Shawn Fenner

Ms. Graham

English 102 (VE)

3 December 2018

Solutions to the Ongoing Concern of Mobile Data Privacy

The invention of smart phones has had a profound impact on how people live their lives. While previously desktop computers provided entertainment and increased productivity at the home or office, technological advancements have made possible many of the same features of desktop computing available to consumers in the form of a small, portable device. Due to an exponential number of applications that smart phone users can download in mere minutes, everyday consumers now have access to a plethora of features that can be taken anywhere. And as with desktop computing, the ability to store enormous amounts of personal information is also at hand. This personal information, ranging from emails to photographs, contact information, phone numbers, credit card numbers, and even geolocation and conversation data, is now readily available and can be transmitted in the blink of an eye. Consequently, consumers must now place their trust in the applications they utilize on a daily basis, hoping that these applications will protect the privacy of their information and use it in a responsible manner. Unfortunately, the privacy of consumer information is not always used in ways consumers would expect. However, by examining the issues surrounding mobile data privacy and how violations of privacy can occur, solutions can be proposed to help to ensure that consumers are aware of how their information is being collected and transmitted. Solutions can also be proposed to ensure application developers are placing a priority on consumer privacy or face consequences.

According to research conducted by the *Pew Research Center*, 95% of Americans now own a mobile device, 77% of which is a smart phone (“Mobile Fact Sheet”). These numbers indicate that an enormous amount of consumer information is now being stored digitally. Smart phones have become digital repositories for consumers’ lives and memories. As a result, consumers have a right to know what type of information is being collected from them, by whom, and how it will be utilized. Corporations, having found themselves with an abundance of data at their fingertips, have a duty to protect the privacy of their customers. Concerns arise when consumer information is collected, stored, and used without consumers’ knowledge and consent or in an underhanded way. With rapid changes in technology and the laws governing consumer mobile privacy struggling to keep up and become modernized, ensuring consumer information is used responsibly while still affording companies the data they need is a daunting task.

For some applications, collection of consumer data is required for the applications to function properly. Take for instance a map-based application that directs users to the nearest eatery based on certain criteria. In this case, the application must gather geolocation data from users and then send it to a server in order to process it and provide accurate directions. Consumers feel some assurance knowing that their information is only being used for what is necessary for the application to perform its desired task. This example illustrates that the context – or how consumers expect an application to work and what type of information it collects given a particular circumstance – is a key principal for companies in identifying and designing applications to best fulfill the privacy needs of consumers. However, when companies design applications that do not meet this context, a violation of privacy is likely to occur. For example, a gaming application collecting geolocation data or requesting permission to access photos and contact information has no need for such data and such practices can actually work towards the detriment of the company.

Various studies indicate that when consumer information is collected out of context, consumers will express negative feelings towards the offending applications and their companies. In one study which examined participants’ expectations with regard to mobile data privacy, the results indicated that applications that collected data not related to the context in which participants expected resulted in feelings of distrust (Martin and Shilton 200). Applications which collected photos and contact information were particularly met with disfavor as participants did not expect these types of information to be collected (Martin and Shilton 212). In another study conducted by researchers at Carnegie Mellon and Rutgers University, participants were to read and understand privacy policies on two applications, a flashlight application and a dictionary application. Participants were surprised to discover that these applications requested not only geolocation data but also unique phone IDs, which the applications would then send to advertisers (Talbot). And in a survey conducted by the *New York Times*, all but two participants of forty surveyed were unaware that an application was collecting their geolocation data for advertising purposes (Hettrich 983). These studies indicate that applications should only collect information from consumers that meet the applications’ context or companies will receive backlash, diminishing the trust between them and their customers and harming future sales.

While comparing the data collection practices of different applications can sometimes seem quite clear in determining which ones are collecting data not pertinent to their functions, not all scenarios are as easy to discern the best course of action regarding consumer mobile privacy. For instance, obtaining geolocation data from mobile devices is useful for some industries and benefits the general population by providing data for reducing traffic congestion, limiting the spread of disease, urban planning, medical responses, and locating lost children (Soper 36). Conversely, geolocation data could also be used by corporations and governments for their own agendas; indeed, with annual revenue of GPS services estimated at over $10 billion, companies are eager to invest in this new industry (Soper 37).

