Fall 2015 www.lawtechjournal.com Volume 19, Issue 2

UCLA Journal of Law & Technology

ATTACKING ANALOGIES: THE NEED FOR INDEPENDENT STANDARDS FOR MOBILE PRIVACY

Matthew Whitten

TABLE OF CONTENTS

Attacking Analogies: The Need for Independent Standards for Mobile Privacy

Matthew Whitten

I. INTRODUCTION

The impact of modern technology cannot be overstated; it has quickly impacted the lives of most Americans in a relatively short amount of time. In 2012, 78% of Americans reported owning a desktop or laptop computer.[1] In 2014, 64% of Americans stated that they owned a smartphone.[2] Of those surveyed, 44% of cell owners admitted to sleeping next to their phones so that they would not miss an important update during the night, and 29% confessed they could not imagine living without their phone.[3] Clearly, new technology has taken firm root in our society and influences the way we live our lives. While this adoption rate speaks to the power of technology, it does not tell the whole story. With the prevalence of these new technologies, however, have come new concerns about individual privacy and how these new developments affect these concerns. Privacy is implicated in ways that have not yet been addressed, even as computers and cellphones have become a routine part of everyday life. While both computers and smartphones are used for Internet access, the manner in which mobile technology interacts with the Internet is unique. Internet use on computers is commonly characterized by browsers and implicates privacy issues associated with the use of cookies. Mobile technology, in comparison, may concern location data privacy issues through the use of mobile applications.

[1] *Device Ownership Over Time*, PEW RESEARCH CENTER, http://www.pewinternet.org/data-trend/mobile/device-ownership (last visited Jan. 15, 2016).
[2] *Mobile Technology Fact Sheet*, PEW RESEARCH CENTER, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet (last visited Jan. 15, 2016).
[3] *Id.*

The manner in which the modern smartphone has become a microcosm of an individual, through text messages, calls, cameras, video recording, and geotagging, may lead to further privacy issues as well if this information is placed in the wrong hands.[4] One in five users turns off location tracking and one in three regularly clears their phone's search history – this evidences a growing concern of the average person to maintain control of privacy as the use of technology is further incorporated into everyday life.[5]

Given the relative infancy of mobile technology, there is not yet an effective system of handling the privacy concerns that arise from its use. Since mobile technology is only going to become more entrenched in our way of life, such a scheme is imperative. This paper will discuss one such potential system. Part II will examine how computer privacy, particularly cookie tracking, spyware, and cloud computing, has typically been viewed and handled. Part III will discuss how location-based data, mobile applications, and the extensive integration of cell phones in modern life implicate longstanding privacy interests. Lastly, Part IV proposes that any shortcomings or disputes with regard to mobile privacy should be resolved with respect to its own body of law, as opposed to analogies to other, distinct technologies, as the area of mobile privacy has previously been handled. This new proposed body of law takes the form of legislation implicating mobile application controls, privacy policy and "Do Not Track" protection changes, and securing phone data.

[4] John B. Kennedy & Annie C. Bai, *Reining In Mobile App Privacy Practices*, LAW 360 (Jan. 25, 2013, 12:23 PM), http://www.law360.com/articles/407974/reining-in-mobile-app-privacy-practices.
[5] *See Mobile Technology Fact Sheet*, *supra* note 2.

II. NEW PRIVACY INTERESTS IMPLICATED BY COMPUTERS

Computer technology and its usage has created significant and important privacy issues. Just as computers were the forerunners to modern mobile technology, the way privacy is handled with computers can serve as a precursor to privacy interests concerning mobile technology.

A. Tracking Private User Behavior via Cookies

The privacy concerns connected with the mass use of computers are numerous and growing. Most readily evident are concerns surrounding the use of cookies to track user movement across the Internet. A cookie is a piece of data that a website associates with a user when they visit a particular website at a particular moment.[6] For example, cookies can store identification information and/or a password so that a subsequent visit to that site is made easier through the streamlining of the login process.[7] While this function clearly has the benefit of making it easier for a user to access a site without having to reenter their credentials, it comes at the price of privacy. Third-party cookies, cookies used by a website other than the one that is currently being visited, may be used to track the user once they have left the initial site and allow the company controlling the cookie to monitor the viewing habits of the user while they continue to browse the Internet.[8] While this alone is already problematic, the real threat to privacy emerges when the data collected by tracking a user across the Internet is aggregated to create a profile of the user.[9] This can enable the third party collecting the user's data to catalogue a variety of information, such as medical conditions and political affiliation or leanings through the information that is viewed by a user.[10] This profile might be used to target the user in negative

[6] *Cookie*, TECHTERMS.COM, http://www.techterms.com/definition/cookie (last updated July 9, 2011).
[7] *Id.*
[8] Chris J. Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 276 (2012), *available at* http://ssrn.com/abstract=2137601.
[9] *Id.*
[10] *Id.*

ways, such as damaging reputations based on the obtained data[11] or losing an important career or educational opportunity, rather than to help facilitate an easier online experience for the user.[12]

This practice of tracking Internet users through cookies, coupled with a general desire by the average person to remain anonymous online,[13] has led to the development of "Do Not Track" settings on browsers. This setting allows users to "opt out" of tracking, for any purpose, by sending an HTTP header, a type of data, to the website that indicates the user is requesting not to be tracked.[14] While this sounds like a perfect solution to those worried about having their Internet activities tracked as they hop from site to site, it remains largely a theoretical solution. Although some entities may accept a user's "Do Not Track" request,[15] more often than not, the request is ignored.[16] This is especially disquieting since 41% of people surveyed acknowledged that they had set up their browser to disable accepting or turning off receipt of cookies.[17] Additionally, a fair number of Internet users are unaware of their ability to opt-out of such tracking, and consequently do not enable the sending of such requests through their web browsers.[18] This lack of knowledge of the available privacy shield thwarts the effectiveness it otherwise might have. Thus, it is easy to see how there is a gap between the desire of a user to be able to use their browser to peruse the Internet while retaining control of information about their

[11] Lee Rainie, Sara Kiesler, Ruogu Kang & Mary Madden, *Anonymity, Privacy, and Security Online*, PEW RESEARCH CENTER (Sept. 5, 2013), http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.
[12] *Id.*
[13] Lee Rainie, Sara Kiesler, Ruogu Kang & Mary Madden, *Part 1: The Quest for Anonymity Online*, PEW RESEARCH CENTER (Sept. 5, 2013), http://www.pewinternet.org/2013/09/05/part-1-the-quest-for-anonymity-online/.
[14] *Do Not Track: Universal Web Tracking Opt Out*, donottrack.us (last visited Jan. 21, 2016).
[15] For a list of companies who have made public statements about their acceptance of user-produced "Do Not Track" requests, see *Do Not Track: Implementations*, donottrack.us/implementations (last visited Jan. 21, 2016).
[16] *See Do Not Track*, *supra* note 14.
[17] *See* Rainie, *supra* note 13.
[18] Curt Hessler, *The Wars of Digital Prosperity* 64 (2014) (unpublished article).

internet usage, and the ability to use available technologies to enable them to meet these wishes by protecting what information is obtained by third parties through the use of browser settings.

