is Childhood Lost?, USA TODAY (Feb. 4, 2009, 4:31 PM), http://usatoday30.usatoday.com/news/health/2009-02-03-tweens-behavior_N.htm. Currently, there are 20 million tweens in the United States and that number is only expected to rise. Id.

• Your location.\textsuperscript{19}

Unfortunately, smartphone users cannot stop service providers from collecting this information.\textsuperscript{20}

Not scared yet? According to another research assistant at Pew, of the 91\% of adult Americans that own a cell phone, 81\% reported using that device to send or receive text messages.\textsuperscript{21} Over half of this 81\% either send or receive e-mail messages from their phone\textsuperscript{22} and “six-in-ten cell owners access the Internet on their phones.”\textsuperscript{23} The same study by this researcher revealed that of these cell phone owners that access e-mail and the Internet, more than one-third reported that their cell phone “is their primary point of Internet access.”\textsuperscript{24} And, if you already fall into the e-mail-user or Internet-user category of all cell phone users and use your phone to get directions to that special new restaurant for date night, there is no need to panic; you are also part of the 49\% of cell phone owners that use their phones for directions and recommendations.\textsuperscript{25} But does your service provider really need to be a part of your special date night?

According to the \textit{New York Times}, there are only three things that matter when it comes to consumer data collection: “location, location, location.”\textsuperscript{26} In the tech-advancement “craze and crave,” consumers have essentially created a new trade in the business and economic subsectors of the marketplace. This new trade is a “conscious consumer submission to surveillance for the sake of convenience.”\textsuperscript{27} Of course the convenience aspect of cell phones is

\textsuperscript{19} Id.
\textsuperscript{20} Id.
\textsuperscript{22} Id.
\textsuperscript{23} Id.
\textsuperscript{24} Id. (emphasis added).
\textsuperscript{25} Id.
\textsuperscript{27} Id.
desired, but it is unlikely that consumers knew that this perk came at the price of having their network provider or other third party continuously record and share their precise movements. Many data aggregators are actually third parties who collect, analyze, and act upon information received on behalf of the first party (the original client, e.g., a service provider or app-developer, rather than the consumer) or fourth parties engaged in additional submarket analysis and reporting. The issue is whether this consumer submission is really a conscious decision or an unwitting acquiescence to pervasive surveillance and tracking for the sake of having the most valuable smartphone amenity—the app.

However, mere collection of information is not what is of highest concern here. Some would argue that, as a consumer, we voluntarily allow companies to access certain data to maintain their competitive edge, and as long as we are satisfied as a purchaser, does it even matter? Rather, it is all part of the vendor-consumer, offer-acceptance, seller-buyer exchange that we have come to respect as

---

28 Data aggregators, also known as data brokers, collect information primarily from public records and criminal databases, but can access other resources. Deborah Pierce & Linda Ackerman, Data Aggregators: A Study of Data Quality and Responsiveness, May 19, 2005, available at http://www.csun.edu/~dwm3265/IS312/DataAggregatorsStudy.pdf. After they collect information, they package it into reports that the broker then sells to businesses, ideally for marketing purposes. Id. Data brokers also sell information to local, state, and federal government agencies. Id. The two most common brokers are ChoicePoint and Acxiom. Id. Though beyond the scope of this article, these companies allow individuals to request their own “consumer reports,” which contain basic biographical information such as name, date of birth, current address, and phone number. Id. Furthermore, “[e]ligible and qualified third parties can request employee background check reports, which contain far more detailed information such as past addresses and length of residence, business affiliations, professional licenses, and criminal history.” Id.

29 Submarket analysis and reporting occurs when an individual app developer or app manufacturing company employs its own data aggregators to gather information from the market (i.e., smart phone users) to use for the benefit of furthering advancement and innovation in their submarket (i.e., apps). See generally Mobile Advertising Market Analysis, Outlook, and Forecasts 2014–2019, CLOUD COMPUTING MAGAZINE, Sept. 19, 2014, available at http://cloud-computing.tmcnet.com/news/2014/09/19/8026706.htm (providing various market research reports accessible to advertising agencies, device manufacturers, content aggregators, etc.).

30 Singer, supra note 26.
our obligation as participants in the economic marketplace. Comfortable with this rationale or not, and assuming that consumers know the “fine-print” regarding the purchase of their smartphones, should your information become the possession of the provider just because you participated in the marketplace? Further, is your provider now the pilot of your personal information, free to distribute it to third and fourth parties? Whether you care about the data aggregation aspect or not, companies that collect your information do so indefinitely, and what they do with it, or what they can do with it, should be your greatest concern.

Currently, there is no combat for consumers to prevent a service provider from collecting the aforementioned data. However, consumers can minimally control their mobile information privacy when it comes to third parties, such as apps, advertising, and social networking platforms.31

III. Apps

“Two key privacy concerns for U.S. consumers arising from mobile advertising practices are: 1) the collection, use, and disclosure of consumers’ personally identifying information that accompanies mobile advertising; and 2) the generation of unsolicited mobile advertising.”32 As consumers, we should have the right to decide, through informed consent, whether to allow collection, use, and disclosure of our information, and whether to participate in mobile advertising.33

Currently, however, this is not our choice, and the market appeal of mobile apps feeds into our disregard for control over this issue. Samsung and Apple Inc.’s domination of the smartphone market has much to do with these manufacturers’ ability to turn a simple handheld phone into a portal of accessibility through apps. Smartphone apps allow mobile users to do more than they would be

31 Social networking is no longer limited to websites; rather, the full understanding encompasses e-mail, group iMessaging, video streaming, and gaming, as well as other features catered to the mobile presences competition. For specific examples, see generally Mobile Social Networking, GOMO NEWS, available at http://www.gomonews.com/mosol (last visited Jan. 17, 2015).
32 King, supra note 3, at 232.
33 Id. at 233.
able to do on a traditional cell phone. Available apps include social networking, gaming, banking, music, news, maps, and more.

Companies of all sizes, aware that consumers desire apps, have entered the market to encourage continued consumer participation in their business. Currently, the iPhone App Store offers over 1 million apps for Apple devices, and Android devices remain competitive with over 1.3 million apps on the market. Today, half of smartphone owners use their devices to download apps, surpassing that of cell phone functions utilized for directions and location-based services that are pre-installed on the device and do not require app configuration. According to the research of trends in the smartphone industry, app downloads across the iOS and Android spheres were estimated to reach 102 billion in 2013—this number includes free apps, as well as purchased apps.

