Marcus Rosti

Prof. Johnson

DS 6002

Oct. 28th 2015

The End of Privacy

A divide exists in the concept of privacy in that people treat physical privacy as more sacred than digital privacy. Internet forums usually burn over issues of privacy but outside of that we see people blindly giving away information digitally. Even Senators and Representatives see digital information as just a thing collected with no inherent value but looking into a neighbors mailbox is a felony. People do not want strangers peaking into their bedroom, but they can close the door or shade the windows. It is society's responsibility to enact proactive laws to defend digital privacy from government and private agents in the way we defend physical privacy.

The dangers of surveillance are much easier to outline in respect to the values of privacy. A surveillance state puts government in a position of power to exercise its control selectively and exert undue justice. That creates division between those surveilled and those in power to surveil. In this state, a government has a blank check on its entire populace for coercion and selective enforcement of laws (Richards). Privacy, however, defies positive affirmation. To put it simply, people want agency over their information. Prof Vaidhyanathan framed the value of privacy as maintaining positive contextual integrity. People should be given the ability to define what context information is viewed (Vaidhyanathan). The lack of good, defendable definitions of privacy and inadequate digital privacy laws have eroded our digital contextual integrity and only proactive legislation can equate digital and physical privacy.

The major difference between physical and digital privacy is the ease with which digital information is collected and the ability to analyze that information nearly immediately. Legislation typically lags behind innovations but in this case it seems our society has lagged behind as well. Historically, the collection of information was a very involved process. The US census requires every person receive a form, to fill it out taking nonzero effort which the census office collects and inputs the data by hand with lengthy. This type of data collection allows the individual the agency to control what data they give. Filling out the form and mailing it

back is a form of active consent the individual has total control over. Today in the online world, most forms of data collection occur passively and more obliquely in secret. Burying implied consent in the terms of service allows companies to discreetly collect every piece of information their users produce. They can collect credit card purchases, every webpage viewed, and every post and message exchanged on their platform. Extracting information from this data had no active consent or even the persons knowledge of how this data was used.

Vaidhyanathan described this as the cryptopticon or a hidden panopticon. The real danger of surveillance lies in their hidden uses. He outlined effectively the devious nature of these systems and how we openly accept the benefits i.e. Netflix recommendations or the security the government can afford. However, he points out that these recommendations can create a bubble of agreement and homogenize our opinions to match those of our peers. He also used the example of the closed circuit television implemented after the IRA attacks in London which did not even go into effect until after the end of the IRA and has had no prevention or capture of crime within London (Vaidhyanathan). This shows how people have normalized passive collection and allowed what was hidden come into public view and just accept it.

Big data erodes contextual integrity and gives power to those that wish to extract information with it. Predictive analytics does not allow people to control the context of their information. Companies and the government use analytics to narrow down your future choices into a few options, so that they can predict actions to either monetize them or to exert some control over them for crime analytics for example. People who employ this new technology use it from a stance of presumption. Analytics comes to a conclusion without considering the due process of what the individual data points mean (Kerr and Earle). Privacy protects society from the potential abuses of big data. It allows people to take back their agency and prevent firms or governments from using it in a way they deem negligent.

It is with these considerations that we need to declare firm laws and precedent against using data with out the informed and positive consent of those on which it is used. The US constitution explicitly forbids violations of physical privacy, and it should afford the same rights to digital privacy as well.

Works Cited

Kerr, Ian and Earle, Jessica. "Prediction, Preemption, Presumption." *Stanford Law Review.* Vol 66. 3 Sept. 2015. Web. 1 Nov. 2015.

Richards, Neil M. "The Dangers of Surveillance." *Harvard Law Review*. Vol 126. May 2013. Web. 1 Nov. 2015.

Vaidhyanathan, Siva. "Privacy Ethics." DS 6002. Charlottesville Va. 11 Oct. 2015. Lecture.