B. Privacy Threats Posed by Spyware

Another concern when discussing Internet privacy as it relates to computers is the threat of spyware. Spyware refers to a class of programs that infiltrate a user's computer and covertly send information back to the creator of the software.[19] The method of infiltration used by spyware varies; spyware can infiltrate through an infected email attachment or by piggybacking on the code of an installation package for software the user chooses to download.[20] There are also many avenues of distribution that make use of a browser itself a prime candidate for the delivery of spyware, including the use of ActiveX in Microsoft's Internet Explorer.[21] To make matters worse, spyware can be difficult to remove once it has infiltrated a computer system. While a normal program might be removed using the operating system's uninstallation feature, or through a customized uninstaller tailored to that program, spyware usually does not include such convenient removal tools.[22] For instance, spyware may diffuse itself throughout a targeted computer so that it is cumbersome to uninstall, or may disguise itself with the name of a legitimate piece of software so a user will be disinclined to attempt to get rid of it.[23]

Side effects that may accompany spyware and which may affect an infected user's computer even if the spyware is removed include performance degradation and loss of the ability to access the Internet.[24] Beyond these performance-oriented side effects, however, are the

---

[19] *Spyware*, TECHTERMS.COM, http://www.techterms.com/definition/spyware. The definition for spyware is not universally accepted. For purposes of this essay, I will adhere to the definition found on TechTerms.com.
[20] *Id.*
[21] Fed. Trade Comm'n, *Monitoring Spyware on Your PC: Spyware, Adware, and Other Software* (Mar. 2005), at 6, *available at* http://www.ftc.gov/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-other-software [hereinafter Fed. Trade Comm'n, *Monitoring Spyware*].
[22] *Id.* at 7.
[23] *Id.*
[24] *Id.* at 8.

privacy interests of the user that are implicated when a computer becomes the nesting ground for spyware. As reported by panelists at a Federal Trade Commission ("FTC") workshop, "keystroke logging" is a primary threat associated with spyware. This type of program, also referred to as a "keylogger," acts by collecting all keystroke information that a user types on his or her computer, regardless of where the information is typed into.[25] This can reveal valuable information, including: passwords, telephone numbers and physical addresses, and other information commonly used in online forms, financial information, and the contents of emails or other communications.[26] These privacy interests closely parallel those mentioned in the above discussion of third-party cookies and also reflect concerns similar to those of browser users.

While there has been little progress, if any, in the battle over third-party cookie usage, the reaction to spyware has been more effective in thwarting privacy leaks. For instance, the emergence of browsers not bundled into the operating system, a rapid growth in the number of available anti-spyware programs, and changes at the operating system level have all occurred since the wide dissemination of spyware began. While there has yet to be a conclusive study as to the effectiveness of these protections, it is significant that potential solutions exist and are growing quickly to help combat this hazard.[27]

One potential solution may be to implement a comprehensive system which would identify permissions when a program requests installation that the user could then accept or reject.[28] Such a scheme would ostensibly allow the user more control of the programs they choose to download onto their computer and would prompt the user to reject programs that either

[25] *Keylogger*, TECHTERMS.COM, http://techterms.com/definition/keylogger (last visited February 1, 2016).
[26] *See* Fed. Trade Comm'n, *Monitoring Spyware*, *supra* note 21, at 10.
[27] *Id.* at 14-17.
[28] *Id.* at 16.

did not conform to the labeling system or that requested permission beyond what the user was comfortable giving.[29]

Another potential solution could arise from forcing the inclusion of a more thorough and regulated End User Licensing Agreement ("EULA") for spyware.[30] One advantage of such an agreement is that the average user would be presented with an explanation of what data the user is being relinquished, and how that data might be used.[31] This would help to curb programs "which operate by installing spyware applications that are invisible to the user" since the user would be made aware of the "vast amount of data that it mines from their personal systems," making installation a much less appealing option.[32] While those in the spyware business are likely to vehemently resist this proposal, such a structure would greatly benefit users by giving them the ability "to make an informed choice" about their software decisions.[33]

A final potential solution might be to implement a "sandbox" for each software program at the operating system level.[34] This "sandbox" would utilize separate, individual compartments for each piece of a program running on a computer, and would allow users individualized control over what that software can and cannot do.[35] This would limit the potential sweep of the software's reach, and curb the extent to which it may collect and disseminate a user's private information.[36]

---

[29] *Id.*
[30] Daniel B. Garrie, *Introduction*: *Creating Legitimate Digital Privacy Rights for Internet Users*, 3 RUTGERS J.L. & PUB. POL'Y 149, 150 (2006).
[31] *Id.*
[32] *Id.* at 151.
[33] *Id.* at 153.
[34] *See* Fed. Trade Comm'n, *Monitoring Spyware*, *supra* at note 21, at 16.
[35] *Id.*
[36] For an explanation on how this process works in the similar context of other malware, *see* Eric Geier, *How to Keep Your PC Safe With Sandboxing*, PCWORLD (Jan. 16, 2012 6:00 PM), http://www.pcworld.com/article/247416/how_to_keep_your_pc_safe_with_sandboxing.html.

While spyware is a considerable threat to the privacy of an Internet user, these three prospective solutions show that there are multiple options available that could be implemented to help limit or eradicate the privacy risks presented by this concealed danger.

C. Traditional Privacy Issues Implicated through Cloud Computing

Cloud computing represents the synchronization of widespread computer use in daily life through the utilization of the Internet. The exact definition of the "cloud" is nebulous, but can best be understood as "on-demand network access to a shared pool of configurable computing resources" controlled by the end user.[37] The widespread adoption of cloud technology has seemingly already taken place, with almost 70% of Internet users already using webmail, online data storage or software located solely online."[38] Among the most common uses of cloud computing are webmail and file storage; this keeps information synchronized across multiple platforms on a company's personal servers.[39] While the business model of cloud services varies between companies, the general trend is that free cloud services result in user information being exploited for advertising purposes.[40] The ability of a given cloud service provider to utilize user-supplied data, either to sell to other advertising companies or to use the data in order to create a profile of the user for direct advertisements, will depend greatly on data retention policies.