The iOS system is a user interface created, developed, and distributed by Apple Inc. since its unveiling in 2007. The user interface of iOS is based on the direct manipulation of multi-touch gestures. Apple Inc. claims that iOS provides built-in security features that are activated the moment users turn on their device to help secure users’ personal information by preventing unauthorized access to the device through passcodes. When the device owner uses a passcode, iOS automatically enables an encryption that protects that user’s e-mail, and prevents third-party apps from disseminating sensitive information. Apple Inc. also proclaims that the iOS interface is designed to put consumer privacy first:

34 See Sarah Perez, iTunes App Store Now Has 1.2 Million Apps, Has Seen 75 Billion Downloads To Date, TC NEWSLETTERS, TECHCRUNCH (posted June 2, 2014), available at http://techcrunch.com/2014/06/02/itunes-app-store-now-has-1-2-million-apps-has-seen-75-billion-downloads-to-date/ (last visited Dec. 1, 2014).
36 Duggan, supra note 21.
39 Id.
40 Id.
41 Id.
For example, if an app wants your location information or data from Calendar, Contacts, Reminders, or Photos, it needs your permission first. Your conversations over iMessage and FaceTime are encrypted. So no one but you and the person you’re talking to can see or read what’s being said. And features built into Safari give you the ability to browse privately, block cookies, and prevent websites from tracking you.\(^\text{42}\)

Android is the platform operating system for devices from smartphone and tablet makers such as Samsung, HTC, LG, Motorola, and Asus for hundreds of millions of devices in more than 190 countries around the world.\(^\text{43}\) It is the largest installed base of any mobile platform and has a unique open marketplace that gives users and developers a platform for creating apps and games with the ability to distribute them instantly.\(^\text{44}\) This open marketplace resource provides a high level of consumer and seller control over which apps are sold, downloaded, played, or shared. However, this open marketplace also nurtures less control over the security or integrity of the information accessible by the app, given that the apps are not independently vetted or tested before being made available to consumers.\(^\text{45}\)

The \textit{Wall Street Journal} (Journal) conducted an investigation in 2010 that revealed just how intrusive smartphone apps can be with regard to consumers’ personal data.\(^\text{46}\) The Journal examined 101 of the most popular smartphone apps for iPhone and Android operating systems.\(^\text{47}\) Through this investigation, the Journal discovered that

\(^{42}\) \textit{Id.}  
\(^{43}\) \textit{See Developers, ANDROID, developer.android.com/about/index.html} (last visited Feb. 6, 2014).  
\(^{44}\) \textit{Id.}  
\(^{45}\) \textit{Id.}  
\(^{47}\) \textit{Id.}
fall of these apps “transmitted the phone’s unique device ID to
other companies without users’ awareness or consent[.]”48 and that
forty-seven of these apps transmitted the phone’s geographic
location.49 Of the thousands of apps that exist, only five apps—a
significantly smaller number—sent “age, gender, and other personal
details to outsiders” without the knowledge or consent of the
consumers involved.50 Though the Journal gave credit to an Apple
Inc. spokesperson for admitting that Apple Inc. considers privacy and
trust important (the company has supposedly created privacy
protections for consumers), these newly created protections were
specific only to location-based protections.51

Unlike a desktop computer where the consumer can block or
delete “cookies,” the smartphone does not allow the consumer to
block or delete “cookies” for particular apps. This distinction
between consumer control over cookies on a computer versus that of
apps is significant. A cookie’s function as a storage mechanism
enables privacy intrusion at the most basic level of a user’s online
experience. Cookies typically record a computer user’s
preferences.53 However, the cookie identifies the requested
information, as well as pages that have been viewed from a website.54
Therefore, any device that can access the Internet and browse
webpages is subject to cookies and collection of that user’s
information.

48 Id.
49 Id.
50 Id.
51 See id.
52 A “cookie,” also known as a “web cookie,” is a small piece of data sent from
a website and stored in a user’s web browser during the time that user is browsing
that particular site. What are cookies?, COOKIECENTRAL.COM,
http://www.cookiecentral.com/cm002.htm (last visited Jan. 17, 2015). It is a text
file saved in a user’s browser directory or folder and stored in RAM (otherwise
known as “random access memory”) while that browser is running. Id. While
most of the information in a cookie is innocuous, some websites use cookies to
store a user’s personal preferences or tracking data. The Cookie Concept,
COOKIECENTRAL.COM, http://www.cookiecentral.com/c_concept.htm (last visited
Feb. 6, 2014).
53 Michelle Z. Hall, Internet Privacy or Information Piracy: Spinning Lies on
54 Id.
Internet providers have been persistent in their arguments that cookies are not privacy violations and that they are actually necessary. Although a cookie cannot be placed on a computer without the user’s permission, if a user refuses to permit the use of a cookie, access to the content on the page they wish to view may be compromised and limited, or even completely prohibited. Another part of the Internet provider’s argument is that because the Internet does not store data or information regarding where a user has previously browsed, “a cookie is required to allow the accessed content provider instant retrieval of what information a user has previously sought.” When the cookie is placed on the user’s computer hard drive, the information collected can be compiled and sold to direct marketers. They can then use that user’s unique web address to specifically target their products to that user.

---

55 Id. This is yet another instance of privacy versus convenience. Cookies are not strictly necessary for consumers to accept if they wish simply to browse web pages, but they may be necessary to conduct transactions such as to establish user names for personalized access to certain pages or to add or subtract contents of a shopping cart. See generally Jay P. Kesan & Rajiv C. Shah, Deconstructing Code, 6 Yale J.L. & Tech. 277 (2003–2004). In these instances, cookies function as a storage chamber in control of session identification of a user per each webpage visit. Id.

56 See Hall, supra note 53, at 614–15. The default configuration of some browsers is to permit cookies, even third party cookies. Id. at 614. Technically, unsophisticated users may not be aware that the settings on their computer system can be changed or know how to change them, thus exposing more users and their activities to unwanted trackers. See generally id.

57 Id. at 615. The Internet is unique in that it has a “stateless” system. Leonid Braginski & Matthew Powell, Running Microsoft Internet Information Server, 621–47 (David Clark et al. eds.,1998). A “stateless” system means that it does not retain any information data regarding which websites and pages the user has already viewed and visited. Id. Because the Internet functions as a portal of the constant transfer of information through the required exchange of data via a Hypertext Transfer Protocol (known as “HTTP” and is the foundation of data communication for the World Wide Web), the host computer needs to know what information has previously been viewed and does so by placing a cookie on that computer’s hard drive. Id.

Just like the intention behind apps today, the cookie protocol was originally designed for consumer convenience.\textsuperscript{59} Malicious behavior of third parties and growing consumer knowledge about technology has forced privacy advocates to speak out and initiate reforms to protect consumer privacy.\textsuperscript{60}

Few exceptions do exist where smartphone users can “opt-out”\textsuperscript{61} of phone tracking, but many apps do not offer even the basic expectation of consumer protection in the form of written privacy policies.\textsuperscript{62} At the time the Journal investigated 101 apps, forty-five of these did not provide consumers with a privacy policy that was listed on their websites, nor did the policy appear anywhere inside the apps themselves.\textsuperscript{63} The Journal also reported that neither Apple Inc. nor Google required app privacy policies.\textsuperscript{64} Even if the policies are not required, there are some app manufacturers that have responded to the privacy concern and have included access permissions that the consumer must acknowledge before they are granted the ability to download the app.\textsuperscript{65}

These permission features function exactly how you would expect, or have experienced, on your computer when downloading a new program or software that requires a “click of acceptance” to proceed with installation. Computer software companies rely heavily on the use of “shrinkwrap” license agreements\textsuperscript{66} due to their ability to


\textsuperscript{60} Id.

\textsuperscript{61} Similar to consumer choice to opt-out of enabling cookies on certain websites that warrant that privilege—assuming that option is available—if no active steps are taken by the user to opt-out, then the computer typically accepts the cookie without the user’s knowledge under the presumption that the user implicitly consents. Hall, supra note 53, at 615.

\textsuperscript{62} Thurm & Kane, supra note 46.

\textsuperscript{63} Id.

\textsuperscript{64} Id.

\textsuperscript{65} Id.

\textsuperscript{66} The permission features are much like the common practice of “shrinkwrap” license agreements for downloading software. Shrinkwrap agreements are unsigned license agreements that state that the acceptances on the part of the user of the terms of the agreement are indicated by opening of the software, use of the software, or some other specified mechanism in the license; see David L. Hayes,
gain consumer consent on a distribution level that reaches the mass market.

