Privacy and the Public in the Technological Age

Waylon Abernathy III

IST 618, Syracuse University iSchool

**Privacy and the Public**

The right to privacy has been a fundamental value to American citizens since the conception of the United States; so much so, that privacy became protected by the founding fathers through the Bill of Rights in 1789. The Fourth Amendment of the U.S. Constitution states, “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized” (U.S. Const., amend. IV). Changes in technology coupled with crises like the terrorist attacks of 9/11 have altered how the government and private sector of the United States view and meddle with personal privacy. The call for policy changes and regulation on internet privacy has become a pressing matter as the public becomes increasingly aware of internet data collection practices.

Through major internet companies like Facebook and Google, Americans have turned themselves, willingly or not, into open books of information and data for the benefit of government use. Legislation post-9/11 brought about the PATRIOT act as well as the FISA Amendments Act. This legislation “enables the NSA to gain access to individuals’ online activity, employ advanced surveillance technology, and increase the use of National Security Letters” (Janbek & Williams, 2014). In 2007, the NSA began using a program known as Prism to acquire access to private communications of user of nine Internet services including Google, Facebook, and Microsoft (Greenwald & MacAskill, 2013). Access to such information gave the government an added advantage in thwarting future terrorist attacks and was viewed as a necessity by those running the program -- “the history of warfare makes clear that electronic surveillance of the enemy is a fundamental incident to the use of military force” (US Newswire, 2006). The ability to stop upcoming attacks via data collection could clearly save multiple lives; however, the “electronic surveillance of the enemy” was not just focused on “the enemy” but also the American people.

The bending of privacy law is not new to the American public. In response to growing public hostility towards entering World War I, the Sedition Act of 1918 allowed the Postmaster General to ban all materials “that might impugn the motives of the government and thus encourage insubordination” (Brinkley, 2006). Modern times are no different. The U.S. Department of Justice released their justification for the broad American civilian surveillance by stating, “the nature of the ‘emergency’ posed by al Qaeda ‘takes matter out of the realm of ordinary crime control’” (U.S. Newswire, 2006). The key difference here is that the Sedition Act was repealed two years after World War I, but President George W. Bush explained the war on terror would “not end until every terrorist group of global reach has been found, stopped, and defeated” (Power, 2007). The “war on terror” that shoulders the rationalization for government internet surveillance has no clear end 18 years after its declaration. This subjects the American people to governmental surveillance indefinitely.

**The Justification… Or Lack Thereof for Surveillance**

The ability to stop a catastrophic event like 9/11 with the use of such surveillance may seem to justify collecting personal information by the U.S. government; however, evidence for the effectiveness of such a program is lacking. In 2013, a Senate Judicial Committee chairman, Patrick J. Leahy, revealed the lack of added safety as a result of Prism. Senator Leahy stated, “not dozens or even several terrorist plots” had been successfully disrupted with the program (Savage & Sanger, 2013). The lack of positive results from the Prism program makes it difficult to support when also considering cost and public perception. According to the leaked slides produced by the former NSA contractor, Edward Snowden, the US intelligence “black budget” for 16 spy agencies was $52.6 billion (Szoldra, 2016). In addition, the NSA was found to be paying hundreds of millions of dollars annually to US companies for access to their networks (Szoldra, 2016).

The United States spends more on the military than the next seven greatest spenders combined (Simmonson, 2018). The budget for these types of operations are funded by taxpayer dollars, and the United States remains the world’s largest spender -- accounting for over a third of global military expenditure (Simmonson, 2018). The extravagant amount of money spent without substantial results could be used elsewhere. The United States ranks 27th in the world for its levels of healthcare and education, and government investment in these sectors has not changed over the last three decades (Bendix, 2018). Allocating more of the military budget to health and education could help America regain respectable the world rankings that it once held.

**The Private Sector Side**

The government use of American internet data and information is concerning, but it is the U.S. private sector that is responsible for the initial collection. The Guardian reported, “google creates an advertisement profile based on your information, including your location, gender, age, hobbies, career, interest, relationship status, possible weight and income” (Curran, 2018). The leaks by Edward Snowden revealed that Google was one of the nine companies working with the NSA Prism program, which is to say that the government may also have access to such information. The U.S. government relies on the large scope of data from companies like Facebook, Google, and Microsoft. This data collection is agreed upon by the consumer with contractual terms and agreements on internet websites; however, the consumer may lack knowledge that it is also being used by the government.

Tracking via cookies by online companies is used to tailor pages, offers, and prices to the behavioral characteristics of the individual shopper (Alreck & Settle, 2007). There is a lack of knowledge by the buyer about how this collection of information may be used (Dinev, Hart, & Mullen, 2008). This lack of knowledge ill-equips the consumer to recognize when and what they are agreeing to in terms of privacy. Consumers need this knowledge when deciding to buy a product. Wearable technology can collect data that could potentially be hacked and sold to insurance companies, resulting in higher prices for insurance. It could also be used to convict a consumer of murder. A man in Connecticut was charged with murder based on the evidence found on his wife’s Fitbit heartrate monitor (Hauser, 2017). The use of such evidence can be unknowingly agreed to because of purposefully confusing terms and agreements made by the company.