In addition to concerns over privacy relating to advertising practices, there is good reason to be concerned over the general security of the data provided to cloud services. Companies have been known to leave vulnerable user data unencrypted despite the fact that encryption makes that

---

[37] Peter Mell & Tim Grance, *The NIST Definition of Cloud Computing*, NAT'L INST. OF STANDARDS & TECH., (Sept. 2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
[38] Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 356-357 (2013).
[39] *Id.* at 358-59.
[40] *Id.* at 359-60. While some of this concern will overlap with the above-discussed concerns with respect to third-party cookies, cloud computing presents its own unique ecosystem of the use of data.

data more difficult to use by a would-be abuser.[41] Encrypting user data is more desirable from a privacy standpoint, since the data would be more difficult to use if accessed through fraudulent means. Despite these advantages, a lack of user demand and the high cost of implementation has kept cloud service providers from widespread adoption of user data encryption. Businesses instead opt to utilize extra resources to ensure up-time (availability to the end user) of its service to "at least 99.9% of the time."[42]

Presently, the legal framework on which cloud services and its interaction with consumer privacy is built is meagre. While there is some regulation to protect privacy with respect to financial institutions, credit reporting agencies, and healthcare data,[43] the vast majority of cloud computing remains a free-for-all with respect to user privacy. The current regulations for cloud computing, when adopted, generally operate as an "opt-in" policy, which requires user consent to be given before any use of the information may occur.[44] Conversely, many non-regulated businesses only offer the ability to "opt-out" of sending their information to a third-party business.[45]

There is some relief available at the state level to those who believe their data has been used in a harmful way. This relief is typically sought through tort law. Although this area of law has not fully matured, its prevalence as a means of relief is rising.[46]At the federal level, the FTC Act provides relief for a consumer whose information was inadequately protected and made

---

[41] *Id.* at 360.
[42] *Id. See* Konstantinos K. Stylianou, *An Evolutionary Study of Cloud Computing Services Privacy Terms*, 27 J. MARSHALL J. COMPUTER & INFO. L. 593, 606-607 (2010).
[43]Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413, 443-444 (2013).
[44] *Id.* at 444.
[45] *Id.*
[46] *Id.* at 446-48. See *id.* at 447, n.139 for a discussion of the court's decision to not dismiss claims arising from the RockYou data breach, in contrast with other courts that have required actual damages to result before a claim can be sustained; King and Raja also note that privacy lawsuits sounding in federal claims generally have a greater probability of succeeding.

vulnerable to outside access and also allows for a consumer to sue when a company engages in deceptive practices with regard to the security of user-supplied data.[47] An example of this would be a company stating in its privacy policy that it would store user data securely, while in reality, failing to implement sufficient security measures.[48] The lack of formal guidelines has led to cloud service providers relying mainly on industry standards and self-regulation, often resulting in low thresholds for the security of user-generated data.[49] Regulation surrounding cloud computing may grow stronger as time progresses, but—for now—cloud-based privacy regulation must make do with the aforementioned tort applications, limited legislation, and self-policing by cloud service providers.

III. CELLPHONES AND MOBILE TECHNOLOGY ENCOMPASS A WIDER ARRAY OF PRIVACY INTERESTS THAN TRADITIONAL COMPUTERS

The recent advent of mobile internet technology—epitomized by the smartphone—has created a unique set of privacy concerns that both overlap with and are distinct from those involved with traditional computers. Far from being a device used for simply making phone calls, these phones comprise a panoply of gadgets, including a camera, video recorder, text message sender, a miniature computer with full Internet access, a media player, and a GPS, all rolled into one compact package.[50] While this integration of devices indisputably provides great convenience for the user, it also complicates the issues that arise from usage of the device.

[47] *Id.* at 448.
[48] *Id.* at 426 n.47.
[49] *Id.* at 449.
[50] Anne T. McKenna, *Pass Parallel Privacy Standards or Privacy Perishes*, 65 RUTGERS L. REV. 1041, 1058 (2013).

A. Location Tracking Raises Concerns in Mobile Technology, but not in Traditional Computers

Location-based services that use both cell tower triangulation and global position systems (GPS) are a popular feature available on smartphones.[51] In one survey, nearly three-quarters of respondents stated that they use their smartphones for both gathering information about their current surroundings and finding directions from their current location, either through automatic detection or manual input, to another destination.[52] This location data is used by pre-installed or user-downloaded mobile applications on the phone, and can be collected and retained by the maker of the application without the users' consent or knowledge.[53] Concerned with unintentionally giving these application makers access to this information, 19% of surveyed cell phone users disable the location tracking abilities of their phones.[54] This speaks to cellphone users' awareness of the privacy tradeoffs created by the convenience gained by having more capabilities packed into one singular device. While the ability for a user to take advantage of location services is a great upside, these same services create geolocation data that application owners often collect for their own uses.[55] These owners can use this data for their own purposes, or sell it to a third party for personalized advertising.[56] While there may be upsides to having applications able to utilize this information, such as location-based recommendations,[57] these apps may not always have the purest of intentions, such as distorting location-based results with advertisements. In a 2012 report, the FTC revealed the shocking practice of silent data collecting

[51] *Id. See id.* at 1058-59 for a cursory technical explanation of the triangulation process.
[52] *See Mobile Technology Fact Sheet*, *supra* note 2.
[53] *See* McKenna, *supra* note 50, at 1059.
[54] Jan Lauren Boyles, Aaron Smith & Mary Madden, *Privacy and Data Management on Mobile Devices*, PEW RESEARCH CENTER, http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices.
[55] See McKenna, *supra* note 50, at 1063.
[56] *Id.*
[57] *Id.* (using the example of built-in GPS technology to locate the nearest Starbucks to the cell phone user's current location).

by mobile applications targeted primarily toward children. These applications gathered not only the location data of young users, but more general information gained through the use of other tracking mechanisms, such as third-party cookies.[58] This sharing of location data happened in one instance within moments of opening the app each time, giving third parties immediate knowledge of the user's whereabouts.[59] This is especially worrisome when the users of these mobile applications are children, since they are not sophisticated enough to know about the information being collected.

In response to the concerns about privacy violations associated with the misuse of location-based data, there have been attempts to fix this problem. The Wireless Association (formerly known as the Cellular Telephone Industries Association, or CTIA) has adopted Best Practices guidelines concerning both cellular service providers and mobile application developers.[60] The purpose of these guidelines is to ensure that users have "meaningful notice about how location information will be used" and that users "consent to the use or disclosure of location information."[61] These are obviously important considerations that would allow the people creating the location information more control over its dissemination. If implemented, these proposals would be a much needed step in the right direction toward how location data should be handled.

The Best Practices additionally call for periodic reminders to users that their location data may be shared and how this sharing would occur.[62] These guidelines would also place a burden on the data-gathering entities to show that consent of the user was received, if an issue were to be

---

[58] *Id.* at 1064 (discussing *Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing*, FEDERAL TRADE COMMISSION (Feb. 16, 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf at 1).
[59] *See Mobile Apps for Kids*, *supra* note 58, at 13 n.27.
[60] CTIA The Wireless Ass'n, Best Practices and Guidelines for Location-Based Services, CTIA (Mar. 23, 2010), http://www.ctia.org/docs/default-source/default-document-library/pdf-version.pdf?sfvrsn=0 at 1-2.
[61] *Id.* at 1.
[62] *Id.* at 4.

raised. The form of such consent would change depending on the situation of the services.[63] However, these Best Practices also allow for a user to revoke consent given to collect his or her data, both in whole and in part.[64] Furthermore, the guidelines provide for the retention of user-generated data "only as long as business needs require," after which it must be expunged.[65] Through the user consent requirement and limited storage of information, along with the other practices suggested by the guidelines, the CTIA puts forward a solid foundation for how users should expect their location data to be treated and utilized.