App permissions are much like these “shrinkwrap” agreements. They are heavy with small text and legalese that the majority of consumers scroll through and accept without a clear understanding of what exactly they have agreed to. These acknowledgments essentially serve as the terms of agreement to proceed with the download of the app. However, what is not made clear to consumers in agreeing to these steps to permission is that “once the permissions are accepted, many apps then have access to every piece of data” on the smartphone they are downloaded to.67

IV. CONSUMER REASONABLE EXPECTATION TO PRIVACY

A. Privacy Under Katz

In Katz v. United States, the Supreme Court expressly determined that the Fourth Amendment protects people rather than places.68 In Katz, the petitioner was convicted of transferring wagering information by telephone, from a telephone booth, in violation of a federal statute.69 At trial, the Government was permitted to introduce evidence overheard by FBI agents, obtained by electronic listening


68 389 U.S. 347, 351 (1967); see Who Knows Where You’ve Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators, 18 HARV. J.L. & TECH. 307, 313 (2004) (referencing Justice Harlan’s concurring opinion, which articulated the two-prong test courts must apply when determining whether a person’s rights have been violated under the Fourth Amendment). Justice Harlan opined that the claimant first “needs to demonstrate that he or she had a subjective expectation of privacy in the place” in which he or she was searched, and “[i]f so, [then] the question [becomes] whether society recognize[d] that expectation as reasonable.” Id.

69 389 U.S. at 348.
and recording devices that were placed outside the public telephone booth where the petitioner conducted the calls.\footnote{Id.}

The court of appeals affirmed the petitioner’s conviction by contending that the recordings were not obtained in violation of the Fourth Amendment because there was no actual, physical entry into the telephone booth by the Government or agents acting on its behalf.\footnote{Id. at 349.} The Supreme Court granted certiorari to clarify two important constitutional questions: (1) “[w]hether a public telephone booth is a constitutionally protected area,” and (2) “[w]hether physical penetration of a constitutionally protected area is necessary . . . to be violative of [an individual’s] Fourth Amendment” rights.\footnote{Id. at 349–50 (emphasis added).}

In conclusion, the judgment against the petitioner was reversed because the Supreme Court affirmed that the Government’s activities in “electronically listening to and recording the petitioner’s words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a ‘search and seizure’ within the meaning of the Fourth Amendment.”\footnote{Id. at 353.}

\textit{Katz} provides important considerations when evaluating an individual’s right to privacy.\footnote{Id.} The most notable of these is the majority’s consensus that an individual’s right to privacy is the right of the \textit{person}.\footnote{Id.} If it was reasonable for the petitioner in \textit{Katz} to rely on enclosing himself in a public telephone booth to warrant privacy protections, should it not also be justified that ownership of a personal smartphone in which one encloses their communications within also warrants privacy protection?\footnote{Id. at 361 (Harlan, J., concurring) (“The critical fact in this case is that ‘one who occupies it, (a telephone booth) shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume’ that his conversation is not being intercepted. The point is not that the booth is ‘accessible to the public’ at other times, but that it is a temporarily private place whose momentary occupants’ expectations of freedom from intrusion are recognized as reasonable.’”) (brackets omitted).} Use of a personal
smartphone in public does not—and should not—grant the public access to how that phone is personally used.

Particular government intrusion aspects aside, a consumer’s expectation to privacy becomes individualized protection of their person when they purchase the smartphone and pay for the service provider plan. Although these are all functions available to the public, personal privacy components should be construed in favor of the individual who has ownership of the device, as made clear under our Fourth Amendment rights and explicitly determined in *Katz*.

### B. *Technology Advances and the Supreme Court After Katz—Smith v. Maryland*

Not too long after the Supreme Court’s ruling in *Katz*, it became necessary to expand the application and interpretation of the reasonableness test proffered in the case, as technologies became part of the consumer’s person. Twelve years after *Katz*, *Smith v. Maryland* forced the Court to decide whether the installation and use of a pen register to record any and all phone numbers from the line on which the numbers were dialed, constituted a search and thus a violation of a person’s Fourth Amendment rights.

In *Smith*, the petitioner claimed that he had a legitimate expectation of privacy that was infringed upon by the Government’s application of the pen register device. The Court invalidated the petitioner’s claim by maintaining that a pen register was wholly different from the listening device used in *Katz* because a pen register does not possess the quality function to acquire the content of any communications.

---

77 442 U.S. 735 (1979).
78 A pen register is a mechanical device that is usually installed at a central telephone facility (as opposed to an individual’s private residence) that records the numbers dialed on a telephone by monitoring electrical impulses caused when the dial on the telephone is released. *Erwin Chemerinsky & Laurie L. Levenson, Criminal Procedure: Investigation* 85 n.4 (2d ed. 2013).
79 442 U.S. at 376.
80 *Chemerinsky & Levenson, supra* note 78, at 87.
81 *Id.* A pen register “does not overhear oral communications and does not indicate whether calls are actually completed.” *Id.* at 85 n.4.
Additionally, the Court reasoned that even if the petitioner had a subjective expectation of privacy in the numbers he dialed, those numbers had to be conveyed to the telephone company before they could be transmitted to the intended receiver.\textsuperscript{82} The Court reasoned that by conveying such information, the caller is waiving his right to privacy; therefore, this is not an expectation of privacy that society would recognize as reasonable.\textsuperscript{83} Essentially, the Court’s determination amounts to the precedent that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.\textsuperscript{84}

1. When Civil Behavior is Subject to Criminal Context

Without a network operator, and likely a contract binding you to certain fees and year-length terms, your smartphone would not be able to function in the capacity to service your needs and wants. Interaction with that network operator—such as Verizon, AT&T, T-Mobile, and Sprint—is the third party requirement to the consumer use of a smartphone.

It is likely that most consumers would concede that the collection of information that is criminal in context should be able to be monitored, and consumers engaged in criminal activity should be stripped of privacy protections if doing so stops ongoing and potential crimes and helps keep the population safe. What about the consumers not engaged in criminal activity? Are our privacy

\textsuperscript{82}Id.

\textsuperscript{83}Id. at 88; see also Joshua A. Engel, Doctrinal Collapse: Smart Phones Cause Courts To Reconsider Fourth Amendment Searches of Electronic Devices, 41 U. MEM. L. REV. 233, 241 (Winter 2010) (arguing that a pen register is very much in contrast to a cell phone because cell phone call records and “address book records typically reveal not only whether a call was completed, but also the length of any communication and the identity of the other person”). Engel also points out that Smith fails to have any application to the content of text messages, e-mails, photographs, and other information that is also retained on cell phones but is not shared with the user. Id. Engel maintains that it is fairly obvious that “[f]or these reasons, people likely have a greater and more reasonable expectation of privacy in the calling records maintained in their cell phones than a landline telephone user had in a pen register,” like the scenario in Smith. Id.

\textsuperscript{84}Id.
protections stripped too because we need the third party provider to collect and transmit what we expect to be private communications?

The real issue arises from the “voluntariness” of dissemination of personal information. This is even more complex in a world where there is a growing number of third party data aggregation companies, and apps are becoming the modern day pen register. The third party is not only your service provider, but your music app, recipe app, social media app, weather app, and even more terrifying—your GPS locator or maps app. Each of these apps is storing and possibly sharing information about the products you purchase at the grocery store, which friends you chat with online, the forecast outside your window, and the street you are driving down right now on your way to the bank that holds your entire life savings—all functioning under your “voluntary” consent by the choice you made and the actions you took to download that app. In 2012, Supreme Court Justice Sonia Sotomayor addressed these very concerns in her concurring opinion to the Court’s decision in United States v. Jones.

