Shawn Fenner

Ms. Graham

English 102 (VE)

8 October 2018

Annotated Bibliography for Mobile Data Privacy Concerns

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 Sept. 2018.

This article discusses the concern and need for regulation in regard to mobile data privacy due to the prominence of smart phones in today’s society. The article lists different examples of companies that have obtained users’ personal information without their knowledge or consent or in an unclear or underhanded way and the penalties these companies have faced as a result. The article also describes the Federal Trade Commission’s involvement in these cases and its role in protecting the consumer. The article also describes several laws that have been enacted that help protect mobile data privacy, such as *The Children’s Online Privacy Protection Act* and the *Can-Spam Act*.

This article will be useful for me because I will be able to use the different cases it describes of consumers’ data being compromised by corporations to illustrate the concern of privacy in today’s society. I will also be able to use it to mention laws already in place that help protect mobile data but are falling short or were written before smart phones were commonplace, in order to further build upon the severity of the issue.

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 Sept. 2018.

This article discusses the concerns involved with location-based tracking in regard to the collection of mobile data. It explains that due to advances in GPS technology, corporations and governments can obtain data from mobile phone users through applications and use this data to determine and document mobile behavioral patterns with a high rate of accuracy. Such human mobility tracking can result in a loss of privacy and could be used for questionable, controversial, or unethical means. The article also mentions the benefits involved with human mobility tracking if used in a noble manner, including urban planning, reducing traffic congestion, limiting the spread of disease, medical response, and determining the location of children for concerned parents.

This article will be useful for me because it examines the concerns involved with how corporations and governments are using GPS tracking technologies to document human mobility patterns for their own agendas. These agendas are oftentimes monetarily related, with annual revenues of GPS-based services estimated at over $10 billion. I can also use the article to provide examples of the benefits of human mobility tracking if the technologies are used responsibly and for the betterment of mankind.

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 16 Sep. 2018.

This article introduces how consumers’ expectation of privacy in regard to the collection of their mobile data varies depending on the type of application and context. This article also describes how consumers’ expectations of privacy oftentimes differ with the actual tracking, usage, and data collection done by the applications and described in their accompanying privacy agreements. The results of a survey are provided in which participants of varying age were to express their trust in a wide range of applications and whether or not the applications met their expectations of privacy.

This article will be useful to me because it explores how the context of a mobile application can change how the consumer determines how an application is trustworthy in regard to what type of data they disclose and how the application treats their data. I can use this information to describe how companies need to revise their policy agreements in order to make them more clear and consistent with consumers’ expectations.

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 2 Oct. 2018.

This article introduces the concern of consumers’ mobile data being collected from applications where it is then sold to third parties or used for other purposes unclear to consumers. Large corporations including Apple, Google, and Microsoft gather GPS tracking information from users according to device privacy settings. Some applications can turn on a device’s microphone and gather sound data through it. A test conducted by the Wall Street Journal discovered that most of the applications it examined shared a device’s unique ID number with third parties; some shared longitude and latitude information while others shared contact information or phone numbers.

This article will be useful to me because it will allow me to bring to attention how applications, some used by millions, gather data from their users that would seem surprising, such as through a device’s microphone. I can list several applications that the article mentions as examples.

“Pew Study Sheds Light on App Users’ Awareness of Privacy Issues.” *Computer & Internet Lawyer*, vol. 29, no. 12, Dec. 2012, pp. 38–39. *EBSCOhost*, ezproxy.fhsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=83479961&site=ehost-live. Accessed 5 Oct. 2018.

This article explores the behavior of participants in regard to mobile data privacy based on a study carried out by the Pew Research Center. It describes how, due to advancements in mobile technologies, consumers are increasingly storing vast amounts of information about their lives on their mobile devices. The research concluded that most consumers are unaware of how and what type of data is collected from the applications on their mobile devices. Also provided are various statistics gathered from the study.

This article will be useful for me because it includes various statistics concerning consumer privacy behaviors. I can use these statistics to illustrate how consumers are concerned about their mobile data privacy yet aren’t entirely aware of how the applications they use on a daily basis are using their information.

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 16 Sept. 2018.

This article describes the increasing use of applications in curriculums and the potential leaking of student data they may exhibit. In 2016, researchers at Carnegie Melon University examined the privacy policy of approximately 18,000 free applications along with their corresponding computer code and found discrepancies between what the policies stated and what data the software actually collected. The article also examines the importance of understanding the privacy policies accompanying free applications and what data is being collected from users.

This article will be useful for me because it will allow me to demonstrate how even though some applications may be monetarily free to use, the real cost of these applications is the data they collect from their users. This article also provides several examples of some common application privacy agreements that may be difficult to interpret or give the applications questionable data collection privileges.

Tucci, Linda. “Mobile Data Privacy Rules Cannot Be Ignored.” *Computer Weekly*, Mar. 2013, pp. 19–21. *EBSCOhost*, ezproxy.fhsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=86374867&site=ehost-live. Accessed 3 Oct. 2018.

This article discusses mobile data privacy recommendations provided by the Federal Trade Commission. These recommendations are aimed at software developers, operating system providers, and social media platforms. These recommendations include providing a privacy policy readily available to consumers through app stores, providing do-not-track settings on mobile devices, obtaining consent from consumers before collecting sensitive data, and taking part in trade associations and self-regulatory programs in order to better understand how to create short, effective privacy disclosures. Developers that use third-party code in their applications in order to integrate tracking or advertising features must understand what kind of data this code is collecting.

This article will be useful to me because I can use the recommendations provided by the Federal Trade Commission to illustrate what application developers should be doing in order to responsibly gather data from and meet the privacy expectations of consumers. I can also describe how developers with good intent might find themselves unknowingly tracking and transmitting particular user data due to the integration of third party code in their applications.

Willis, Lauren E. "Why Not Privacy by Default?" *Berkeley Technology Law Journal*, vol. 29, no. 1, Spring2014, pp. 61-134. *EBSCOhost*, ezproxy.fhsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=96521421&site=ehost-live. Accessed 15 Sept. 2018.

This article explores how consumers decide upon what mobile privacy settings to enable, disable, ignore, or express confusion or misconceptions towards in regard to their devices and tracking. The consumers’ thought processes, including assumptions, decision biases, technical knowledge or lack-of, is also explored. The article also addresses the default settings for tracking which encompass numerous categories of data and data collection practices, including the type of information collected (e.g. email; global positioning; medical), the type of user (individual or company), and where the data was collected (e.g. website; application).

This article will be useful for me because it will help me provide a contrasting argument. I will mention that, while consumers are concerned about the privacy of their data and how companies might use it, consumers also have a role in ensuring that their data is shared in a responsible way.