

George Gordon

ENG 1710

Professor Robert Leston

October 23, 2015

Privacy Concerns

Privacy has been lost. Swept up under the defense of “National Security,” or forgotten and ignored by the public who flock to join any new social media site or uploading their files to the so called “cloud.” Corporations are easily making millions off our stripped privacy rights, along with the government with the NSA. They able to track us through our phones, target specific advertisements to us for profit and learn just about anything about us. There needs to be serious discussion and actions brought forward to protect privacy, something that is virtually nonexistent in today’s modern age.

Financial Aspect. After 9/11, the National Security Agency (NSA) began to hire private contractors to help sift through the tremendous amount of information they would be collecting. Among these contractors was Booz Allen Hamilton, a private consulting company worth around \$5 billion annually. \$1.3 billion of that comes from major U.S intelligence agencies according to Bloomberg Business. This company had gone relatively unknown for many years until Edward Snowden came along and exposed government surveillance secrets. Not only was Booz Allen making serious profit from the U.S Intelligence budget but, according to Tim Shorrock’s *The corporate takeover of U.S Intelligence*, 70% of the U.S Intelligence budget goes directly to private contractors.

Shorrock names Booz Allen, The Science Applications International Corporation, Northrop Grumman, and Narus as some of the contractors hired by the NSA. If 70% of the budget for the NSA is going into contracting, with an \$8 billion budget, around \$6 billion must be going into NSA contracting alone. With \$42 billion going into intelligence contracts as of 2005, which is significantly more than the \$18 billion that was spent back in 1995. A government intelligence officer is estimated to make \$126,000 annually, however, an intelligence contractor would be paid around \$250,000 annually. Then we have RSA Security who were paid \$10 million to provide a backdoor for the NSA in its security (Blaze). Which, if someone other than the NSA could figure out would mean a massive security breach for the U.S. Russell Goldman in *The Secret History of NSA Contractors*, described it as “Like contracted mercenaries hired to fight the wars in Iraq and Afghanistan, intelligence contractors were given access to government information and resources.”

In 2012, the Direct Marketing Association reported “the data-driven marketing economy added \$156 billion in revenue to the U.S. economy and fueled more than 675,000 jobs” (Bachman). Due to practically every company collecting data on its customers and using that data to direct advertisements towards consumers or target specific audiences. Google tracks your searches and emails through Gmail and by analyzing this data creates specific ads for you. Most of Google’s revenue comes directly from these advertisements, with \$36.5 billion coming from advertisements in 2011. Even Facebook is estimated to receive \$75 billion off of advertisement revenue alone.

In the article, *Carriers Sell Users’ Tracking Data in \$5.5 Billion Market*, details how phone companies are tracking our locations, web surfing and apps to sell to third party companies. With companies like Verizon Wireless and Sprint Nextel Corp. making \$5.5 in 2012 and it is reported that this figure will increase to \$9.6 billion by 2016. Even pharmacies and hospitals are selling patient records and prescription information for up to \$10 billion (Robertson). Selling personal data has become a huge market with it expected to become a \$48.3 billion market by 2018 with \$600 billion of additional value each year (Oak). By tailoring ad campaigns based off our web history, by selling our personal data, by surveilling our conversations and movements, by basically stripping us of our right to privacy, corporations make the big profits.

Privacy Issues. Due to the leaks provided by Edward Snowden we were able to see how surveillance is going on. “The leaks led to revelations of dragnet phone metadata surveillance, the same for email until 2011, subversion of encryption technology, spying on porn habits of persons of interest, monitoring of the phone calls of world leaders, hacking of tech companies” (Hill). With two G20 summit meetings in 2009, attended by many foreign politicians, having been monitored and having phone calls intercepted (MacAskill). However, this isn’t limited to just the U.S. According to WikiLeaks, “Surveillance companies like SS8 in the U.S., Hacking Team in Italy and Vupen in France manufacture viruses (Trojans) that hijack individual computers and phones (including iPhones, Blackberries and Androids), take over the device, record its every use, movement, and even the sights and sounds of the room it is in.” As well as, the citizens of Egypt and Libya discovering listening rooms that could be traced to the UK, France, South Africa and China monitoring internet history and phone calls.