In order to allow benefits of data collection and guard against potentially deceitful practices, not only must all data collection practices clearly be disclosed by applications but laws must also be in place which help to protect consumer information and punish those companies that misuse it. The Federal Trade Commission (FTC) has already taken legal action against several companies, including local search-service provider *Yelp*, mobile gaming developer *TinyCo.*, and social networking service *Path* for privacy violations (Hettrich 998). Still, with potential profits as high as they are and outdated or yet-to-be enacted mobile data privacy laws, this solution will currently only be a deterrent for some. Fines in the hundreds of thousands are nothing compared to profits in the millions for a large company. Additionally, companies may argue that they were granted permission by their customers to gather information. Did their customers not read the fine print within the privacy policy, which states what types of information will be collected?

Data collection practices are to be described in an application’s privacy policy. Such documents though are often times lengthy and use jargon that is difficult to understand for the everyday consumer. Rather than spend a great deal of time in one’s already busy schedule attempting to understand a fairly technical document written by professionals, research has shown that most consumers would instead choose to accept such policies without reading them so that they can begin using their new application immediately (Talbot). Unfortunately, by doing so, consumers unknowingly grant applications full privileges to gather sensitive information. To help protect the privacy of consumers and maintain their trust, developers should write their privacy policies to be as easy-to-understand, concise, and as short as possible. When such policies are amended in future updates, consumers should be alerted to such changes.

Even if such policies are improved in clarity, problems still exist when consumers’ information is collected by applications without consumers’ knowledge or consent. Take for instance the application *Angry Birds*, which has been downloaded over one billion times and has been guilty of collecting contact information, geolocation data, and unique phone IDs without device owners’ knowledge (Hettrich 982). Other examples include *ShopKick* and *Color*, which collect background noise data from a device’s microphone, *Pandora*, which collects age, geolocation data, and unique phone IDs, and *Bejeweled 2*, which collects contact information (Paul and Rose 14). The primary reason for gathering consumer information is to sell it to advertisers for monetary gains. If the cost of applications that are free or low-priced were to be increased, less tracking of consumer information would be involved. Indeed, the greater the cost of an application, the less likely it is to track users; whether this solution helps to offset the loss in revenue due to reduced advertising is difficult to determine (Sundaresan and Vallina-Rodriguez). However, as mentioned earlier, companies may simply accept legal penalties and continue to collect consumer information in underhanded ways if they see such a practice as offering a competitive advantage. Therefore, guidelines need to be put in place that companies must follow that will allow consumers to easily recognize what types of data an application will be collecting.

Consumers have grown increasingly accustomed to downloading free or ninety-nine cent-priced applications. Consumers must be aware that companies need to make a profit somehow and a valid argument is that collecting consumer information for advertising monetization should be expected. However, regardless of the pay model, applications should still disclose upfront all data collection practices as consumers have a right to privacy. Companies can still rely on several practices in place that earn revenue for low-priced apps, such as serving ads but disabling them after consumers have paid a fee. This concept extends to offering in-app purchases for specific features or advantages notable in gaming applications, such as awarding extra in-game currency or additional levels or power-ups. Still, some companies may wish to continue to gather information even in perceived underhanded ways due to the current laws surrounding mobile data privacy.

Such laws are either outdated or continually having to be reinterpreted as new technologies are introduced, and when compared with other areas of the legal system, are limited, posing complex questions on how to best handle mobile data privacy (Hettrich 984). The FTC can seek civil monetary penalties if violations do occur and is actively trying to address numerous privacy concerns and how to advise companies to comply with privacy statutes, but much work still needs to be done (Hettrich 985). Improved privacy laws need to be enacted exclusively for the mobile environment in order to limit the data collection practices of device manufacturers and developers who have been taking advantage of the current, outdated system (Hettrich 983). Thus, consumers need to be wary whenever installing new applications and organizations such as the FTC and others can help educate consumers on how to best protect their privacy on mobile devices. Carefully reviewing data collection practices and limiting the amount of sensitive data stored on smart phones are ways consumers can help to keep their information secure in the meantime, although such practices will most likely be required for years to come.

The application industry is highly competitive and companies try to keep their development times as short as possible. One way developers commonly speed up the development process is to integrate collections of code written by other companies – referred to as *third-party libraries* – into their applications. Although these third-party libraries provide useful functionality, such as monetization through displaying ads, connecting users with social media, and providing analytical data by tracking user engagement, they often times collect sensitive data not pertinent to an application’s intended function and without consumers’ knowledge. In one study, researchers from various universities across the United States developed a custom application in order to analyze what type of consumer information applications were collecting and transmitting along with the recipients of the data. This study discovered that more than 77% of the applications tested sent consumer information to one or more third-parties, 15% of which transmitted said data to five or more third-parties (Sundaresan and Vallina-Rodriguez). Many of the trackers identified through the tested applications were also found to track consumer information through websites, a technique known as *cross-device tracking*. Using this technique, companies can piece-together detailed profiles of users, such as by linking contact information with geolocation data and then serve them targeted advertisements (Sundaresan and Vallina-Rodriguez). One can imagine how this technique raises privacy concerns that would be difficult to discover, leaving consumers to ponder how companies know so much about them.