A major issue with these Best Practices, however, is that compliance is largely evaluated through self-certification.[66] Because of this, there is no indication of how many companies adhere to these proposed guidelines, since they are not required for either service providers or mobile application creators.[67] Additionally, the guidelines also suffer from lack of a concrete standard for how end-users should be notified of data collection.[68] While there have also been some proposed bills that seek to correct the inadequacies of protecting location-based data,[69] none have yet accomplished the task since they have not been enacted into law. A more complete legislative or industrial approach will likely be necessary to better control how location-based data is collected and utilized.

---

[63] *Id.* at 5.
[64] *Id.* at 6.
[65] *Id.* at 7.
[66] *Id.* at 8.
[67] Daniel L. Pieringer, *Recent Development: There's No App for That: Protecting Users from Mobile Service Providers and Developers of Location-Based Applications*, 2012 U. ILL. J.L. TECH. & POL'Y 559, 567 (2012).
[68] *Id.* at 573.
[69] *See* Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011) (calling for those retaining locational data to implement certain security measures to protect the data and give more complete notice of how collected data would be used); Location Privacy Protection Act of 2011, S. 1223, 112th Cong. (2011) (requiring providers of location-based services to obtain "express authorization" to collect and use the data).

B. Important Privacy Considerations Involving Mobile Applications

One of the biggest draws to modern smartphones has been the emergence and proliferation of mobile applications. Last year, there were 1.5 million apps offered for download with 1,600 new apps being pumped out each day.[70] A recent study found that mobile users now use 86% of their mobile application usage to access the Internet, averaging 2 hours and 19 minutes per day.[71] According to the same study, 32% of this application use is centered on gaming, 28% on social media, 18% on news and other productivity functions, and 8% on entertainment.[72] This speaks to the pervasiveness of mobile applications as they continue to gain prominence in the lives of mobile technology users. While this explosion undoubtedly gives these users a host of new features to use, and new information to consume, it is not without its issues, as the makers of these applications are provided with extensive access to user information that they can easily exploit for profit.

An especially egregious example of how this personal data has already been compromised can be seen in a recent proposed consent order drafted by the FTC against the maker of the Android application "Brightest Flashlight Free" in December of 2013. This application, supposedly a simple flashlight app, sent device identification information and precise location data to third parties, including advertising services, without consent of its users.[73] The application additionally presented the user with an option to cease the transmission of the information, but would continue sending it regardless of the choice made.[74] The FTC's

[70] *See* Kennedy, *supra* note 4, at 1.
[71] Simon Khalaf, *Apps Solidify Leadership Six Years into the Mobile Revolution*, FLURRY INSIGHTS BLOG (Apr. 1, 2014), http://www.flurry.com/bid/109749/Apps-Solidify-Leadership-Six-Years-into-the-Mobile-Revolution.
[72] *Id.*
[73] *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers*, FEDERAL TRADE COMMISSION (Dec. 5, 2013), http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.
[74] *Id.*

consent agreement required the application maker to: (1) inform consumers of what data would be collected and how it would be used and shared; (2) obtain affirmative consent from users in order to collect and share data in the future; and (3) delete any information obtained through its previous bad practices.[75] While this behavior may not be representative of how every mobile application functions, it clearly demonstrates the real concerns that exist for users with respect to their private data.[76]

The breadth of data at risk by the mass usage of mobile applications is not limited to that which is taken deceitfully. It is becoming commonplace to use applications on mobile devices to pay for purchases, complicating the privacy issue by including sensitive financial information. Additionally, with the rise of electronic medical records, users now transmit private health information to and from health care providers through their mobile devices.[77] These are examples of information that end-users have a great interest in protecting and limiting access to. By entering this information into mobile applications, these users place great trust in the entities who develop and monitor activity within the application.

Sadly, the protection of this information has not always risen to the requisite level; Credit Karma, a company which aids customers in monitoring their credit scores, was recently subject to an FTC investigation for failing to implement appropriate measures to secure the user data it had gathered through its mobile application.[78] Specifically, Credit Karma's application bypassed

[75] *Id.*
[76] On this same theme, while other applications that commit especially atrocious acts of consumer deception and misuse of private data exist, it is highly unlikely that each and every mobile application will become subject to an FTC investigation and eventual consent decree regulating how its developer will have to act.
[77] Kathy Ossian, *Legal Risks of Mobile Apps: Rules, Standards, and Gaps*, LAW360 (June 11, 2014, 6:42 PM), http://www.law360.com/articles/546611/legal-risks-of-mobile-apps-rules-standards-and-gaps.
[78] *Fandango, Credit Karma Settle FTC Charges*, FEDERAL TRADE COMMISSION (Mar. 28, 2014), http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers.

default validation processes, exposing user data to possible interception and theft.[79] Unlike the makers of "Brightest Flashlight Free," who deceitfully took steps to provide third parties with access to user information, Credit Karma acted wrongly by omission. This company, undoubtedly not alone in its failure, hurt its customers by failing to provide them with adequate data protections, despite having access to tools for both iOS and Android that would have easily enabled it to provide said security.

Similar to the above discussion about location-based services, there have been pushes for industry regulation in regards to data privacy. A 2013 proposal by the Digital Advertising Alliance (DAA) appealed to app makers for increased transparency in how location and personal data are handled and stored.[80] Particularly for personal data, the DAA suggests obtaining user authorization before such information is accessed by either the entity itself or any third-party entity.[81] The fatal flaws of this proposal are similar to those presented in the previous section; these regulations are not mandatory and rely too heavily on self-regulation. While some state legislatures have tried to step in to fill this regulatory void by providing statutory protection for user data, such as the California Online Privacy Protection Act,[82] these steps have not resolved the issues left by the lack of consistent, mandatory industry standards.