Then we have cases like how the retailer Target tracks what customers are buying or looking at through a guest ID they assign you. Using this information, they are able to send your specific coupons or booklets. Which leads to how a Target managed to find out a young girl was pregnant before her own father was. Since they can track and notice specific patterns across women who are pregnant, they

began to send coupons to the family for cribs and diapers. This outraged the girl's father who complained to the store believing Target was encouraging his daughter to have sex. However, after speaking to his daughter, he found out she was indeed pregnant (Hill). Rather disturbing to know that a retailer can know things about you or your family before even you do. But Target isn't the only retailer or company that is doing this either. Multiple retailers and websites are tracking what you look at or purchase to tailor what types of ads you will see.

However, it's not just the government and corporations that invade our privacy, it is the public doing it to each other, take the iCloud data celebrity breach for example. iCloud being an Apple service that allows users to store and backup their pictures, files, and videos. It's a service most people find convenient and useful but in this case, a group of people were able to get into iCloud services and release the private pictures of notable celebrities (Lewis). Many of these photos were naked pictures these people had taken of themselves and were now up on the internet for everybody to see. Due to this scandal, many of the celebrities worked with the FBI to find those responsible for leaking the pictures as this was huge invasion of their privacy (Duke). However, these types of stories of people having their private photos leaked online are a common place on the web.

A boyfriend or girlfriend is broken up with and because they still have nude pictures of their ex in their hands they upload them to the internet as revenge. This act is being called revenge porn and has become a rather big privacy issue. With the founder of the Cyber Rights Initiative, Holly Jacobs, reported about 1000 cases of revenge porn were brought up to her back in 2013, however, many more must go unreported. Most states don't have laws in regards to these actions and people are freely allowed to go uploading pictures of their exes onto the internet with no repercussions. California passed a law that made revenge porn a misdemeanor, however, it contained a loophole which made around 80% of revenge porn cases totally legal (The New York Times). A Redditor by the name of TastyJams, asked people to share their stories about how revenge porn has affected their lives. With one woman reporting she had to quit her job, another being body shamed and humiliated, and another having to worry about her own personal safety after a video of her was leaked online (Bahadur).

Or we have cases of social stalking, where we may meet someone and we can find out almost a huge amount of information about them through the internet. Or take the amount of fake websites online waiting to steal your identity or the scammers waiting to steal your money. Which is why a number of people are afraid of putting their credit card or contact information online. Even when websites promise our information is protected they are still vulnerable to hackers. Look at the Ashley

Madison scandal where a group of hackers were threatening to reveal the names of the users of this infidelity website and they eventually did (Feinstein). Hackers are persistent and they will find ways to get information that is held private by websites if they are so inclined. We aren't hidden, our information is out there for everyone to see or being monitored and it's easily compromised and accessed.

What can we do about Privacy? We would need to start by bringing awareness to this issue and having people care. In an episode of Last Week Tonight with John Oliver about government surveillance, he brought up a congress meeting on the topic of the patriot act. It was to allow the public come and discuss issues or concerns relating to the act, however, only three people showed up. Edward Snowden leaked the NSA surveillance information but the public didn't care or even know about it. We could try putting this information in easily accessible places online for people to get involved or through artwork placed around the city which can get people talking. We can protest retailers and websites to deter them from monitoring us. If we all get together and choose to stop going to or using these places, it will hurt their bottom line and be forced to give in to our demands.

Perhaps a more direct and risqué way, where we could show easily people are being tracked and monitored by their devices or exposure to the internet. Rounding up groups of people and emailing them information about themselves that will show how easily someone can get their hands on it because it's already accessible to corporations and the government. Going so far as using people as examples could bring people together and discussing the issue at very least. People won't care if they don't experience the situation firsthand, so, we need to show them how vulnerable and exposed they really are.

