Development of government surveillance on the internet

Internet Survey Essay

George Orwell’s novel Nineteen Eighty-Four showed the public a dystopian universe where the government had complete control and surveillance over the masses. Although this concept seemed farfetched at its publication, which preceded the title’s year by thirty-five years, it is almost parallel to the reality we are living today. After the events of September 11th, 2001, the public demanded more security. David Lyons states that in the years following the terrorist attack it has been increasingly common for the public’s civil liberties to dissolve and for the government to spy on the population, then collect and store that information. After the events of 9/11, the US government decided that the laws surrounding the internet did not keep up with the growth in technology and digital media and created the surveillance laws relevant to today. (Lyons, 2014). Although it may be reasonable to spy on the internet activity of a person of interest in a crime, this government practice is making the entire population people of interest. The internet enables too much surveillance as it strips the public of its basic right to privacy. This is clear when one examines the extent of the surveillance and the effects these breechings have had on our society. Who knew George Orwell was reading the future?

North Americans use the internet every day, and our entire lives are on our phones and computers. A report from the USC Annenberg Center for the Digital Future reported that the average American uses the internet 17. 6 hours per week. This extremely high amount of time online means we produce multitudes of data such as with whom we talk, where we are, what we post about, and what we buy. The government uses their relationships

with digital companies such as Facebook, Google, and Microsoft to extract even more information on us such as our emails, messages, search history, and other personal data (Venkatatdri, Giridhari). Even in cases when the surveillance does not capture incriminating evidence, it is still scary that there are databases full of information that could be used against people in the future. A decade ago, police had to have a legitimate reason to search a person. Now, police can flag you as suspicious based on your internet posting activity. In the words of Edward Snowden: “ During an arrest, police traditionally have had the ability to search anything they find on your person — if you had a note in your pocket, they could read it. But now we all carry smartphones on us… Your entire life now fits in your pocket.” With all of the new laws being put in place by programs such as the NSA (National Security Agency), and the FISA (Foreign Intelligence Security Agency), we are losing our right to privacy. The government should not have the right to have access to multitudes of data on the population. Electronic devices are personal items and anyone who is not the owner should not see their data.

Another way the government surveillance threatens our right to privacy is by tapping into laptop webcam cameras. This attacks our basic right to privacy by giving them the option to legally watch the public at any time, even in their home. Whistleblower Edward Snowden revealed an NSA program called Optic Nerve in 2014 that captured webcam images every five minutes from Yahoo video chats (Bauman, Zygmunt). A home should be a place of worry-free privacy and this is not possible knowing that you could be being watched. The way the government gets access to the webcam is the same process as illegal hacking. According to Marcus Thomas, the former assistant

director of the FBI OPT Division, the FBI uses “ the same technique as ratters, by infecting the computer with a malicious software – ‘ malware –through phishing.” This practice should also be outlawed as it is a complete breach of privacy. Behind closed doors, a human is meant to be out of the public eye. The thought that the government could be watching people doing things “ in the privacy of their homes,” such as changing clothes, gossiping, or other activities that merit privacy is disturbing. This malware is entirely unnecessary, and it is crazy that people need to worry about something so Orwellian.

A final way the internet has allowed surveillance has gone too far is GPS tracking. With apps like Find My iPhone, Snap Chat, and Maps, it is clear that iPhones have GPS features. Government agents can also use this feature as “ cell phones reveal your location, and companies want to retain and use that information… exploit it,” (Stanley, 78) There are arguments that this is unlawful as it can lead to unreasonable search and seizure as the information given about the location on the phone is not publicly available. The government argues back that if the device is used in the process of illegal activity, they should be free to track it. (Serwer, Adam). This is disturbing because it essentially states that if the government can do a form of surveillance, it should be free to do so. The government is capable of breaking into a house, or stealing a car; however, the fact that they can does not dismiss the expectation of privacy in a house or car. This opinion compares phone data to a witness description, or scent followed by a police dog or recalling a license plate number, but those things you observe by looking around, with phone data, it cannot be acquired without directly

trying, such as asking a phone company for a user’s location data. In the words of Catherine Crump, an attorney for the American Civil Liberties Union: “ It is just as invasive for the government to track you through your cell phone… because you have your cell phone with you 24 hours a day, people even sleep with them by their beds…If all the police have to do is track you through your phone instead of your car, then that doesn’t mean very much in terms of protecting Americans’ privacy.” This is a breach of human privacy as it attacks the expectation of privacy the public has.

