Final Project Part 4: Internet - Data Privacy

Jared Broyhill

University of Advancing Technology

Author Note

This paper was prepared for LAW370, taught by Professor Scott Beemer.

Abstract

The purpose of this paper is to provide a description of data privacy legal issues and an explanation of them (along with any laws or court cases, if relevant), in addition with identifying a Wikipedia article related to the issue along with an evaluation of its accuracy and comprehensiveness as it relates to the issues.

Final Project Part 4: Internet – Data Privacy

Data privacy has been a sensational topic in the conversation about personal rights and general privacy of the individual in an increasingly digital landscape. Fueled by events such as the leak of classified federal documents by former NSA (National Security Agency) employee Edward Snowden and the Cambridge Analytica and Facebook data collection scandal, provoking an outcry for privacy rights from members of the American populace.

The general contention from the public seems to be that individuals are against the government (and, to an extent, corporations) conducting surveillance on them through private means without even informing them that they are doing so. Cases like *Lloyd v Google LLC* showcased how some people tried to force corporations to legally include them in decision making since their data was being used in those decisions. Cases like these almost always play out in the corporations' favor, ensuring that the companies can continue collecting data as they please without having to answer to the public (though some states have more stringent laws than others regarding this topic).

Generally, data privacy does not appear much in the realm of judicial review setting legal precedent. This is somewhat worrying as data privacy becomes a greater issue amongst the American public and continues to be unaddressed by the state officials of the federal government. The vast majority of court cases that set something of a precedent for data security are simple decisions made to protect the general privacy of an individual in certain cases that some judges extrapolate to the cyber realm. While this does not always carry over well (as judges disagree on whether or not the ruling can be continuous with computer and data-related affairs as opposed to the more physical and practical means which it was originally addressing), it does help somewhat to protect the data rights of individuals from corporations or state/federal

governments that seek to exploit them.

The issue of data collection as it relates to private entities is another large component of data privacy. When Facebook was revealed to be letting corporations like Cambridge Analytica harvest hundreds of millions of individuals' data (particularly their voting preferences, common locations, family, religion, friends, favored activities, etc.), an outcry was sparked regarding the ethics of corporations utilizing their massive social media platforms to not only collect such information but sell it to distributors, making significant profits as a result. This issue is addressed in documentaries such as *The Great Hack* on streaming platform Netflix, as well as a plethora of articles by journalist outlets such as The Guardian. Interest is routinely proven to be among the American populace regarding this aspect of data privacy: many are unnerved and unpleased by Facebook (among other, similar corporations, such as Google and Apple) collecting such massive swaths of data from them not only without telling them but sometimes without their consent as well.

Google in particular has routinely been a target of data privacy advocates, as it harvests and contains great stores of data from all its users, never deleting any information that is given to them. For example, if an individual with a Google account was to make a google search, write something in a Google Drive document, speak something into their Android Phone (such as a request for directions), or any similar activity that utilizes the Google Cloud and requires an internet access and a Google account, that information is stored permanently by the company. Users have recently been able to request Google to send them the information the corporation has on them have sometimes received results of hundreds of gigabytes, occasionally even terabytes, from the information Google has collected from them and has purposefully not deleted. Not only is it a privacy concern but it is one of security as well. If Google was to be

breached or somehow compromised, it would mean that the countless banks of data they have of people from all across the world could be utilized for malicious purposes, such as identity theft, malware installation, and physical robbery. Google has neglected to seriously address any of these issues, instead speaking through lawyers and public relations representatives in corporate tones, communicating that the information they store is necessary and is being safety kept.

Finally, one other major aspect of data privacy is that of the ISP (Internet Service Provider) in relation to their customers. Internet service providers typically have the ability to monitor the web traffic of their customers and have even utilized that monitoring ability to slow down traffic if customers visit rival websites or utilize competing services. Additionally, the monitoring of internet service providers mean that they can constantly monitor and see whatever a customer of theirs is doing on the internet: the websites they visit, the things they download, the pictures they open online, etc. This has sparked in itself a conversation regarding data privacy (which is also related to net neutrality, as when it was established in American law by the FCC (Federal Communications Commission, it was illegal for internet service providers to slow down, impede, or otherwise "shaft" the traffic of their customers compared to their competitors. When that was repealed in 2018, it became legal), but also questions of ethics. Is it moral for these corporations to so intently monitor the web traffic of their customers? Some have tried to circumvent these measures by enlisting in services such as NordVPN or ExpressVPN to encrypt their traffic, ensuring that their internet service providers can no longer see the specifics of what they do over the internet. Despite the fact that alternatives exist, it continues to be a contentious subject not only regarding the legality of its privacy, but the morality of it as well.