2. Global Positioning Sotomayor: “A New GPS”

In Jones, the Court was called to determine whether the attachment of a Global Positioning System (“GPS”) device to an

85 Multiple smartphone manufacturers and carriers utilize the mobile logging software known as Carrier IQ. Know the Customer Experience, CARRIER IQ, http://web.carrieriq.com/network-operators/know-the-customer-experience/ (last visited Oct. 14, 2014). Carrier IQ promotes its product as a tool network operators need to understand their consumers and improve customer satisfaction while lowering support costs. Id. Carrier IQ claims that the software agent they employ does not gather content from a consumers’ smartphone; however, a network operator is allowed to select from a series of “measurements” that the agent evaluates in order to detect issues and let network operators “see what consumers see.” Id. The software delivers “user-centric” information based on these measurements directly from a consumer’s mobile device to the network operator. Id.

86 Independent research has shown that Carrier IQ is capable of tracking exactly which apps consumers are running, the location of the smartphone, and even which buttons the consumers press. Chris Velazco, Carrier IQ: How to Find It, And How To Deal With It, TECHCRUNCH NEWS (Dec. 1, 2011), http://techcrunch.com/2011/12/01/cARRIER-IQ-how-to-find-it-and-how-to-deal-with-it/.

87 132 S. Ct. 945 (2012).
individual’s vehicle for purposes of tracking that person’s movements on public streets constitutes an unreasonable search and seizure under the Fourth Amendment. Justice Sotomayor specifically addressed societal expectations in her opinion, noting that these expectations “can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.”

Irrespective of government ascertainment of such information, it is hard to imagine that consumers reasonably expect that their movements will be recorded and aggregated from GPS services. Further, it is unlikely that a consumer would also voluntarily allow such aggregation in a way that permits a third party to discover his or her eating preferences, political agendas, religious beliefs or even sexual habits. More importantly, Justice Sotomayor suggested the Court revisit the premise established in Smith in which the Court declared that an individual has no reasonable expectation of privacy in the information that is voluntarily disclosed to third parties. Her concurring opinion is encouragement for consumers, and holds:

This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

88 Id. at 946; see CHEMERINSKY & LEVENSON, supra note 78, at 38.
89 Smith, 132 S. Ct. at 957.
90 Id.
91 Id.
In the world of technology, change occurs faster than is sometimes comprehensible. Barely two years old, the discussions of Jones might as well have been chiseled in stone, housed in an actual physical structure, and buried far away from the current “at your fingertips” digital archive. Thankfully, Jones’s attention to location tracking started chiseling away at the front door of legislative hesitation.

C. What’s New? In re HTC America, Inc.

Recognizing the rapid and undisciplined growth of smartphones and apps, in February 2013, the FTC finally stood on a pro-consumer platform and addressed particular privacy infringements imposed by HTC America.92 The FTC accused HTC America, a leading Android manufacturer, of failing to secure the software it provided in millions of smartphones it produced.93 The FTC issued its decision in June 2013, ordering HTC America to refrain from any misrepresentation, expressly or implicitly, regarding the security, privacy, confidentiality, and integrity from any covered information94 from or about its consumers.95

---

93 Id.
94 “Covered Information” was defined by the FTC to include the following: [i]Individually-identifiable information from or about an individual consumer collected by respondent through a covered device or input into, stored on, captured with, or transmitted through a covered device, including but not limited to (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an e-mail address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other state-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a ‘cookie,’ a static Internet Protocol (IP) address, a mobile device ID, or processor serial number; (j) precise geolocation data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information; (k) an authentication credential, such as a username
The FTC’s main concern was that the lack of security on the software could permit certain apps on HTC devices to access information such as financial account numbers or other passwords and access codes that serve as a privacy blockade to sensitive information. The FTC explicitly ordered HTC America to:

[E]stablish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing covered devices, and (2) protect the security, confidentiality, and integrity of covered information, whether collected by [HTC] or input into, stored on, captured with, accessed or transmitted through a covered device. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to [HTC’s] size and complexity, the nature and scope of [HTC’s] activities, and the sensitivity of the covered device functionality or covered information . . . .

The FTC’s order included specific provisions requiring HTC America to designate employees to coordinate and remain accountable for the security program, maintain risk management and password; or (l) any other communications or content that is input into, stored on, captured with, accessed or transmitted through a covered device, including but not limited to contacts, e-mails, text messages, photos, videos, and audio recordings.


96 See Mayer, supra note 92.
tactics, provide training and management for employees in response to the new security measure, as well as assess product design, development, and research. The order required HTC America to “secure software design and testing, including secure engineering and defensive programming,” and review, assess, and respond to third party security vulnerability reports.

The FTC maintained that its primary focus was essentially to keep HTC America honest to its Android permission-based security model of operation. Under the Android operating system, third party apps are supposed to only have restricted access to certain user information, such as location information or the contents of text messages. Additionally, third party apps should only have restricted access to device functionality, such as the ability to record audio through the device microphone or take pictures with the camera. This access was granted solely through a permission-based approach that puts control of the access in the hands of the Android device consumer. The third party apps’ responsibility is the requirement to declare, at the installation phase, exactly what information and functionality the app accesses, and then request the user’s permission prior to engaging in such access.

The FTC began its investigation out of concern for prevalent existence of “‘permission re-delegation’ vulnerabilities.” Through its own custom applications and pre-installed software on HTC devices, HTC America was allowing third parties to exploit these pre-installed apps and circumvent the requirement of asking

---

98 Id.
99 Id.
100 Id.
102 Id.
103 Id.
104 Id.
105 Id.
106 Id.
permission from the user. 107 The rationalization for this action was that the user had “consented” to the HTC applications by choosing to purchase HTC America’s version of an Android device. 108 The mounting concerns revealed by investigation into HTC America led to the declaration of three definitive claims by the FTC: (1) that HTC America’s practices constitute unfair business practices due to risk of substantial injury, physical harm to consumers, or both; (2) that HTC America engaged in deceptive business practices; and (3) that HTC America was using a deceptive user interface. 109

I. The Claims of the FTC

With respect to its first claim, the FTC concluded that unfair business practices were causing, or were likely to cause, substantial injury to consumers by potentially compromising their financial information, personal history information, or text message information as well as allowing outsiders to physically track and stalk HTC users by manipulative sensitive device functionalities. 110 To its second claim, by making false or misleading representations about HTC data and device security while also including custom pre-installed applications that negate the operating system’s permission-based security model, HTC America was engaging in deceptive business practices that were contradictory to the business goals established by the FTC. 111 Finally, the FTC singled out the particular “Tell HTC” 112 reporting tool that existed on its Android product

107 Id.
108 The FTC alleged that through the use of logging apps such as HTC Logger and Carrier IQ, HTC was implementing insecure communications mechanisms, given that part of the logging apps’ functions included saving important information about the user and his or her device. Id. According to the FTC, these logging applications stored information such as GPS, network locations, web-browsing, media-viewing history, the user’s personal phone number, text message content, and any other usage and device information specified for collection by network operators. Id.
109 Id.
110 Id.
111 Id.
112 “Tell HTC” is an app feature of HTC Android devices that allows users to send information to HTC when a user experiences a software error or other crash on his or her mobile device. See Tell HTC: HTC Android, T-MOBILE SUPPORT,
device.\textsuperscript{113} According to the FTC, HTC America was using a deceptive user interface in the sense that the tool purported to require user consent before transmitting location data to HTC America, when in fact the data was transmitted without such consent.\textsuperscript{114}