The information recorded by consumers is considered a contractual agreement between the customer and the company (Swire, 1997). One of the main issues with the “contractual agreement” is that the customer may incur significant costs in effort to learn and understand the company’s privacy policies one is agreeing to (Swire, 1997). The terms of agreement a user is required to adhere to in order to use a product or service like Facebook would require multiple hours to read and a background in contractual law to fully comprehend the material. One could argue that this is in violation of the Federal Trade Commission’s Consumer (FTC) Protection Laws. Section 5 of the FTC, “prohibits unfair or deceptive acts or practices in or affecting commerce” (FTC, 2016). Acceptance of these terms and agreements to data collection are required to function in today’s society. A student must agree to Microsoft’s terms in order to access their Syracuse University’s email account. The student is forced to comply to Microsoft’s data collection in order to receive emails in regard to class, which could be interpreted as “unfair” in Section 5 of the FTC laws

**Policies, the Future, and Conclusion**

Policies are needed to ensure that the American citizen is not being taken advantage of by online companies and the government. The European Union has been spearheading privacy laws for its citizens with the GDPR. The GDPR website self-proclaims to be “the most important change in data privacy regulation in 20 years”. This regulation gives EU consumers control of their data and the use of their information. This law requires contractual consumer consent information for data collection to be condensed without the use of illegible terms. The GDPR gives consumers the right to access their data and also the right to have it erased. Ideas from these new laws have started to cross the Atlantic Ocean to America. Recently, California passed a digital privacy law granting consumers more control and insight into the spread of their information online, which may spearhead much needed legislation for America (Wakabayashi, 2018). Policies like these not only protect the consumer, but they also ensure fair agreements between company and user.

Policies to protect consumers online are needed, and it is difficult finding the balance when views differ in regard to security and surveillance. “American citizens were willing to support a surveillance program if they believed it was intended to protect them… when the same question was asked, but stripped of any mention of terrorism, the majority of the respondents said they disapproved” (Dinev et all, 2007). Society is changing with technology. Public and private boundaries are becoming increasingly unclear, and it may be impossible to take back what has already been made public online through policies like “the right to be forgotten” (Garcia-Murillo & MacInes, 2018). Educating the public about internet privacy and how their actions online impact daily life is a necessity moving forward. Large internet companies have created access and convenience in the modern world but not without a price.

Word Count: 1578

References

Alreck, P. L., & Settle, R. B. (2007). Consumer reactions to online behavioural tracking and targeting.*Journal of Database Marketing & Customer Strategy Management, 15*(1), 11-23. doi:http://dx.doi.org.libezproxy2.syr.edu/10.1057/palgrave.dbm.3250069

Bendix, A. (2018, Sep 27). The US was once a leader for healthcare and education – now it ranks 27th in the world. *Business Insider.* Retrieved from <https://www.businessinsider.com/us-ranks-27th-for-healthcare-and-education-2018-9>

Brinkley, A. (2006) Civil Liberties in Times of Crisis. *Bulletin of the American Academy of Arts and Sciences, 59.* 26-29. Retrieved from https://www.amacad.org/publications/bulletin/winter2006/brinkley.pdf

Curran, D. (2018, Mar 30). Are you ready? Here is all the data Facebook and Google have on you. *The Guardian.* Retrieved from <https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy>

Dinev, T., Hart, P., & Mullen, M.R. (2008). Internet privacy concerns and beliefs about government surveillance. *Journal of Strategic Information Systems, 17*(3), 214-233.

Federal Trade Commsion. (2016). Big Data: A Tool for Inclusion or Exclusion?. Retrieved from <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>

Garcia-Murillo, M. and I. MacInnes (2018). "Così Fan Tutte: A better approach than right to be forgotten." *Telecommunications Policy* 42(3): 227-240.

Greenwald, G. & MacAskill, E. (2013, Jun 7). NSA Prism program taps in to user data of Apple, Google, and others. *The Guardian.* Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Hauser, C. (2017, Apr 27). In Connecticut Murder Case, a Fitbit Is a Silent Witness. *New York Times.* Retrieved from <https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html>

Janbek, D., & Williams, V. (2014, Spring). The role of the internet post-9/11 in terrorism and counterterrorism.*The Brown Journal of World Affairs, 20*, 297-308. Retrieved from https://search-proquest-com.libezproxy2.syr.edu/docview/1649692616?accountid=14214

Justice department: NSA program to detect and prevent terrorist attacks: Myth v. reality. (2006, Jan 27). *U.S.Newswire* Retrieved from <https://search-proquest-com.libezproxy2.syr.edu/docview/451162627?accountid=14214>

Power, S. (2007, Jul 29). Our war on terror.*New York Times (1923-Current File).* Retrieved from <https://search-proquest-com.libezproxy2.syr.edu/docview/848056034?accountid=14214>

Simonsson, L. (2018, May 01). Study: US, china and saudi arabia biggest military spenders in 2017.*DPA International (English)* Retrieved from <https://search-proquest-com.libezproxy2.syr.edu/docview/2033014319?accountid=14214>

Swire, P. (1997). Markets, self-regulation, and government enforcement in the protection of personal information. In Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce.

Available online at <https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy> OR <http://dx.doi.org/10.2139/ssrn.11472>

Szoldra, P. (2016, Sept 16). This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks. *Business Insider.* Retrieved from <https://www.businessinsider.com/snowden-leaks-timeline-2016-9>

Wakabayashi, D. (2018, Jun 28). California Passes Sweeping Law to Protect Online Privacy. *New York Times*. Retrieved from <https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html>