Shawn Fenner

Ms. Graham

English 102 (VE)

4 November 2018

Should There Be Limitations About What Data Your Phone is Sharing About You?

You have just purchased a brand new smart phone complete with the newest features. You have set up a new phone number and made several calls, taken numerous photos, and installed a dozen new applications, many of which were free. You are enjoying your new phone immensely. Strangely, though, you’ve been receiving phone calls from people you don’t recognize, primarily advertisers. And you have been receiving various advertisements through your email and your installed applications, all of which are offering discounts and suggestions on products that seem all too familiar. Some even appear to know where you went to dinner last night and who your friends are.

In an age where the majority of people possess a mobile device, many of whom can’t imagine living without one, privacy concerns have arisen as a continuous supply of consumer data is transmitted around the globe every day. According to a report conducted by the Pew Research Center, ninety-one percent of adults in the United States now possess a cell phone, approximately fifty-six percent of which is a smart phone (Hettrich). As such, one can easily surmise that an enormous amount of consumer data is now being stored digitally. As smart phones have become digital repositories for peoples’ lives and memories, corporations now have access to a plethora of information, some of which consumers would be wary of or completely against sharing, especially if they realized what sensitive information of theirs was being transmitted on a daily basis.

Applications can collect varying types of consumer information from mobile devices, including telephone number, unique ID, contacts, and geolocation. Unknown to most consumers, this list also includes conversations through the device’s microphone and even photos. Where this information will be stored and for how long and its intended purpose is difficult to answer. Therefore, with so much uncertainty regarding privacy concerns that exist today in our technologically-driven society coupled with our reliance on the ubiquitous smart phone, limitations need to exist concerning the collection and usage of data of everyday mobile device users.

One of the initial steps prior to installing an application is reading and understanding an accompanying privacy policy agreement. This document commonly describes what type of information the application will gather and provides the consumer with some assurance knowing that, for instance, their location will be tracked regularly due to the necessity of a map application to provide directions to the nearest eatery. While such scenarios are understandable in order for certain applications to function properly, sometimes applications collect data from users without their knowledge or consent. Take for example one popular application that most people will instantly recognize – *Angry Birds*. This application has been downloaded over one billion times but has been found responsible of collecting consumer data, including contacts, longitude and latitude information, and unique phone IDs, without device owners’ knowledge, where it was then transmitted to third parties for later advertising (Hettrich). Other examples include *Bejeweled* *2*,which collects phone numbers, *ShopKick* and *Color*, which collect background noise from the device’s microphone, and *Pandora*, whichcollects age, location, and phone ID (Paul and Rose). Some may argue that these and other free or inexpensive applications must collect data from users to offset their low price point. However, collecting data without consumers’ knowledge or consent is a clear example of where limitations of data collection need to be in place so that consumers can understand what type of information they will be sharing and with whom it will be shared.

Privacy policies should disclose an application’s data collection practices, but such policies are often times difficult to understand. Their excessive length combined with their technical terminology makes reading them a time-consuming chore that most consumers would rather ignore. Most consumers would rather simply scroll to the bottom of the document and click the “I Agree” button so that they can try their new app. Some may wonder how companies can get away with making consumers agree to policies the consumers can’t even understand. Even when consumers do take the time to attempt to understand the document, certain wording and terminology can grant data collection privileges to applications whereas consumers might believe otherwise. “Provider may modify the terms of this agreement at any time...,” indicates that the company can simply rework the privacy policy at any time in order to collect additional data from the user (Sparks). Another example includes wording similar to, “Providing data or user content through this service grants provider an irrevocable right to license, distribute, transmit, or publicly display data or user content,” which fails to include that the company can only use the data for its intended service (Sparks). To avoid consumers finding their data being used in unexpected ways, limitations need to be imposed on applications preventing them from containing privacy policies that are too lengthy and difficult to understand for the everyday consumer.

Besides the accompanying privacy policy, the context in which the application is used is also important to consider in regard to mobile data privacy. What type of information consumers expect an application to collect can sometimes differ with that of the actual data collected by the application. For instance, an application utilizing the device’s flash light has no need to collect geolocation or contact information. Based on a study which examined participants’ expectations with regard to mobile application privacy, the results concluded that participants were surprised and expressed a negative feeling towards applications that were serving them targeted advertisements based on data collected from them that was not pertinent to the application’s intended purpose (Martin and Katie). Participants were also surprised and did not expect contact information and photos to be collected by any application (Martin and Katie). Therefore, applications need to collect only information that meets the expectations of consumers and the context in which it is relevant.

While consumers may unknowingly grant data collection privileges to applications due to perceived context, sometimes the developers themselves, while good-intentioned about consumer privacy, are the ones who make the mistake. Applications commonly rely on third-party collections of code, referred to as *libraries,* which become integrated with that of the code written by an application’s original developers. Issues arise when these third-party libraries collect data from consumers that the developers had not intended, contrasting with what was actually specified in the application’s privacy agreement. Indeed, one study found that more than seventy percent of applications send personal consumer data to one or more third-parties, fifteen percent of which transmit said data to five or more (Sundaresan and Vallina-Rodriguez). This means that applications may be collecting information from consumers that is not pertinent to an application’s functions and thus data limitations need to exist to protect consumers’ data from being used without their permission. Even though certain types of a user’s data may be collected by separate applications, the information may eventually end up being pieced-together to form a detailed profile of that user, such as by linking location and contact information (Sundaresan and Vallina-Rodriguez).

With society’s reliance on mobile devices for communication and storage of personal information, the privacy of consumer mobile data is often times violated. While consumers are responsible for reading privacy agreements and choosing which applications to install on their mobile devices, developers must collect consumer information in a responsible manner that is clear to consumers. Providing easy-to-read privacy agreements that clearly state what types of data will be collected and with whom it is shared is one way. All parties that will receive and work with consumer data must be specified and the data must only be used for its intended purpose. Developers must also be aware of the tracking capabilities of any third-party libraries they include in their applications which may be collecting and transmitting consumer data to a variety of recipients. Having data collection limitations in place is therefore a necessary step in protecting the privacy of consumers.

Works Cited

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 15 Oct. 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-Jun2016, pp. 200-16. *EBSCOhost*, doi:10.1080/01972243.2016.1153012. Accessed 15 Oct. 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 15 Oct. 2018.

Sparks, Sarah D. "Reading the Fine Print." *Education Week*, vol. 36, no. 26, 29 Mar. 2017, pp. 24-26. *EBSCOhost*, ezproxy.fhsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=122227196&site=ehost-live. Accessed 15 Oct. 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 15 Oct. 2018.