In furtherance of the initiatives that were laid out in the consent order to rectify the issues outlined in the FTC’s three major claims, the FTC also ordered HTC America to develop security patches to fix security vulnerabilities.\textsuperscript{115} HTC America ultimately settled the charges with the FTC and agreed to develop and release these software patches.\textsuperscript{116}

2. \textit{Implications of the HTC Settlement}

This step toward privacy regulation regarding smartphone apps is commendable, but it can also be considered a smoke screen. On the surface, it is an action toward the need for privacy regulation. This order is recognition that companies should not be able to get away with putting its unknowing consumers at such risk. Where the FTC failed is that absent consumer due diligence, this action is fruitless. Smartphone users that own an HTC America phone, assuming they were aware of the impending issues, were required to access the HTC America website to see if their particular smartphone required download of the necessary security patches in order to protect their device from these previously downloaded malicious apps. Consumers are inherently fallible and should never have to suffer for their own lack of due diligence when a national protection agency is in place to take on this responsibility on the consumers’ behalf.

Any other industry would demand a recall as a form of taking action against safety and security on behalf of its consumers, instead

https://support.t-mobile.com/docs/DOC-4108 (last updated June 3, 2014). The idea is for HTC to be able to readily identify and resolve the problem. \textit{Id.} When a user’s device detects an error in the system, a Tell HTC report message automatically appears. \textit{Id.} When implemented, Tell HTC captures information regarding the error report type, package name and version, installation, process name and time, device active time, process active time, system app, device name, model, product, version release, and location related information. \textit{Id.}

\textsuperscript{113} Ritchey et al., \textit{supra} note 101.

\textsuperscript{114} \textit{Id.}

\textsuperscript{115} \textit{Id.}

\textsuperscript{116} \textit{See} Mayer, \textit{supra} note 92.
of forcing consumers to become catalysts for resolving the issues of a product they entrusted not to have those malfunctions in the first place.\footnote{See \textit{The United States Consumer Product Safety Commission}, \url{http://www.cpsc.gov/en/Recalls/}, for examples of recent recalls. \textit{See also \textsc{Recalls.gov}}, \url{http://www.recalls.gov/} (last visited Jan. 26, 2015) (an online resource to view all U.S. government recalls by federal agency jurisdiction.).} As Christopher Olsen, an assistant director in the FTC’s Division of Privacy and Identity Protection, stated: “Consumers don’t have a good idea about what information is being collected and used by various companies and apps . . . . The responsibility really lies with the companies providing mobile services to help consumers determine which apps to download and use.”\footnote{See Mayer, \textit{supra} note 92.}

\subsection*{D. The Sneaky Path: Path Inc.’s Social Networking App}

In February of 2013, Path, Inc. (Path) settled with the FTC over charges brought by the FTC that revealed a social networking app operated by Path was deceiving its users.\footnote{See Press Release, Federal Trade Commission, Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users’ Mobile Address Books (Feb. 1, 2013), \textit{available at} \url{www.ftc.gov/opa/2013/02/path.shtm}.} Path’s deception involved collecting personal information from their consumers’ smartphone device address books without users’ knowledge or consent.\footnote{\textit{Id.}} The Path social networking app allowed users to keep “journals” of moments that occurred in their lives, which they could then share with up to 150 friends.\footnote{\textit{Id.}} The app permitted users to upload, store, and share photos, written thoughts, their location, and even a list of the names of songs that specific users were listening to in real time.\footnote{\textit{Id.}}

The FTC claimed that “the user interface in Path’s iOS app was misleading and provided consumers no meaningful choice regarding the collection of their personal information.”\footnote{\textit{Id.}} The FTC also alleged that the privacy policy that Path provided, deceived
consumers “by claiming that [the app] automatically collected only certain user information such as IP address, operating system, browser type, address of referring site, and site activity information.”124 Therefore, even if a consumer had done their due diligence before downloading the app and then proceeded to agree to its terms and conditions, Path was dishonest with regard to what that consumer agreement actually entailed.

The FTC’s main concern was that if an app company could access a user’s contact list, then it could sell or share that information with anyone, at the company’s discretion,125 thus continuing to multiply members of the third party predator’s club.

Path ultimately agreed to settle with the FTC for a civil penalty in the amount of $800,000, and was also barred from making any misrepresentations about the extent to which it maintains the privacy and confidentiality of its consumers’ personal information.126

In addition to its orders on Path, the FTC introduced the Mobile App Developers: Start with Security business guide as a resource to ensure future app developers’ compliance with reasonable consumer data security.127 In this guide, the FTC urges operating system providers and app developers to “provide smartphone owners with easy-to-understand disclosures about the data they’re collecting and how it could be used.”128

---

124 Id.
125 See Mayer, supra note 92. Path offered a feature to its app called “Add Friends” that allowed users to add new connections to their network through three different options: (1) “Find friends from your contacts[,]” (2) “Find friends from Facebook[,]” or (3) “Invite friends to join Path by email or SMS.” FTC Press Release, supra note 119. However, the FTC discovered that even if a user did not select the option to connect with friends through that user’s contact list, Path automatically collected and stored that personal information from the user’s device. Id.
126 Press Release, supra note 119.
127 Id.
128 Mayer, supra note 92 (emphasis added).
V. REGULATION INITIATIVES

A. Mobile Device Privacy Act Proposal

Introduced to Congress in September 2012 by Representative Edward Markey, a Democrat from Massachusetts, The Mobile Device Privacy Act (MDPA) proposal focused primarily on requiring disclosures to consumers regarding the capability of software to monitor mobile device usage.\(^{129}\) The MDPA also proposed disclosures to require the express consent of the consumer prior to such monitoring, among various other things.\(^{130}\) The MDPA directed the FTC to create official regulations to require sellers or manufacturers of mobile devices, providers of mobile services, and other operators of online services to disclose to consumers information about the installation and use of monitoring software by those companies.\(^{131}\) The MDPA also directed the FTC to require sellers to allow exemptions for uses consistent with a consumer’s reasonable expectation of privacy.\(^{132}\) Specifically, the MDPA asked the FTC to require and implement the following:

(1) \(\text{The express consent of a consumer before monitoring software begins collecting and transmitting information and giving the consumer the opportunity to prohibit such collection and transmission at any time;}\)

(2) \(\text{recipients of information transmitted from monitoring software to implement information security practices for the treatment and protection of the information;}\)

(3) \(\text{the filing with the FTC or the Federal Communications Commission (FCC), as appropriate, of a copy of an agreement under which a person receives the type of information regarding which disclosure is required by this Act provides for enforcement by the FTC and FCC of}\)

---

\(^{130}\) Id.
\(^{131}\) Id.
regulations promulgated under this Act under the Federal Trade Commission Act and the Communications Act of 1934, respectively.\footnote{Id.}

The proposed remedy for violation of the MDPA was the allowance of civil enforcement actions by states and by private persons injured as a result of violation of the above regulations.\footnote{H.R. 6377 (112th): Mobile Device Privacy Act, Summary, supra note 132.}