C. Privacy of Data Retained on Mobile Devices is treated as a Mixture of Old and New Privacy Rules

Cell phones and tablets have become one-stop shops for all modern technological needs. Whether it is traditional voice calling, sending text messages, or browsing the Internet, mobile

---

[79] *Id.*
[80] Digital Adver. Alliance, *Application of Self-Regulatory Principles to the Mobile Environment*, DIGITAL ADVERTISING ALLIANCE (July 2013), https://www.aboutads.info/DAA_Mobile_Guidance.pdf.
[81] *Id.* at 30.
[82] This act covers any online service, inclusive of mobile applications, used by a California resident, requiring disclosure of polices relating to the collection of personal information; *see California Online Privacy Protection Act (CalOPPA)*, CONSUMER FEDERATION OF CALIFORNIA EDUCATION FOUNDATION (July 29, 2015), http://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3.

technology now makes use of, and generates, a monumental amount of personal information that users want to keep private. In fact, 78% of mobile technology users regard the information kept on their phones and tablets at least as private as comparable data stored on their traditional computers.[83] Similar to the other privacy issues addressed above, there is no overarching privacy law governing an individual's information or data.[84] At best, the FTC is able to regulate some privacy through consumer protection; however, the FTC is still limited in its authority over even this small area of concern.[85] Outside of the realm of consumer protection, the privacy of data on mobile technology is largely protected on a case-by-case basis. For example, with respect to text messages sent in a work environment, the general rule is that an employee has no reasonable expectation of privacy in such communications,[86] but a decision in the Ninth Circuit held that in particular circumstances, an employee using an employer-provided device has a reasonable expectation of privacy under the Fourth Amendment.[87]

The Fourth Amendment expectation of privacy is not static; it continues to change and adapt to the advent of new technologies.[88] How sensitive data contained within cell phones is handled, with much debate, is best illustrated in the search and seizure of cell phones. Sensitive cell phone data has been hotly contested in terms of search and seizure of cell phones. The Supreme Court has noted the importance of cell phones and its functionalities, but has admitted

[83] *See* Kennedy, *supra* note 4.
[84] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014).
[85] *See* Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217, 1225 (2013).
[86] Amanda J. Lavis, Note, *Employers Cannot Get the Message: Text Messaging and Employee Privacy*, 54 VILL. L. REV. 513, 517 (2009).
[87] Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008).
[88] 5 DAVID BENDER, COMPUTER LAW: A GUIDE TO CYBERLAW AND DATA PRIVACY LAW, § 21.02 (Matthew Bender, Rev. Ed. 1997).

that the expectation of privacy in that data was not clear-cut.[89] In *People v. Diaz*,[90] which concerned a search pertaining to text messages on a cell phone that was carried by a person at the time of his arrest, the court found that, since the cell phone was "personal property…immediately associated with" the arrestee, a search of its contents incident to arrest was valid.[91] The Court followed existing case law in holding that the nature of the thing to be searched did not affect how a warrantless search would proceed, citing the fact that the record contained no facts that explained why *all* phones, "including those with limited storage capacity," should be exempt as a class from search and seizure rules.[92]

In her dissent, Justice Werdegar recognized that the potential cache of information stored in a cellphone made it unique among personal property that might be on a person at arrest, distinguishing cellphones from pagers and address books.[93] This line of reasoning can also be found in *State v. Smith,*[94], cited by Justice Werdegar, dealing once more with the search of a cell phone incident to arrest. The court ruled that a warrantless search of a cell phone – either with or without "smart" capabilities -- incident to an arrest was improper due to the large amount of stored personal information.[95] This holding casts doubt on the view of cell phones advanced in *Diaz*.

Most recently, the Supreme Court considered the treatment of cell phone data in *Riley v. California.*[96] This case also concerned the search of a seized cell phone incident to an arrest. The intermediate state appellate court relied on *Diaz* to find the search reasonable.[97] The Supreme

[89] *See id.* § 21.03 (discussing City of Ontario v. Quon, 560 U.S. 746 (2010)).
[90] People v. Diaz, 51 Cal. 4th 84 (2011).
[91] *Id.* at 93.
[92] *Id.* at 97.
[93] *Id.* at 104 (Werdegar, J., dissenting).
[94] State v. Smith, 124 Ohio St. 3d 163 (2009).
[95] *Id.* at 170-171.
[96] Riley v. California, 134 S. Ct. 2473 (2014).
[97] *Id.* at 2481.

Court, however, disagreed with the application of existing jurisprudence to the realm of digital data, and held that a warrant was required in order to search a cell phone seized incident to arrest. The Court reasoned that the prior rationales did not meet the realities of the actual technology. In examining the risks of harm to officers and destruction of evidence, the *Riley* Court determined that the digital data contained on cell phones did not implicate the same concerns of traditional, tangible property.[98] The Court discussed how the data on a cell phone could not potentially harm an officer and there was no "unknown" item at issue.[99] With respect to the destruction of evidence, the Court observed that once the phone was taken by the police, the arrestee was incapable of erasing the data on it.[100] In arriving at their ultimate determination that a cell phone seized incident to arrest requires a warrant before being searched, the Court noted that contemporary cell phones "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[101] The Court recognized that the novel technology manifested in cell phones required a redrawing of the lines to better support the changing playing field.[102] Thus, there has been an evolution of how cell phones are seen and treated in recognition of their preeminence in modern life.

IV. PROPOSED SOLUTIONS FOR MOBILE TECHNOLOGY PRIVACY

Having discussed some of the traditional treatments of privacy rights as they pertain to computers and smartphones, and the unique privacy issues being faced in light of the recent

[98] *Id.* at 2484-85.
[99] *Id.* at 2485.
[100] *Id.* at 2486.
[101] *Id.* at 2488-89.
[102] In his concurring opinion, Justice Alito suggested that it may be preferable that courts not be the ones who determine how cell phones should be treated but rather that "legislatures, elected by the people, are in a better position…to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future." *Id.* at 2497-98 (Alito, J., concurring).

emergence of such technology, a modest proposal can be put forth to address these challenges. This proposal will contain provisions for control and congressional action with respect to mobile application permissions, privacy policies, Do Not Track requests, and the security of sensitive data stored on mobile devices.

A. User Control of Application Permissions

As discussed above, mobile applications have become a staple of smartphones. However, they are a double-edge sword, since they can also expose a user's private information as easily as they can provide convenience. To that end, it would be beneficial for the end-user to be able to take more control of the applications on their phones.[103] This could be achieved by using the underlying structure of the operating system already installed on the phone. For example, on the Android operating system, there are built-in permission-based security measures that protect "sensitive information…and sensitive device functionality."[104] This security measure functions in a two-step process. First, a third-party application (one not pre-installed by the manufacturer of the operating system) must state that it will access sensitive information or functions such as GPS data. Second, when a user goes to download the application to his or her phone, the user is provided notice any sensitive areas of the phone the application requires for its use.[105] At this point, the user makes his or her own determination of whether the application should have access to the requested information or function. If the user does not want the application to have the requested permission, the application will not be not installed.

---

[103] While I will mainly discuss applications relating to cell phones, the two dominant operating systems, Android and iOS, function equivalently on a tablet environment and therefore can be covered under the same suggested action.

[104] *See* HTC Am. Inc., FTC File No. 122 3049, No. C-4406, at 1 (F.T.C. July 2, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf [hereinafter HTC Consent Order] (complaint).

[105] *See id.* at 2.