Or through the creation of organizations such as, The Cyber Civil Rights Initiative, which is aiming to help victims of cyber abuse and educate the public on this topic. Having organizations dedicated to protect our privacy right and combating the exploitation of said right even if the majority of the people do nothing. One of the major issues with privacy is that there are no specific laws on privacy. Nowhere does it say that we are legally allowed privacy, however, it's a given that this something we should have. We would need to get the government to pass laws that will protect our privacy, that can forbid or, at least, limit the amount of surveillance that is placed on us. While there are safety concerns, there has to be a line where safety can no longer protect our invasion of privacy but we must also be willing to compromise some privacy for the sake of safety.

Conclusion. The way our privacy is being handled by ourselves, corporations, and the government, we are reaching the point where privacy will be a thing of the past. We may eventually have a world in which every single detail of our lives will be common knowledge. The biggest issue with privacy being the lack of care by the public. The government and corporations are easily allowed to do all these things either unknowingly to us or because we allow them to do it. As well as, instilling the value of privacy in ourselves and stop things like revenge porn or hacking into our accounts to steal our information and identities. We need to bring not only awareness, but to convince people that privacy is an important right that we should discussing. No more “who cares” comments. Or we can sit here doing nothing and embrace our new panopticon world.

Works Cited

- Bachman, Katy. "Big Data Added \$156 Billion in Revenue to Economy Last Year [Updated]." *AdWeek*. Web. 25 Oct. 2015.
- Bahadur, Nina. "Victims Of 'Revenge Porn' Open Up On Reddit About How It Impacted Their Lives." *The Huffington Post*. TheHuffingtonPost.com. Web. 25 Oct. 2015.
- Bennett, Drake, Caroline Savello, and Robert Levinson. "Chart: How Booz Allen Hamilton Swallowed Washington." *Bloomberg.com*. Bloomberg, 13 June 2013. Web. 25 Oct. 2015.
- Blaze, Matt. "How Worried Should We Be About the Alleged RSA-NSA Scheming?" *Wired.com*. Conde Nast Digital. Web. 25 Oct. 2015.
- Duke, Alan, Catherine Shoichet, Faith Karimi, Bill Mears, Dan Simon, Rachel Wells, Dave Alsup, and John Sutter. "FBI, Apple Investigate Nude Photo Leak Targeting Jennifer Lawrence, Others." *CNN*. Cable News Network. Web. 25 Oct. 2015.
- Feinstein, Amy. "Thousands Of DC Users Of Ashley Madison Find Out The Internet Is Not Secure." *The Inquisitr News*. Web. 25 Oct. 2015.
- "Fighting Back Against Revenge Porn." *The New York Times*. The New York Times, 12 Oct. 2013. Web. 25 Oct. 2015.
- Goldman, Russell. "The Secret History of NSA Contractors." *ABC News*. ABC News Network, 10 June 2013. Web. 25 Oct. 2015.
- Hill, Kashmir. "How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did." *Forbes*. Forbes Magazine. Web. 25 Oct. 2015.
- Hill, Kashmir. "The Biggest Privacy Stories of 2013." *Forbes*. Forbes Magazine. Web. 25 Oct. 2015.
- Kharif, Olga, and Scott Moritz. "Carriers Sell Users' Tracking Data in \$5.5 Billion Market." *Bloomberg.com*. Bloomberg. Web. 25 Oct. 2015.
- MacAskill, Ewen, Nick Davies, Nick Hopkins, and Julian Borger. "GCHQ Intercepted Foreign Politicians' Communications at G20 Summits." *The Guardian*. Web. 25 Oct. 2015.
- Oak, Robert. "The Economic Populist." *This Big Business of Big Brother*. Web. 25 Oct. 2015.
- Robertson, Jordan. "States' Hospital Data for Sale Puts Privacy in Jeopardy." *Bloomberg.com*. Bloomberg. Web. 25 Oct. 2015.

Shorrock, Tim. "The Corporate Takeover of U.S. Intelligence." *Saloncom RSS*. Web. 25 Oct. 2015.

Shorrock, Tim. "Meet the Contractors Analyzing Your Private Data." *Saloncom RSS*. 10 June 2013. Web. 25 Oct. 2015.

"The Spy Files." *WikiLeaks*. Web. 25 Oct. 2015.

"iCloud Data Breach: Hacking And Celebrity Photos." *Forbes*. Forbes Magazine. Web. 25 Oct. 2015.