The MDPA’s driving force of support was its attack on Carrier IQ-style data collection.\footnote{Adi Robertson, Mobile Device Privacy Act, meant to stop Carrier IQ-style data collection, introduced in Congress, THE VERGE (Sept. 14, 2012, 12:26 PM), http://www.theverge.com/2012/9/14/3332018/mobile-device-privacy-act-introduced. See also supra notes 85–86 for an explanation of Carrier IQ.} With MDPA’s success, consumers would be fully informed as to the monitoring software’s details about the type of information that is being collected from their mobile device, who is receiving that collected information, and how that information will be used.\footnote{Id.} Further, the MDPA clarified that consumers must consent to the tracking that monitoring software engages in and must be free to opt out, even if they had initially agreed to have the information collected when they purchased the device or data subscription.\footnote{Id.} Congress’s active participation to meet consumer

\footnote{Id. The Federal Trade Commission Act is the primary statute governing the Commission, specifically outlining the Commission’s responsibilities: to (a) prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce; (b) to seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices; (d) conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and (e) to make reports and legislative recommendations to Congress. Enforcement: Statutes Enforced or Administered by the Commission, FEDERAL TRADE COMMISSION, http://www.ftc.gov/enforcement/statutes (last visited Nov. 1, 2014). The Communications Act of 1934 was enacted to provide for the regulation of interstate and foreign communication by wire or radio, and for its provisions to be executed and enforced by the Federal Communications Commission. 47 U.S.C. § 151 (2012).}
needs and to address a situation the FTC should have already addressed under an established regulatory scheme was short-lived. The MDPA bill was referred to the House Committee of Energy and Commerce and died upon vote. Consumers were once again forced to rely on the promises of monitoring software manufacturers to maintain customer privacy in spite of these same manufacturers’ admissions of, and justifications for, intrusive tracking.

B. Senator Al Franken’s Location Privacy Bill

Senator Al Franken, a Democrat from Minnesota, began his quest for consumer location-based privacy in 2011. Senator Franken feared that once this data was collected, companies would store it and build upon it over time, following location patterns that ultimately could “create an intimate portrait of a person’s familial and professional associations, political and religious beliefs, [and] even health status.” The senator’s main goal has been to establish location data collection as an “opt-in only” condition of technologies, and even after prior failed attempts, he decided to reintroduce his solution bill in 2013.

1. The Location Privacy Protection Bill

The Location Privacy Protection Bill (LPPB) that Senator Franken has been working to refine would essentially require tracking entities, such as app developers, to obtain “explicit, one-time consent,” from a consumer user before recording the locations of that consumer’s mobile devices. In his presentation to the Senate Judiciary Committee, Franken alerted many members when he declared, “[s]omeone who has this information doesn’t just know

139 Singer, supra note 26.
140 Id.
142 Singer, supra note 26.
where you live . . . [t]hey know the roads you take to work, where you drop your kids off at school, the church you attend and the doctors that you visit.” 143

Although in a position of power greater than the average consumer, Franken was wise to appeal to the committee’s consumer side. Senator Franken undoubtedly knew that each member of the committee would be able to relate to some part of that harsh truth, whether they had dropped their kids off at school before coming to the meeting that day, or were considering the new route they would travel home when the meeting was over.

Senator Franken was persuasive, and the Senate Judiciary Committee approved the bill, which also promulgated the requirement for mobile services to disclose the names of the advertising networks and other third parties with whom they may also share consumers’ locational information. 144 Once approved for reintroduction at the start of 2013, LPPB’s relevance was renewed and Franken became outspoken about its necessity once again. 145

In March of 2013, Franken focused his advocacy outreach on provoking public awareness and approval of the opt-in only policy by highlighting the lack thereof by Euclid—a retail analytics firm designed to work with clothing stores, restaurants, and shopping malls to measure in-store consumer activity by tracking the Wi-Fi signals given off by the consumer’s mobile phone. 146 Although Euclid’s privacy policy explains that it only collects “basic device information,” not including “who you are, whom you call, or the websites you visit,” 147 Franken drafted an outcry letter claiming this was not enough:

It’s one thing to track someone’s shopping habits through a loyalty card or credit card purchase; folks understand that their information may be collected. It’s another thing entirely to track consumers’ movements without their permission as they shop,

143 Id.
144 Id.
145 Id.
146 See Tarran, supra note 141.
147 Id.
especially when someone doesn’t buy anything or even enter a store. People have a fundamental right to privacy, and I think neglecting to ask consumers for their permission to track them violates that right.148

In response to Franken’s letter, Euclid’s chief executive officer, Will Smith, explained that Euclid does employ a permanent opt-out process for consumers, and that no data collected is linked to a specific individual.149 Regardless, are we as consumers willing to gamble on the privacy promise of the CEO of any company that has an obvious interest in continuing tracking practices they have already committed to?

Senator Franken was appreciative of the response, attention, and assurance, but was adamant that it was still insufficient.150 Franken did not think that Euclid’s protections satisfied Americans’ fundamental rights and stated, “Euclid’s use of opt-out location tracking—regardless of whether a consumer actually enters a store equipped with this technology—simply doesn’t meet the standard of privacy Americans should be able to count on.”151

Senator Franken’s aversion to quick-fix promises is grounded in the potential development of tracking-based Fourth Amendment violations of unreasonable search and seizure without a warrant—a parallel to be known as “warrantless commercial intrusion.”152 Franken’s LPPB is directed to protect consumer privacy, but his opt-in only policy was an extreme measure meant to provide damage control for future considerations. Among Franken’s many interests is the underlying issue of the future of consumer data property rights and the unpredictable answer to the question of who actually owns the information transmitted and disseminated by an individual who

148 Id. (quoting from a letter Senator Franken sent to Euclid on March 13, 2013).
149 Id.
150 Id.
151 Id. In the concurring opinion in United States v. Jones, 132 S. Ct. 945, 962 (2012), Justice Alito anticipated that “[n]ew technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile.”
152 Singer, supra note 26.
uses a digital mobile device—whether use of that information by a third party without explicit authorization constitutes trespassing.153

2. Supreme Court Uncertainty Still Remains

In June 2011, it was reported that there were more than 322 million wireless devices in use in the United States.154 Whether your wireless device is an older model or a trendy smartphone, location tracking is part of your ownership and use. Unfortunately, even the Supreme Court remains unclear as to whether the expectation of privacy among consumers in this regard falls within the Fourth Amendment context, either under property rights or under personhood rights.

Justice Alito seems to support Justice Sotomayor on these issues, particularly with regard to the Jones case, and offers Senator Franken a statement of gold to present to his colleagues in the legislature:

[286x480]Id.; see also Dr. Saby Ghoshray, Looking Through The Prism of Privacy and Trespass: Smartphones and the Fourth Amendment, 16 UDC L. REV. 73, 82 (Fall 2012) (connecting the sanctity of the home to that of a smartphone, and suggesting that smartphones create an “electronic community” analogous to that of a home). Dr. Ghoshray emphasized that technology sophistication allows individuals to be interconnected in an electronic community created by smartphones through forums such as Twitter, Facebook, and MySpace. Id. Through this community interaction, “[s]martphones are the catalysts for the communication required to form the postmodern electronic community” and a new sphere of privacy arises “in part as a result of the enhanced capabilities of modern smartphones.” Id. Dr. Ghoshray further claims that “[a]n intrusion into an individual’s smartphone has the collateral consequence of desecrating the privacy of both the individual and the community.” Id. at 83.

A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.\textsuperscript{155}

Before the specific concerns of smartphone use, the FTC was confronted with privacy protections of online content in the context of computers, desktops and portable laptops alike. As the world continues along this spectrum of desired connectivity—and at high speeds—the privacy of personal data continues to raise important consumer concerns and legal issues.

