Jacob Dineen

Information Policy

6/3/2018

Reading Reflection Privacy and Security

In Nishita and I’s debate writeup, we, by design, countered any benefits to the explicit mass surveillance on the American population as government overreach, and the marginalization of personal privacy in favor of security. That assignment focused more on the curtailment of privacy in a library setting, while this will emphasize a broader paradigm. Approaching an issue with the intent to disregard any notions of benefits, instead only focusing on costs, is a somewhat dangerous, one-sided view to take regarding any piece of legislation – Such is the landscape of our political climate in the U.S. A reasonable individual is one who researches and analyzes both sides of an issue, and doesn’t just appeal to confirmation bias. Here, we will focus on both the advantages *and* disadvantages of the collection of personal identifiable information at both the government and private sectors, specifically weighing the tradeoffs between U.S. civil liberties and the need to protect our vital infrastructure and the lives of American citizens.

I’ll first start with the disadvantages, noting some of my points from the past assignment. Namely, we mention violations of basic civil liberties and the US Constitution, specifically noting disintegrations of probable cause and illegal search and seizure of personal information. Referencing back to the Solove journal, the ‘nothing to hide’ position crumbles when we talk about chilling effects brought about by government impositions – When people know that they are being monitored, or their data is being collected, they will deviate from their natural intellectual curiosity. If people are deprived of the obtainment of knowledge, we, as a country, might face economic implications as well as unintentionally enforcing uniformed political views [1]. The latter argument is referred to as the suppression of dissent, where a more powerful entity might act to oppress point of views, directly or indirectly [2]. When opposing opinions are stripped from a conversation, we essentially work to eliminate the checks and balances system of political opinion, which could lead to dangerous political regimes. Also, we must think about the rising role of machine learning and the dangers of misclassification at a grand scale, particularly for terrorist identification. Any false positives of any kind might unintentionally trigger unjust suspicion and overgeneralize a person’s digital footprint as being something other than it truly is [4]. In short, before getting into the actual storage and use of the data, the counterpoint to the above disadvantages is the safety of the general population. If there are behavioral and economic patterns that can be exposed to help in the tracking and detainment of enemies of the state, no matter how the information was/is obtained, the ends might justify the means. It’s relatively easy to mitigate the importance of safety when you aren’t personally the one in harm’s way, and I think that’s where the issue arises. We aren’t necessarily being asked/required to sacrifice our personal privacy for the promise of personal security, we are being asked to render our own personal information to protect the notion of the greater good, an overarching hierarchy. This ties back into one of the earlier modules that dealt with showing empathy and action based on proximity.

Getting more into the readings from this week, particularly the Swire journal, we can start to look at how data collection is happening, how it is regulated, and how it is protected across the different sectors. As the Cambridge Analytical situation scandalized Facebook, America got a firsthand look at the institutional solutions promulgated at the private sector, notably market-regulation in Facebook’s case. Market-regulation works at the private level, theoretically, because companies that are reliant on their consumers for their bottom line and are less likely to intentionally or unintentionally violate their trust [3]. The other institutional solution is one that is regulated by government entities and enforces laws and regulation that act to deter abuses and promote the security and privacy of their users. Zuckerburg’s ‘testimony’ on Capitol Hill was mainly countered by congress as being a failure for Facebook to market-regulate, and opened the door for more government interjection moving forward – Not just for Facebook, but for large conglomerates that benefit directly from consumer data. There are benefits and downfalls to government and market regulation – Market regulation is often the result of firsthand knowledge of consumer preferences, dynamically adapting per both parties, while government regulation is more set in stone, enforcing legal penalties and allowing violated parties to take action against the opposing party [3]. One issue with market-regulation is the idea that is nearly impossible for an individual consumer to understand, implicitly, a company’s privacy policy. Even harder it is for them to be able to monitor and identify wrongdoing, eg.. a company selling personal information to a third party against the contractual setting that they abided to upon commencement of service. Much of this was related to market-regulation, but we now move toward government-regulation. One of the main failures of government-regulation is incurred costs, especially costs directed at the American taxpayer to uphold regulatory activities/agencies. There are also costs imposed at the private level, mainly centered around ‘compliance costs’ [3]. Another issue arises when an outside party is directed to conduct/impose regulations – They are often under-armed in the domain knowledge of a setting and regulations are either hyper specific, or too broad, leaving way for loopholes. While each set of regulations has its benefits and pitfalls, I personally think that government regulation in private affairs might be an overreach, and the market regulation system, based around the court of public opinion, seemingly works to deter direct violations of consumer privacy. As we saw Facebook stock plunge after the revelations, we also saw a substantial effort for them to shift tides in terms of privacy, and a lot of competitors and adversaries in the internet realm followed suit. The consumer hit them in their bottom line, and this seemingly enacted change without government interference. Time will tell if change was truly enabled.

If I had to say who’s rule I’d rather follow with regulation, in reference to which sector, I would say the government. Most private companies operate with a business plan that centers around consumer data, and the dissemination of that information for profit. The government, while sometimes overtly ignorant to transparency, should be tasked with upholding a higher standard for the collection, storage, and transference of data at all levels. While the cost to the American taxpayers will be monetarily greater, the ensuing comfort of knowing that they could directly hold a company responsible for breaches of their contractual obligations is important. People look for someone to blame and hold accountable when things go wrong, and they would likely willingly do so at the expense of some of their tax dollars. Self-regulation is also an option, driven by domain expertise an ever-present awareness of a respective target audience, but is countered, in part, by the idea that a company may not desire to regulate if it explicitly targets their bottom line – They may instead let other companies organize the efforts and incur the cost [3]. Personally, I don’t believe there is enough accountability brought about by self-regulation, and would much prefer markets or governments driving change under the threat of financial or legal repercussions.

To protect policy, I think that contractual agreements should be made clear and legible for prospective customers, rather than being muddled in vagueness and legal jargon that deters from readability. The market-regulation landscape often fails in adequately informing consumers on what exactly they are giving up to gain access to a service. It should however be noted that the FTC works to protect American consumers, specifically as it relates to ‘unfair and deceptive acts and practices in or affiliating with commerce... the agency also enforces other federal laws relating to consumers’ privacy and security’ [5]. I still believe that the most effective change is driven by the consumers themselves. If journalists continue to expose unethical practices of violations of consumer privacy, it is the responsibility of American citizens to band together and hold those institutions responsible, financially, for their wrongdoings.

\*Professor, had some trouble delineating exactly what the prompt was asking for on this assignment. I believe I covered each of the questions to some extent.

References

**[1]**S., & J., D. (2007, July 12). 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. Retrieved from <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565>

**[2]** “Suppression of Dissent: What It Is and What to Do about It.” *Ecofeminism and Globalism*, [www.uow.edu.au/~bmartin/dissent/intro/DNAleaflet.html](http://www.uow.edu.au/~bmartin/dissent/intro/DNAleaflet.html).

[3] Peter. “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.” *Redirecting*, Hindawi, 15 Aug. 1997, dx.doi.org/10.2139/ssrn.11472.

**[4]**Christian Grothoff & J.M. Porup. (2016, February 16). The NSA's SKYNET program may be killing thousands of innocent people. Retrieved from <http://arstechnica.co.uk/security/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people>

[5] “Enforcing Privacy Promises.” *Federal Trade Commission*, 2 May 2018, www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.