Although this seems to give the user control over which applications have access to private information stored on the mobile device, the reality is not so simple. The Original Equipment Manufacturer (OEM) has control over what software comes preinstalled on its phones, even if the phone is running an operating system produced by another company.[106] This software can undercut the security features of the operating system through "permission re-delegation vulnerabilities."[107] The re-delegation vulnerabilities allows an application that has been granted access to the sensitive areas at issue to extend that permission to another application that has not been expressly given that same level of authorization.[108] Thus, even within the operating system, there are ways in which applications can gain covert access to private information.

On the iOS operating system (hereinafter "iOS") as well, there is a system by which applications gain access to private data with explicit approval from the user. When an app is initially installed, there is no authorization for access to sensitive data or settings of the phone.[109] Instead, when an app is opened for the first time and such access is needed, the app presents a pop-up to the user with a request for consent.[110] This pop-up gives users more control over what sensitive data to release to an application, and it allows the user to decide whether the application can be trusted before doing so. For example, the user can deny permission and the application will continue to function, or the user can pick and choose which permissions are granted to a

[106] *See* HTC Consent Order, *supra* note 104. For example: HTC, a Taiwanese electronics company, manufactures various Android smartphones. The Android operating system is made by Google, who also includes some of its proprietary applications as part of its certification of handsets. Once HTC receives this code for use on its hardware, it can then add its own applications to the handset before it is shipped out to the consumer; *Id.*
[107] *See* HTC Consent Order, *supra* note 104.
[108] *Id.*
[109]Chris Hoffman, *iOS Has App Permissions, Too: And They're Arguably Better Than Android's*, HOW-TO GEEK (December 15, 2013), http://www.howtogeek.com/177711/ios-has-app-permissions-too-and-theyre-arguably-better-than-androids/.
[110] *Id.*

given application.[111] The user can also enter the privacy menu of iOS and manually select which permissions each application can access at any time.[112]

There are clear advantages and disadvantages of each system's approach to permission requests. While Android provides the user with more information upfront about what potential interactions will occur, iOS gives the user more granular control once the application is installed and specific functionality is required. While giving users more control over their applications is something that is understandably good, making it too cumbersome to process and sort through permissions defeats this purpose. Given concerns about mobile applications surreptitiously accessing sensitive data and utilizing legitimate access for unintended purposes, a combination of the Android and iOS approaches to application control would be the optimal solution. This could be accomplished by a federal statute for national uniformity, which would provide that particular criteria are met for all mobile applications released on the open market.[113]

One hypothetical example of control would begin when the user selects to download an application. The user would be presented with a pop-up dialogue, similar to the one used in Androids, that informs the user of the permissions requested for access in order for the application to function. Departing from the Android model, this notification would not require the use to grant or reject the permission at this point, but rather serve to provide the user with

[111] *Id.*
[112] *Id.*
[113] Over time there have been a few third-party marketplaces for the downloading and installation of mobile applications, some of which have thrived and some that have fallen due to malicious content. While it would be ideal to regulate all applications that a user could potentially have access to, regulating the official markets—the Google Play Store and Apple App Store, for instance—would have the greatest effect on giving users the benefit of these refined controls.

information.[114] The application would then be installed without providing any access to sensitive information or controls.

Upon using the application, when a sensitive permission is necessary to enable a functionality, the application would produce a new pop-up notification, which would provide two important pieces of information: (1) the specific permission being requested (e.g. access to locational data through the GPS or accessing the information of contacts kept within the data storage of the phone); and, (2) equally as important, the reason that it will be accessed. This would only appear for the first use of the individual permission. The initial choice of acceptance or denial would be remembered by the operating system and treated as the default for that application's use of that specific permission. If a user changes his or her mind after granting or denying a specific permission request, the application allow users to change permission status.[115] This would give users the necessary control over their private data without obstructing use of an application by excessive permission decisions.

However, there are a few downsides to this approach. First, users might "break" applications by denying them, either purposefully or inadvertently, the access to phone capabilities necessary to carry out the function the app was made for. This would not only lead to a loss of utility from the application, but could also lead the user to become hostile toward the developer of the application if the app does not work as advertised. A developer could alleviate these problems by explaining on the download screen that denying the requested permissions will cause malfunction. Second, if users are given the ability to selectively deny permissions to

[114] While this is not the end of the proposed solution of how application permissions are handled, it is my belief that this step is, in and of itself, a great advance toward securing the privacy of the end-user because they will be more informed of what they are faced with while not having to decide then and there to grant the necessary permissions.
[115] Ideally, the app feature allowing for changes to permission status would be contained in an in-application menu accessible by an overflow option. While the menu would hide when not in use to avoid application clutter, it would remain available without having to exit the application and access a centralized or system-wide settings menu.

applications, developers might limit the functionality of their applications so that a user would be forced to grant access to particular data in order for the application to work properly.[116].

Additionally, the applications might not be able to collect the information that advertising relies upon, causing the developer to lose a revenue stream and dis-incentivizing application development. This is facially troubling because a lack of development would stifle the usability of phone operating systems. However, the reality of paid or subscription-based applications makes it unlikely that developers would have to rely solely on advertising revenue in order to be profitable. Thus, the ability of users to control application permissions, through express notification at download and during first use, coupled with the capability to change user settings at any time, would provide the user with greater control over access to their most sensitive private data with minimal loss of functionality or harm to the market.

B. Legislative Action Is Necessary to Assure Mobile Privacy

While the aforementioned changes to individual users' interactions with mobile applications are necessary, truly successful privacy protection will require high level reform across all applications. A strong legislative response is necessary to help combat the threats to privacy that exist, and legislation at the national level would be the most effective means of enacting such reform. A successful Congressional reform will provide users of mobile platforms with a secure, uniform experience, wherever they are within the United States. This proposal should include provisions for privacy policies, "Do Not Track" measures, and the securing of all information locally stored on mobile platforms.

[116] This has already been seen with the reworked permissions model introduced in Android 6.0. While users now have the ability to accept or deny individual permissions requested by an application, most developers have not updated their applications to work with the new system, causing a denied permission to hinder the usability of the application.

1. Privacy Policies Need to Be Made More Transparent

Some states have already begun to realize that changes to privacy protection are necessary. For instance, the California Online Privacy Protection Act of 2003 (hereinafter "OPPA"), requires commercial web sites to post their privacy policies for users to review.[117] This is a common sense first step that is necessary in a successful fight against infringement of privacy; when users are aware of how their information is accessed and may potentially be used, they are able to make an informed, calculated decision about the websites and services to which they want to provide information. Requiring this to be easily accessible to mobile users of websites should be a major part of the reform legislation.