\section{The FTC’s Privacy Agenda for 2014}

On December 6, 2013, Jessica Rich, Director of the FTC’s Bureau of Consumer Protection, addressed the International Association of Privacy Professionals to discuss the need for stronger privacy and security protections and why these should be important to every business that touches consumer data, as well as the FTC’s privacy agenda for the upcoming year.\textsuperscript{156} Rich claimed that “privacy is a top priority for the Commission.”\textsuperscript{157} The Commission has placed major mobile players—such as Facebook, Google, and Microsoft—on high alert by filing at least forty-four privacy cases and forty-seven data security cases since 2001.\textsuperscript{158} Rich indicated that the FTC has continued to examine the implications of new technologies on business practices and consumer privacy, and will specifically focus on three areas for the 2014 agenda—data transparency, mobile

\begin{thebibliography}{9} \bibitem{2} \textit{Jones}, 132 S. Ct. at 963–64 (Alito, J., concurring) (emphasis added) (citation omitted).
\bibitem{4} \textit{Id.} at 6.
\bibitem{5} \textit{Id.} at 7.
\end{thebibliography}
technologies and connected devices, and sensitive data involving children, health information, and financial data.\textsuperscript{159}

1. \textit{Data Transparency}

The focus on data transparency is consistent with the FTC’s concerns that stem from unlimited data collection without consumer knowledge or consent, risk of data breaches, and “risk that companies will make inferences about consumers that simply are not true.”\textsuperscript{160} The FTC intends to release a report on the data broker industry—including but not limited to, advertising networks, Internet service providers, operating systems, and social networks—for the primary purpose of increasing data broker industry transparency and awareness about its collection practices.\textsuperscript{161}

2. \textit{Mobile Technologies and Connected Devices}

Rich’s efforts to ease concerns about FTC intervention in this area seem to be nothing more than face-saving. Rich indicated that the FTC has already issued multiple reports on the lack of mobile privacy disclosures and the recommendations the Commission made to enhance security measures.\textsuperscript{162} With regard to enforcement, Rich mentioned the charges that the FTC brought against HTC America and Path, Inc. as clear examples of the FTC policing in the mobile ecosystem.\textsuperscript{163} Rich claimed that mobile initiatives are just the “tip of the technology iceberg” and that with consumers’ capability to “connect remotely to their refrigerators, bank accounts, thermostats,

\textsuperscript{159} \textit{Id.} at 9–12.

\textsuperscript{160} \textit{Id.} at 8. “Unless data brokers use consumer data for credit, employment, insurance, housing, or other similar purposes, there are no general laws requiring them to maintain the privacy of that data.” \textit{Id.} The Fair Credit Reporting Act imposes obligations on consumer reporting agencies. \textit{See generally} 15 U.S.C. §§ 1681–1681x (2012).

\textsuperscript{161} Rich, \textit{supra} note 156, at 8. In addition, Rich claimed that the FTC will continue to enforce the Fair Credit Reporting Act because it covers practices that are of the FTC’s greatest concerns. \textit{Id.}

\textsuperscript{162} \textit{Id.} at 10; \textit{see infra} Part VI.A–C of this article for details regarding these proposed recommendations.

\textsuperscript{163} Rich, \textit{supra} note 156, at 10.
[and] cars,” our world is simply getting more and more connected.\textsuperscript{164} Including an invitation for public comment as to where their focus should lie, the 2014 FTC agenda would involve development of yet another report to “summarize the findings and, where appropriate, set forth best practices for managing privacy and security with new interconnected devices.”\textsuperscript{165}

\section*{3. Sensitive Data Involving Children, Health Information, and Financial Data}

The FTC’s focus on sensitive data has previously been aimed at protecting children’s privacy.\textsuperscript{166} With keen attention still placed on children, the Commission has started to educate businesses and companies on the necessity of keeping health and financial information private as well.\textsuperscript{167} Rich claimed that the FTC has used and will continue to use “a variety of means such as webinars, a compliance hotline, the business center blog, and other business guidance,” to maintain the practice of holding businesses accountable for the impact their data-collecting has on consumers.\textsuperscript{168}

\section*{VI. The Plea for Reform}

Initially, the FTC was supportive of company self-regulation strategies, agreeing that companies are in a better position to protect their specific consumers from unwanted personal data distribution.\textsuperscript{169}

The FTC urged providers of on-line content and services to develop [and implement] policies,  

\begin{itemize}
\item \textsuperscript{164} Id. at 11.
\item \textsuperscript{165} Id.
\item \textsuperscript{166} 15 U.S.C. § 6501 (2012) defines the Children’s Online Privacy Protection Act, which was placed in effect in 1998 to strengthen children “privacy protections and give[] parents greater control over the personal information that websites and online services may collect from children under 13.” Rich, supra note 156, at 12.
\item \textsuperscript{167} Id.
\item \textsuperscript{168} Id.
practices and procedures for [consumer] personal data that . . . [met] the following key criteria: (1) provide notice to consumers as to the information being gathered and its uses; (2) offer consumers an opportunity to control how their information will be used; (3) provide consumers access to review and correct their data; and (4) develop security measures sufficient to protect the data from unauthorized use.  

However, despite these suggestions, the online industry did not adequately respond to privacy concerns, so in 2009, Congress began to consider implementing privacy legislation that granted the FTC oversight regulatory rights of broad online privacy matters. The dilemma now focuses on what “broad online privacy matters” actually means and encompasses.

A. **Smartphones Are Computers Too: A Suggestion for Proper Regulatory Oversight**

Although proposed in the context of computer networks and what the appropriate limits to comprehensive regulatory oversight should be, the discussion should remain directed at the original intended purpose of the oversight: personal data privacy protection. If the regulation is to be as comprehensive as intended, for such regulation of information privacy to be enacted, the “regulations should apply equally to data in all formats and all media.” If the smartphone is considered a miniature computer that is functionally equivalent to a device that computer-based networks target, then the smartphone should be subject to FTC initiatives to regulate privacy of data on these devices as well.

The unfortunate reality, however, seems to be a movement away from broad oversight of online regulations and a step backwards to revisit the online scheme. The FTC is backpedaling to recover from their failure to establish an effective online scheme and is now

---

170 Id.
171 Id. (citing Amy Schatz, *Lawmakers Blast Internet Data Collection*, WALL ST. J., June 19, 2009, at B3.).
172 Id.
173 Id.
attempting to narrow the framework to focus on which specific content forms of personal data should be subject to the FTC’s discretion on regulatory oversight.\footnote{Id. Particular concern arises in the context of consumer financial information, as well as in health and medical information. A growing number of software applications make it possible for smartphones “and other devices to collect and analyze personal health and medical information from consumers.” Id. These applications can provide valuable capabilities for consumers that allow them to more actively manage their health and medical histories; however, widespread use raises privacy concerns. “Currently, the HIPPA privacy protections do not directly apply to personal health data collected or processed using apps . . . .” Id.}

\section*{B. The Internet of Things}

The FTC uses the phrase the “Internet of Things” when referring to any Internet-enabled device.\footnote{Rich, supra note 156, at 11.} With the interconnection of technology and human, this reference to such devices goes far beyond the smartphone or tablet, and expands the meaning of a technology user to include consumers that have interest in such advancements in their vehicles and even household appliances. It can no longer be ignored that the high-tech market—what was once a foreign market—is becoming mainstream, and the digital privacy issues that come with technology are becoming mainstream as well.

