Khayyam Saleem

Professor Michael Kowal

HSS 371EV – Computers and Society

15 October 2017

Privacy vs Freedom

The liberties of the American citizen have always been a topic of deliberation and enumeration. Formally yet abstractly listed in the Constitution, we have certain "inalienable rights," a reward we reap in return for compliance with the government of and maintaining membership in the United States of America. Among these rights, we have some that are concrete and relatively unambiguous: the freedom of speech, the right to bear arms, right to a speedy and public trial, etc. However, we also have quite a few unenumerated or implied rights. Since the Constitution and the Bill of Rights are so open to interpretation, the unenumerated rights we have are often contested. One of the most controversial, as of late, has been the right to privacy. In general, we tend to agree that we DO have the right to privacy, provided that the maintenance and protection of an entity's privacy does not infringe upon the maintenance and protection of national security or the rightful upholding and enforcement of the law. This boundary, however, is a difficult one to assess; so difficult that it almost necessitates the questions: in what scenarios can government compromise individual privacy for the sake of national security, what governing body gets to make that decision, and what can we do to ensure that this is not being abused? As important as national security is, we absolutely must respect the implied rights to privacy that the Constitution allows us, lest we face the repercussions of a dystopian society imagined (or perhaps foretold) by the likes of George Orwell or Ayn Rand.

The Constitution and the Bill of Rights is the primary source of our implied right to privacy and information security as American citizens. Given that we have trusted, protected, and honored this document for as long as our country has lived, we should understand that it is a living, breathing document, whose interpretations and stipulations will vary dependent on the temporal and societal context. In and around 1792, the representation of privacy that could be

afforded to people was that they should be able to enjoy the sanctity of their own homes without being subject to an illegal search and seizure of property. Today, we have a different representation of "property." Several amendments do imply the right to privacy. The first amendment allows us the privacy to our own beliefs. The third amendment grants us dominion and privacy in our own homes. The fourth amendment allows us privacy over our person and property, protecting us from unlawful search and seizure. Lastly, the most important implied right comes from the fifth, that shields us from being compelled to self-incriminate, or alternatively, gives us personal privacy over our information. Today, a digital photo is property. An email is property. The contents and data in an iPhone are property. If we allow for the aforementioned liberties to be taken away from us, we invite more and more picking of fruit from the poisoned tree. If we are to hold the stipulations of the Bill of Rights in the same regard as we always have, then we have to acknowledge these new definitions and acknowledge that these are also protected by that same document. Hence, a supporting argument to value and protect individual privacy is that the Bill of Rights we swear by agrees.

One might argue that if we are to use the temporal context of the Constitution in our favor, we must also acknowledge the analogous competition: modern national security threats. With modern terrorism, widespread access to semi-automatic weapons and explosives, and other advances in the violent sciences, we are under the impression that our national security is threatened from unaffiliated individuals with strong agendas, now more than ever. We are under the impression that, with the Patriot Act and other national security measures implemented since the 2001 wake-up call, we are safe and the government has done its part. However, the statistics disagree. "Security theatre" is a concept that has come about to describe the illusion of security that measures such as more invasive TSA screenings provide. In reality, since 2004, the Government Accountability Office has confirmed that 16 individuals accused of involvement in terrorist plots have flown through US airports 23 times since 2004, completely undetected by TSA behavior detection officers (Keteyian, 2010). Full-body scanners at TSA security checkpoints were supposed to protect the nation's travelers from terror attacks, and perhaps they

do deter attacks and discourage would-be terrorists from attempting to bring weapons on planes, but this comes at the cost of every single passenger's individual privacy. On top of that, fear-mongering by the government has brainwashed individuals into thinking that this is necessitous; that it is for the greater good. Even if these measures genuinely protect our citizens, is it right for the government to use fear as a tool to push their agenda?

Perhaps the biggest offender in stripping the American populace of their right to personal privacy is the NSA. From the NSA's website: "In the past, we used our close partnership with the FBI to collect bulk telephone records on an ongoing basis using a Top Secret order from the Foreign Intelligence Surveillance Court (FISA). The metadata we collected from this program gave us information about what communications you sent and received, who you talked to, where you were when you talked to them, the lengths of your conversations, and what kind of device you were using." Statistics report that the NSA collects and stores almost 200 million text messages a day globally (Mardell, 2014). They store data about international payments, social network communications, browsing activity, and more (SPIEGEL, 2013). Perhaps worst of all, by Section 215 of the Patriot Act, the government may compel companies to hand over information and create backdoors to allow their surveillance to continue. The claim is that all of this information is in pursuit of foreign intelligence and national security, and that the rest of the data is expunged or held highly secure. But what if the NSA makes a mistake, and all of this data is leaked or released? It is definitely not outside the realm of possibility, considering famous instances of internally sourced NSA leaks have happened before! With the case of Edward Snowden, we saw just how much of our liberties were being surreptitiously taken away from us, and based on the outlash from government against Snowden and the ensuing manhunt, they certainly did not want to reward such behavior: behavior that finally let the citizens of the United States out of the dark, and exposed them to the vices of big data and the true exploitation of modern technology and modern fear.

Protection of our individual privacy does not have to be at the expense national security. Invasive domestic surveillance, without probable cause or reasonable suspicion, is unambiguously

a violation of the rights granted to us by the Constitution and its modern-day implications. With the cost of data storage decreasing, and technological means of data collection increasing, we cannot expect for the abusive collection of our data to slow or stop without explicitly making it clear that we are aware of the violation of our rights and refuse to let it persist. Through whistleblowers, outspoken citizens, and well-intentioned businesses, we have been able to make strides toward the protection of our data from unlawful pervasion by government officials. National security should not come at the cost of personal liberty, and so long as we allow the fear-mongering to continue and allow ourselves to be deluded by talks that it is all "for the greater good," we will never be able to have control or security over the personal property that is most near and dear to us today: our information. However, the question of whether or not it is all worth it, or for the greater good, is contestable on both sides. Until the matter has been resolved, and a consensus that balances morality, individual privacy, and national security can be reached, we should not let it continue.

Works Cited

Mardell, Mark. “Report: NSA ’collected 200m texts per day’” *BBC News*. BBC, 17 January 2014.

SPIEGEL. “NSA Spies on International Payments” SPIEGEL.de. 15 September 2013.

UMD.edu, “START: American Deaths in Terrorist Attacks” *UMD.edu* October 2015.

Keteyian, Armen. “TSA’s Program to Spot Terrorists a $200M Sham?” *CBS News*. CBS Networks, 19 May 2010.

Office of the Press Secretary, “Statement by the President on the Shootings at Umpqua Community College, Roseburg, Oregon”. *Archives.gov* ObamaWhiteHouse. 1 October 2015.