Wikipedia Article

The Wikipedia article that primarily addresses the concept of data privacy and its legal

implications and components as it relates to the United States is the *Information Privacy* article. The article itself covers a multitude of different types of privacies, from the educational information of individuals (such as their grades and classes), their financial information (stocks, general assets that they hold), and even their medical information. Medical privacy is itself an extensive issue that commonly overlaps with general data privacy, hence its heavy regulation in the field of HIPAA.

For typical data privacy itself however, Wikipedia generally classifies the issue under *Internet Privacy*, which it has its own article regarding. The information it conveys to the reader is brief but informative, detailing the history of internet privacy from the advent of the internet itself toward the end of the 20th century to the more surveillance-related worries and implications of the modern day. The history it covers is accurate and relevant, assisting readers with understanding the issue while not drawing on tangents or unrelated information that could possibly distract from the issue on hand.

Additionally, the article does well to address all the different complains of data privacy, mentioning the data mining utilized by search engines (and by extent, the corporations that control them, such as Google and Microsoft) along with the guidelines and regulations that have been passed down regarding them (such as the "Fair Information Practice Principles." The article covers the concept of email privacy, discussing on its history and regulation, and includes how some parties have gone about trying to ensure that their email communications are private, mentioning mix nets such as I2P or Tor (The Onion Router). It also notes VPNs (Virtual Private Networks) as another "anonymizer" that can assist individuals, corporations, and any interested parties by giving them protection online through tunneling their IP (Internet Protocol) address through another and encrypting its traffic, rendering any monitoring of the traffic as

unidentifiable to parties interested in surveillance.

The concepts of PII (Personally Identifiable Information) and data regarding location are mentioned as another primary concern within the realm of data privacy. The article goes into detail regarding these concepts, detailing how data about location can be accidentally published by individuals who post pictures of a store in the background, and how PII can be accidentally revealed and thus mined by malevolent parties through similar careless publication of information and pictures.

The article proves itself to be competent and comprehensive, detailing the primary concerns of individuals regarding data privacy but not going into an unnecessary amount of detail (which it leaves to other, more specific articles related to the pertaining subjects). The history it details are accurate and the practices and countermeasures it mentions regarding how parties have attempted to address the increasing issue of data privacy are modern and realistic, assisting interested readers by giving them alternatives if they wish to improve their privacy after reading the article.

References

Aaronson, T. (2019, October 10). *Court ruling shows how FBI abused NSA mass surveillance*. The Intercept. https://theintercept.com/2019/10/10/fbi-nsa-mass-surveillance-abuse/

American Civil Liberties Union. (2020, February 27). *NSA surveillance*. https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance

Collins, K. (2018, June 11). *Net neutrality has officially been repealed. Here's how that could affect you*. The New York Times - Breaking News, World News & Multimedia. https://www.nytimes.com/2018/06/11/technology/net-neutrality-repeal.html

Layton, J. (2007, February 1). *Is the FBI reading my E-mail?* HowStuffWorks. https://people.howstuffworks.com/fbi-surveillance.htm

Lowry, B. (2019, July 23). *'The great hack' dissects Cambridge Analytica and the rise of big data*. CNN. https://www.cnn.com/2019/07/23/entertainment/the-great-hack-review/index.html

Mack, Z. (2019, July 9). *Net neutrality was repealed a year ago. The Vergecast explains what's happened since*. The Verge. https://www.theverge.com/2019/7/9/20687903/net-neutrality-was-repealed-a-year-ago-whats-happened-since

Meehan, M. (2019, November 26). *Data privacy will be the most important issue in the next decade*. Forbes. https://www.forbes.com/sites/marymeehan/2019/11/26/data-privacy-will-be-the-most-important-issue-in-the-next-decade/#65c1e3241882

Meldium. (2019, November 25). *How to protect your business online from ISP surveillance?* https://www.meldium.com/how-to-protect-your-business-online-from-isp-surveillance/