OPPA provides a number of regulations that should serve as a potential model for how the national standard should regulate this area. OPPA requires a number of additional disclosures, which should be co-opted into a national standard for privacy on a mobile platform. Among these disclosures are the types of personal data the service collects, the third parties with whom the information might be shared, and the means available to the user to review and change the private information that has been collected.[118] In addition to these disclosure requirements, national reform should include requirements that websites provide consistent definitions of important terminology. Again, OPPA is illustrative of how a definition should be structured. Under the applicable code sections, "personally identifiable information" is any information that allows for physical or online contact with a specific person.[119] This is particularly important for

[117] CAL. BUS. & PROF. CODE §§ 22575-22579.
[118] CAL. BUS. & PROF. CODE §22575.
[119] CAL. BUS. & PROF. CODE §22577. This section provides a non-exhaustive list of information meeting this definition: first and last name, physical street address, email address, telephone number, social security number or "any other information" that would result in contact with the user.

users of mobile platforms because the devices those users are using to access the Internet contain a much larger store of private, sensitive data that might be accessed.

Under the system I propose, a website would recognize that the request was coming from a non-computer platform when a mobile user sends a request to view the webpage and would display the requisite privacy policy notification.[120] This would be an even stronger protection than afforded under OPPA because it would affirmatively direct users to the privacy policy, immediately informing the user of the specific site's data policies. The obvious disadvantage to this proposed step is that the user experience would be disrupted by having to first view a privacy policy. This disadvantage can be mitigated or avoided by adopting a similar structure for both the website and the privacy policy for mobile users: when the website is accessed by a mobile browser, it will not only deliver a mobile-optimized version of the website, but also a comparably optimized privacy policy. This version of the policy would quickly highlight the data policies of the website which are most applicable to mobile platform use, including location data, tracking of browsing history, and access of any data stores from within the phone, such as contacts or a calendar. This could be presented so as to minimally impact the user's experience on the website while still giving them access to the important privacy information necessary to make informed choices.

2. Do Not Track Requirements Must Be Better Enforced and Regulated

In order to better secure the privacy of mobile technology users, more aggressive implementation and policing of "Do Not Track" requests is also necessary. To begin, the

[120] The default behavior of a web browser is to request a mobile-optimized version of the page so that users have a more pleasurable experience navigating it. There is, though, the ability for mobile users to request a "desktop" version of the website, which would appear just as it would on a desktop computer. While this functionality is available on most major browsers, the default behavior is to access the web through "mobile" versions of pages and so this step of triggering privacy policies when a mobile-version request is sent would cover a large majority of mobile user interactions.

implementation of a "Do Not Track" option should be made uniform across all web browsing experiences. Legislative reform should include a provision calling for "Do Not Track" to be offered as an opt-out as opposed to opt-in format. This would require all browsers, both standalone or integrated applications, to send the necessary request whenever a user navigates to a webpage on his or her mobile device.[121] Such a system would allow users to enjoy the benefits of a "Do Not Track" request without having to navigate each browser's maze-like settings menus.[122] This is particularly necessary when using a mobile device, because the breadth of private information which may be collected from a mobile device is often much greater than that which could be collected from a traditional computer platform. In addition, making the request default to "on" with an option to turn it off would ensure that users make an explicit choice to share personal information.

A second major hurdle to the effectiveness of "Do Not Track" requests is that they are virtually unenforceable.[123] This must be changed so that a default request would have an effect of protecting user privacy. The proposed legislation should require any website who receives a "Do Not Track" request to honor it. This is necessary because under the current framework, a majority of websites receiving these requests from users choose to ignore them.[124] For the requests to have any chance at being effective, there must be mandatory compliance with these requests when they are received by the web service provider.[125] Legislation should include the

[121] Implementation such as the one proposed here has already started at a small level on the traditional computer platform, with Microsoft making these requests default on their Internet Explorer 10 browser. *See* Joshua A.T. Fairfield, *Do-Not-Track as Default*, 11 NW. J. TECH. & INTELL. PROP. 575, 578 (2013).
[122] Creating a relative ease of access to this privacy request is paramount since the majority of users are unaware this option is even available to them. *See id*.at 579 n.18.
[123] *See id*. at 582.
[124] *See id*. at 578-79 n.16.
[125] Such a scheme would also force those websites who do not want to honor the request to make a statement as to why, increasing the amount of information to the user in making their choices. *See* Lauren E. Willis, *Why Not Privacy By Default?*, 29 BERKELEY TECH. L.J. 61, 66 (2014).

ability to penalize those websites that fail to comply.[126] This penalty, imposed under a strict liability framework, would likely take the form of monetary sanctions against the company and could include a period of "probation" during which the company's performance would be monitored.[127]

Finally, a primary issue that makes "Do Not Track" requests ineffective is the absence of a central, regulatory body to monitor compliance.[128] This hurdle could be resolved by assigning control of "Do Not Track" enforcement to an existing government agency—most likely the FTC[129]—or by creating a new governmental body whose function is specifically to handle such enforcement. This vein must also follow through to the cellular service providers, who are capable of performing the same type of user tracking implicated by websites, but with perhaps even more of an ability to go about it undetected.[130] With this triad of changes, "Do Not Track" can shift from a theoretical privacy fix to a realistic privacy guard.

These changes to the state of "Do Not Track" requests would not be without viable counter arguments and pushback. Website operators will likely strongly disfavor this top-down, legislative reform approach because much of the benefit in hosting a website comes from

---

[126] The FTC has previously endorsed a system of self-regulation in dealing with "Do Not Track" requests. Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change* (2010), *available at* http://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework. This system has shown its inability to provide real privacy protection for consumers, necessitating a stronger, more regulated approach.

[127] For reasoning behind the strict liability standard, *see* Tracy A. Steindel, *A Path Toward User Control of Online Profiling*, 17 MICH. TELECOMM. & TECH. L. REV. 459, 489 (2011).

[128] *See* Fairfield, *supra* note 121, at 581 (contrasting the treatment of Do Not Track requests with the national Do Not Call Registry).

[129] The FTC would have control over the enforcement discussed in the proposed legislation by virtue of its oversight of unfair and deceptive trade practices. *See* Angelica Nizio, *Taking Matters into Its Own Hands: Why Congress Should Pass Legislation to Allow the FTC to Regulate Consumer Online Privacy with A "Do Not Track" Mechanism*, U. ILL. J.L. TECH. & POL'Y, Spring 2014, at 283, 289.

[130] There has not been any revelation of tracking by cellular providers on a large scale, though the Electronic Frontier Foundation has disclosed tracking by Verizon and AT&T using a similar cookie method. *See* Jacob Davidson, *Verizon and AT&T Snooping on Customers' Web Activity*, TIME (November 4, 2014), *available at* http://time.com/money/3556165/verizon-att-supercookies/.

advertising revenue. With the enforcement of "Do Not Track" requests, the amount of useful information which could be used to target users with customized advertisements or to sell to third party advertisers will be greatly reduced. This may result in a wave of websites refusing to allow users access without disabling their "Do Not Track" request.[131] A workaround to this would be to allow the website to inform the mobile user that the website may not function optimally unless the page is accessed again without the "Do Not Track" request being sent. The user would then be given the choice to either continue to use the website without tracking, or reload the page, accept the tracking request but doing so in exchange for a "better" experience. Additionally, websites may be able to simply adapt their revenue streams if "Do Not Track" requests are universally enforced, by relying on less personalized advertising; the websites would be able to continue receiving advertising income while honoring the "Do Not Track" requests sent by users. These changes represent a substantial alteration to the status quo, but could be satisfactory to both Internet users and website operators.