Some weary consumers may argue that there is no need to impose immediate and restrictive regulations on the technologies that currently perforate the existing market. They may maintain that such regulations do not take into account the “trial-and-error” window that exists when other products are introduced in the market. The argument is that while new inventions may carry risks to consumer privacy, these risks and threats are mistakes that can be remedied once the invention or product is adequately established as part of the consumer demand. Is privacy regulation the new game of “which came first, the chicken or the egg?”

Consumers and the FTC arguably already participated in this confusing game with the introduction of the Internet. The Internet phenomenon revolutionized our world. With its introduction, we advanced to a new level of existence. Never before seen technologies were introduced, everything became faster, and the
human language gained new words, phrases, neologisms and expansions to its vocabulary. Businesses became more efficient and profitable, new jobs were created, people were able to view images, videos, and other information of places around the world they had only dreamt of, and ultimately, the world continued to want more. If exploration in advancing technology could produce something as fascinating as the World Wide Web, then what else could it do? Smart technology became more than a luxury—it became a necessity.

As people began quenching their curiosity thirsts, the excitement and freshness of the Internet was a distraction from danger. In the beginning, very few were concerned with the fact that instant information dissemination could be harmful. And when these new harms, such as hackers and social and business networking stalkers, proved that this exciting innovation had powers of evil, only then did we take a step back and think that something should have been done. Did we not learn our lesson? The demand for advanced new toys has once again left us to play a game for which the federal government refuses to provide rules. The FTC is the nation’s chief privacy agency and should start acting like it.

C. Not for Nothing: The FTC’s Efforts Toward Reform

In May 2012, the FTC hosted a workshop based on “enforcement and policy experience with mobile issues.” The workshop “brought together representatives from industry, trade associations, academia, and consumer privacy groups to explore privacy disclosures on mobile devices.” The FTC developed a report of suggestions for the major participants of the mobile ecosystem, highlighting what they believed should specifically apply to app developers, advertising networks and other third parties, as well as trade associations in partnership with academics, usability experts, and privacy researchers.178


177 Id.

178 Id.
I. The FTC’s Suggestions for Mobile Platforms

Mobile platforms will continue to be staples of our media culture and a driving force behind consumerism, and these suggestions only put a spotlight on the issues rather than establish anything concrete:

The [2012] report recommend[ed] that mobile platforms should:

[(1)] Provide just-in-time disclosures to consumers and obtain their affirmative express consent before allowing apps to access sensitive content [such as geographic location];
[(2)] Consider providing just-in-time disclosures and obtaining affirmative express consent for other content that consumers would find sensitive in many contexts, such as contacts, photos, calendar entries, or the recording of audio or video content;
[(3)] Consider developing a one-stop “dashboard” approach to allow consumers to review the types of content accessed by the apps they have downloaded;
[(4)] Consider developing icons to depict the transmission of user data;
[(5)] Promote app developer best practices. For example, platforms can require developers to make privacy disclosures, reasonably enforce these requirements, and educate app developers;
[(6)] Consider providing consumers with clear disclosures about the extent to which platforms review apps prior to making them available for download in the app stores and conduct compliance checks after the apps have been placed in the app stores; and
[(7)] Consider offering a Do Not Track (DNT) mechanism for smartphone users. A mobile DNT mechanism, which a majority of the Commission has endorsed, would allow consumers to choose to prevent tracking by ad networks or other third parties as they navigate among apps on their phones.\[179\]

\[179\] Id.
Considerations such as these create additional voids in the already inconsistent patchwork of requirements imposed upon businesses in the confusing combat on consumer privacy.

2. The FTC’s Suggestions for App Developers

Reasonable data security practices are merely an expectation of the FTC, and are professed as such. However, if expectations translated to reality in the way they were intended, then the enactment of laws and punishment for lack of obedience would have become obsolete years ago. The FTC report stated:

App developers should:
[(1)] Have a privacy policy and make sure it is easily accessible through the app stores;
[(2)] Provide just-in-time disclosures and obtain affirmative express consent before collecting and sharing sensitive information (to the extent the platforms have not already provided such disclosures and obtained such consent);
[(3)] Improve coordination and communication with ad networks and other third parties that provide services for apps, such as analytics companies, so the app developers can better understand the software they are using and, in turn, provide accurate disclosures to consumers. For example, app developers often integrate third-party code to facilitate advertising or analytics within an app with little understanding of what information the third party is collecting and how it is being used;
[(4)] Consider participating in self-regulatory programs, trade associations, and industry

---

organizations, which can provide guidance on how to make uniform, short-form privacy disclosures.181

If the FTC does not impose security and privacy as part of the job requirement for app developers, but rather as merely suggestions to employ, the motivation for reform is minimal among these players in the media culture, if it even exists at all.

3. **The FTC’s Suggestions for Advertising Networks and Other Third Parties**

The FTC decided that “[a]dvertising networks and other third parties should: [(1)] ‘[c]ommunicate with app developers so that the developers can provide truthful disclosures to consumers; [and (2)] [w]ork with platforms to ensure effective implementation of DNT mechanisms for mobile [devices].’”182

With respect to other influential players, the FTC indicated these professionals may: “[1] develop short form disclosures for app developers; [(2) p]romote standardized app developer privacy policies that will enable consumers to compare data practices across apps; [and (3) e]ducate app developers on privacy issues.”183

The FTC proffered that if the dominating players of the mobile ecosystem expeditiously worked to implement the suggestions of the report, then they would likely enhance consumer trust in the various mobile companies operating in this ecosystem.184 The FTC indicated that The National Telecommunications and Information Agency within the United States Department of Commerce was actively working with other stakeholders in the mobile technology industry to develop a code of conduct on mobile application transparency and that, “[t]o the extent that [such] strong privacy codes are developed, the FTC will view adherence to such codes favorably in connection with its law enforcement work.”185

---

181 See FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures: Recommendations Would Help Build Trust in the Mobile Marketplace, Agency Says, supra note 176.

182 Id.

183 Id.

184 Id.

185 Id.
VII. CONCLUSION

So, are you satisfied with the FTC’s suggestions? Do you feel as though your role as a consumer is valued and that the agencies in charge are putting their best efforts forward? Probably not, and it would be rather alarming if you were.

The FTC boasts its position as an agency that works for the consumer, to protect the consumer from big bad businesses. However, what the FTC has offered is just a suggestion. Many provisions of the 2012 report begin with the word “consider”—a word that carries no obligation or authority, and that merely postulates where the FTC thinks more attention should be paid.

If consumers have a fundamental right to privacy, as given to us by the founding fathers that established the very government system that justifies the existence of agencies such as the FTC, then why is the FTC merely “suggesting” that businesses, app developers, and third parties, etc., implement these safeguards in order to uphold that right? The FTC might as well have handed a twenty-dollar bill to a five-year-old and suggested that they consider going to the bank instead of the toy store.

Much like five-year-olds, or children in general, businesses need rules and guidelines in the form of concrete instruction. Businesses need regulations that are written policy and enforced as close to the strictness, if not possible to be established, as that of black letter law. As citizens, we are expected and required to abide by the laws of this country that were put in place to make sure that every individual’s fundamental rights are upheld. Where are the laws for businesses to abide by so that our fundamental right to privacy can be upheld?

The FTC is going to have to do more than make suggestions if it is to effectively meet consumers’ expectations and make consumers believe that the agency is as much an advocate on the consumer’s behalf as it is for the businesses consumers keep open.