Professor Xiaoxing Xi, a Chinese-American professor at Temple University in Philadelphia, is a prime example of what can go wrong with the level of surveillance the government uses. He was falsely accused of wire fraud and was arrested, called a spy for China in May 2015. Four months later, the charges were finally dropped as it was revealed that Professor Xi was only communicating with colleagues in China about Physics and had no connection to foreign agencies. The government alleged that Professor Xi had shared information about a “ pocket heater” device that violated an agreement he had made to keep it a secret. However, Dr. Xi’s emails “ concerned a completely different kind of technology and had nothing to do with a pocket heater at all,” (Parchment, Ryan). Because of Professor Xi’s line of work, his emails back and forth with his Chinese counterparts contained keywords that the NSA’s surveillance looks for. These words were taken out of context and Professor Xi was racially profiled and flagged as a possible foreign agent. According to Parchment, Dr. Xi was subjected to the same racial bias and discrimination as several other innocent Chinese-Americans who were wrongly pursed and prosecuted. The level of power

internet surveillance gives the government over us is frightening. The fact that the government incriminated him using nonsense data, tried to cover for themselves by lying about the pocket heater, and racially profiled him is simply inexcusable and should not be legal. According to the Foreign Intelligence, “ Section 702 of the Foreign Intelligence Surveillance Act authorizes the Intelligence Community to target the communications of non-U. S. persons located outside the United States for foreign intelligence purposes. A key anti-terror tool that has helped to thwart numerous terror plots.” Although the government does not “ target” residents for internet surveillance with the Section 702 law, nevertheless, they rely on this surveillance to in bulk collect the electronic communications of innocent Americans who contact international people (Bazan, Elizabeth). Today, even after the charges being dropped, Professor XI’s reputation is tainted. He lost his job at the school and has trouble finding work in the academic community. Innocent people are being caught in the crossfires of plot bigger than their internet activity. Professor Xi is not the only person to fall victim to internet surveillance as according to Sir Paul Kennedy, the retiring FISA commissioner, “ nearly 979 errors were made during such interception operations during 2012 (alone), often involving monitoring data from the wrong telephone numbers, email addresses or over the wrong time period. In about 20% of cases, the internet and phone companies handed over the wrong internet and phone records to the authorities.” This surveillance has serious consequences and this story teaches the lesson that the government cannot be trusted to use the surveillance without causing harm.

To conclude, the internet has enabled surveillance to go too far as the public's basic civil liberty of privacy, and expecting privacy are eroding. The government using webcams hacking, GPS tracking, and monitoring online activity are a complete breach of privacy as humans carry phones everywhere in this day and age. It is frightening to know that a person's everyday life and activities are being collected and could be used against them. The laws and ethics of internet surveillance need to be seriously discussed and tweaked as they are not serving society in a positive way and are threatening the privacy we deserve.

BIBLIOGRAPHY

- Bauman, Zygmunt, et al. " After Snowden. Rethinking the Impact of Surveillance." *International Political Sociology,* vol. 8, no. 2, 2014, pp. 121-144.
- Bazan, Elizabeth B. *The Foreign Intelligence Surveillance Act: A Sketch of Selected Issues.* 2008.
- Chaffee, Ian. " Internet use at home soars to more than 17 hours per week." *USC News,* January 22, 2018
- Lyon, David. " Surveillance, Snowden, and the Big Data: Capacities, Consequences, Critique:" *Big Data & Society,* vol. 1, no. 2, 2016.
- Parchment, Ryan. " The Chilling Surveillance and Wrongful Arrest of a Chinese-American Physics Professor." *ACLU Journal* , October 31, 2017
- Serwer, Adam. " The US Government Can Track Your Location at Any Time Without a Warrant." *Mother Jones."* August 16, 2012.
- Stanley, Manuel. " The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance." *Annals of The*

American Academy of Political and Social Science, vol. 616, no. 1, 2008, pp. 78-93.

- Venkatadri, Giridhari, et al. “ Privacy Risks with Facebook’s Pll-Based Targeting: Auditing a Data Broker’s Advertising Interface.: *2018 IEEE Symposium on Security and Privacy (SP),* 2018, pp. 89-107.