A major concern with relying on third-party libraries is the services they provide frequently run in the background and transmit data over networks all the while presenting no indicators of any kind, leaving consumers and even the developers themselves with no insight towards their presence (Allman et al. 1). For developers relying on functionality provided by third-party libraries, extra precautions should be taken to ensure the privacy of users is not violated. Developers using third-party libraries need to themselves understand what data these libraries will be collecting and with whom it will be shared. Developers must then clearly disclose these data collection practices within their applications’ privacy policies. While some companies might argue that building certain functionalities into their applications or identifying the tracking capabilities of third-party libraries would add to development time, not being conscientious towards customers’ privacy might ultimately prove more costly due to potential fines, lawsuits, and consumer distrust.

Smart phones, possessing much the same functionality as desktop computers, have become prevalent in our society. Many people rely on these devices in their everyday lives in order to store sensitive information. Privacy concerns arise when applications gather consumer information from these devices in ways that consumers do not expect or without consumers’ consent or knowledge. Developers relying on third-party code libraries also may be inadvertently compromising the privacy of their users as the code from these libraries collects and transmits consumer data in the background. Privacy policies might also be overly long and too complex for everyday consumers to understand.

Having companies clearly disclose all data collection practices, having them charge more for applications to reduce advertisement and data collection monetization, or issuing them fines for instances of privacy violations are several, albeit not complete, solutions to the ongoing issue of mobile data privacy in our society. Additionally, new laws will need to be enacted to help protect consumer mobile privacy as many are still outdated. Consumers can take actions to keep their information secure, such as by storing the least amount of sensitive information on their mobile devices as they can and by taking caution when installing new applications by reading data collection policies. While privacy issues will always be a concern in our society and the laws accompanying them complex, all of these solutions will go a long way towards helping to maintain the integrity of mobile data privacy.

Works Cited

Allman, Mark, et al. “Apps, Trackers, Privacy, and Regulators.” *International Computer Science Institute*, 2018, pp. 1-15. https://haystack.mobi/papers/ndss18\_ats.pdf. Accessed 30 Nov. 2018.

Hettrich, Matthew. "Data Privacy Regulation in the Age of Smartphones." *Touro Law Review*, vol. 31, no. 4, Oct. 2015, pp. 981-1011. *EBSCOhost*, ezproxy.fhsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=108794666&site=ehost-live. Accessed 30 Nov. 2018.

Martin, Kirsten and Katie Shilton. "Putting Mobile Application Privacy in Context: An Empirical Study of User Privacy Expectations for Mobile Devices." *Information Society*, vol. 32, no. 3, May-Jun 2016, pp. 200-16. *EBSCOhost*, doi:10.1080/01972243.2016.1153012. Accessed 30 Nov. 2018.

“Mobile Fact Sheet.” *Pew Research Center*, Feb. 2018, http://www.pewinternet.org/fact-sheet/mobile/. Accessed 30 Nov. 2018.

Paul, Ian and Brent Rose. “Smartphone Spying Reality Check.” *PCWorld*, vol. 29, no. 7, July 2011, pp. 13–15. *EBSCOhost*, ezproxy.fhsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=61155081&site=ehost-live. Accessed 30 Nov. 2018.

Soper, Daniel. “Is Human Mobility Tracking a Good Idea?” *Communications of the ACM*, vol. 55, no. 4, Apr. 2012, pp. 35–37. *EBSCOhost*, doi:10.1145/2133806.2133819. Accessed 30 Nov. 2018.

Sundaresan, Srikanth and Narseo Vallina-Rodriguez. “7 in 10 smartphone apps share your data with third-party services.” *The Conversation*, May 2017, http://theconversation.com/7-in-10-smartphone-apps-share-your-data-with-third-party-services-72404. Accessed 30 Nov. 2018.

Talbot, David. ”Using Crowdsourcing to Protect Your Privacy.” *MIT Technology Review*, April 2012, https://www.technologyreview.com/s/427390/using-crowdsourcing-to-protect-your-privacy/. Accessed 30 Nov. 2018.