C. Security of Stored Private Data Must Be Scrupulously Protected

Beyond affirmative steps taken by mobile users to put their information out into the world, it is necessary to keep private information that is automatically created and stored on user devices secure from any transmission that occurs without the user's consent. The standard of the search and seizure of mobile devices must be modified to guarantee not only consistency, but also adequate protection of sensitive data. Proposed legislation should include language that augments the privacy protections afforded to mobile devices under contemporary search and

[131] This would probably mirror the way that certain websites handle browsers that attempt to access them while rejecting cookies: the user is told that the website will not function properly without accepting the cookies and will therefore limit their ability to use the site.

seizure law.[132] Some academic proposals have tried to define how far police can delve into a mobile device before a warrant is required.[133] But, more regulation than that offered by these proposals is needed in order to secure private data. The proposed legislation should therefore include the necessary language to require not only a search warrant to issue any search and seizure of a cell phone incident to arrest,[134] but also to extend this concept further to require a highly specific search warrant that details the exact information expected to be contained within the phone. The prototypical requirement for a search warrant is probable cause and particularity in the description of the thing to be searched.[135] A police officer requesting permission to search a cell phone should be able to describe exactly what information is contained within the phone, as opposed to simply claiming that the phone contains evidence of a crime.[136] Under this approach, officers would not be entirely prevented from searching mobile devices for evidence in the course of a criminal investigation, but would need an officer to state exactly what is expected to be found on the phone. A likely argument against this approach might concern the necessity of finding pertinent evidence to combat crime. If police officers were required to obtain a search warrant in every instance that a mobile device is involved, the criminal justice process would become overwhelmed and the usefulness of the data stored on the phone would be less helpful to prevent crime.[137] While this is a valid concern, it must be balanced against the interests of the user in protecting the data stored on their mobile device.

---

[132] This would be possible since constitutional guarantees—like the one found in the 4th Amendment pertaining to search and seizure—set the floors for protection, not ceilings.
[133] *See* Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 54-55 (2008) (arguing that a "five-level deep" rule would help protect private information stored on a mobile device).
[134] *See generally* Riley, *supra*, note 103.
[135] U.S. Const. amend. IV.
[136] An example of this would be an affiant stating that a cell phone contained photographs of the user engaged in a criminal act.
[137] Much has been made about the ability of sophisticated mobile technology users to quickly access, and delete, damning files on modern mobile technology. *See The iPhone Meets the Fourth Amendment*, *supra* note 133, at 40.

Furthermore, the proposed legislation ought to include explicit protections for mobile devices protected by a password and encryption.[138] This language would prevent police who have seized a protected mobile device incident to an arrest from having an unlimited number of opportunities to unlock it, particularly in light of the common feature that erases data after numerous failed attempts to enter the correct password. Similar to current rules, a phone seized incident to a valid search warrant may be subject to attempted "cracking" passwords or encryption by a law enforcement technician, although wiping the phone through repeated invalid passwords should also remain forbidden.[139] Finally, it is necessary that the proposed legislation contain rules differentiating between data that remains locally on the phone and data which is accessible by using the phone to access the Internet. This illustrates the distinction between searching items found on the person and being unable to search any item owned by that person that is not on the person at the time of arrest.[140] A search incident to arrest applies only to the person being searched and any items on their person, while seeking a search warrant to inspect information held elsewhere should be held to the heightened particularity standard described above. Thus, any data on the mobile device that would be accessible absent an active connection to the Internet, such as text messages and photos, would be subject to the *Riley* standard of requiring a search warrant pursuant to a search, while any information requiring the Internet, such as clouded-based files, would be strictly off-limits to the police once the device is seized.[141]

---

[138] This point is particularly salient since both Android and iOS have implemented, or will soon, implement automatic encryption of data on the device. *See Google Fires Back at Tim Cook, Says Android L Will Protect Users With Encryption*, DAILYTECH. (Sept. 22, 2014), http://www.dailytech.com/Google+Fires+Back+at+Tim+Cook+Says+Android+L+Will+Protect+Users+With+Encryption/article36579.htm.

[139] *See* Adam M. Gershowitz, *Password Protected? Can A Password Save Your Cell Phone from A Search Incident to Arrest?*, 96 IOWA L. REV. 1125, 1154 (2011) (arguing that police should not be permitted to attempt guessing a password so many times that it would erase the contents of the cell phone).

[140] *See* Gershowitz, *supra* note 133 at 57.

[141] This result also comports with the rationale of preventing the destruction of evidence by warrantless seizure: if the information is unavailable to the user absent an Internet connection, simply securing the phone would prevent

This would not preclude total access to the data on the mobile device, but, rather, requires the police to obtain a warrant to search through cell phone data that requires an internet connection. Therefore, language specific to the protection of stored data on mobile devices is imperative to the protection of mobile user privacy.

V. CONCLUSION

The solutions proposed here are important and necessary steps to safeguard the privacy of mobile technology users. By changing the way that application permissions are handled and giving users substantially more control over them, mobile applications can continue to function as a primary means of mobile interaction while being less of a threat to sensitive information. Likewise, though the proposed legislative action is not a silver bullet fixing all the problems of mobile privacy, the proposed changes to how mobile data is handled is a key step in the right direction. By ensuring that privacy policies are clear and brought to the user's attention when visiting a website, the mobile user is able to make a more informed choice and better manage their private data. Similarly, requiring "Do Not Track" requests to be automatic and enforceable will make certain that those using mobile technology will not face the false security that exists under the current system. Finally, increasing the protection afforded to data residing locally on mobile devices recognizes the growing reliance that people are placing on them and the evolving privacy concerns arising out of this developing technology.

It may seem that this proposal is placing an undue amount of importance on mobile technology. It is undisputed that all technology implicates important privacy rights. The reality, however, is that now, more than ever, mobile devices are the dominant means by which the

---

them from modifying or erasing that information by means of the mobile device itself; the police could always subpoena that provider of the service to obtain the same information from the user's account.

average person conducts their life and as a result, users entrust devices with their most sensitive information. It seems that every day another major data breach is being reported with the most sensitive of personal information—financial information, health care data, and social security numbers chief among them—being leaked for the whole world to take. With the increasing reliance on mobile technology to make our lives convenient, the protection of the information at risk is paramount. As mobile technology continues to change and grow, the potential for its misuse and the damage caused therefrom proceeds in lockstep. Therefore, it is of the utmost importance that the protections afforded to privacy—and the data comprising such privacy—adapts at the same pace.