Government Surveillance in the Information Age – A Necessary Evil or A Means to an End?

CS4001 – Final Term Paper

Sneha Ganesh

Introduction

My term paper discusses the evolution of government surveillance with respect to the impact it has on people's privacy. With technology progressing at such a fast pace, it is already taxing our existing laws to keep up with them. The laws laid down by our founding fathers are no longer as effective as they once were. Government surveillance was developed as means to keep peace within the nation, but the general consensus today is that government surveillance is doing more harm than good. Which brings us to crux of this paper, is government surveillance really as bad as it sounds? Sure, it is interfering with people's privacy rights, but is that a necessary evil or can the system be salvaged while at the same time appeasing the people and acknowledging their rights? This paper also discusses the ethical ramifications of government surveillance; it serves to answer questions like would the people be appeased if the government could make surveillance ethical?

History of Surveillance

The meaning of government surveillance changed after 9/11 and the terrorist bombings of 2001. Shortly after the attacks that killed nearly 3,000 people in New York, Virginia and Pennsylvania, then-President George W. Bush authorized the NSA to conduct broad domestic and national surveillance, the kind that had previously been banned for decades. Bush's newly built spying regime was bolstered a short time later by the passage of the Patriot Act. One Patriot Act passage in particular—Section 215 —allowed the secret Foreign Intelligence Surveillance Act court to authorize blanket warrants for federal authorities to obtain massive swaths of personal data, including bank, doctor and phone company records. Under Section 215, the government does

not need to prove any terrorist activity to request these documents, only to show that the information is “relevant” to an ongoing investigation.

Surveillance was always present, even before 20th century but has gotten more forceful over the years. Traditional surveillance is defined as “close observation, especially of a suspected person”. Examples of traditional surveillance would be following a person, listening behind closed doors etc. New Surveillance is defined as “scrutiny through the use of technical means to extract or create personal or group data, whether from individuals or contexts". Examples include: video cameras computer matching, profiling and data mining; work, computer and electronic location monitoring; DNA analysis; drug tests; brain scans for lie detection; various self-administered tests and thermal and other forms of imaging to reveal what is behind walls and enclosures. The use of "technical means" to extract and create the information implies the ability to go beyond what is offered to the unaided senses or voluntarily reported. New surveillance involves an automated process, so basically it involves computers and other technological devices.

Traditional surveillance often implied a non-cooperative relationship and a clear distinction between the object of surveillance and the person carrying it out. In an age of servants listening behind closed doors, binoculars and telegraph interceptions that separation made sense. It was easy to distinguish the watcher from the person watched. Yet for the new surveillance with its expanded forms of self-surveillance and cooperative surveillance, the easy distinction between agent and subject of surveillance can be blurred.

What new technology is the government employing?

For years, there's been ample evidence that authoritarian governments around the world are relying on technology produced by companies to facilitate human rights abuses. The reach of these technologies is astonishingly broad: governments can listen in on cell phone calls, use voice recognition to scan mobile networks, read emails and text messages, censor web pages, track a citizen's every movement using GPS, and can even change email contents while en route to a recipient. Some tools are installed using the same type of malicious used by online criminals to steal credit card and banking information. They can secretly turn on webcams built into personal laptops and microphones in cell phones not being used. And all of this information is filtered and organized on such a massive scale that it can be used to spy on every person in an entire country.

Some of the most prominent examples of Technology used for government surveillance would be Radio Frequency Identification (RFID tags), Global Positioning system (GPS) and Electronic Tracking systems (credit cards, loyalty cards etc). The use of RFID tags is currently expanding from inventory control systems into the everyday world. Within the next two decades, there is every possibility that all manufactured items would have an RFID tag. The U.S. government had already incorporated RFID tags into passports by 2005. Similarly, the EVI Management Group has proposed to develop the 'e-Plate', a car license plate which would contain an RFID chip. This system would find use when the government needs to know which roads are most used when developing say a road tax. The 'e-Plate' would allow a government to monitor exactly the routes driven by each of its citizens, storing this information ostensibly for urban planning or taxation purposes. However, there is absolutely no reason to believe that this data could not be used for

more sinister citizen tracking purposes. With the cost of each tag soon to drop below 5 cents, we can only expect the number of scenarios to increase as tags are affixed to anything (or anyone) whose location may be of interest. GPS has become a standard add-on for many other technologies. Cell phones carry the units in order to locate their callers in case of an emergency, and vehicles carry GPS to allow display of local maps on onboard computers, track stolen cars and provide usage data to car rental agencies. However, it should be noted that the ability to locate a device, such as a cell phone or a vehicle, is akin to being able to locate its owner. In the United States, more and more often law enforcement agencies are taking advantage of this feature. Due to a Patriot Act provision, it is legal for any service provider to turn over locational data on their customers in times of 'emergency.' Albert Gidari, a Seattle-based lawyer whose clients include AT&T Wireless, Cingular Wireless and Nextel, has stated that the companies he represents receive 20-25 calls a day requesting the location of various cell phones, based on an 'emergency' such as a missing person. No proof of this emergency is asked nor given, and no record of the request is ever made, but the requested data is always turned over. This currently occurring scenario, combined with the fact that cell phones are becoming near ubiquitous, means that many people are now carrying homing beacons accessible to any law enforcement agency. All persons of interest could almost certainly have their movements recorded; this is a frightening prospect at a time when secret 'No-Fly' lists are quickly lessening the criteria for becoming of interest to the government.

Another manner of surveillance is electronic transaction monitoring. Every time a person uses a credit, debit, or store loyalty card that information is recorded. This amounts to a huge amount of data. Wal-Mart has over 460 terabytes of data stored on various servers, a number that

is twice as large as the estimated amount of data on the entire Internet. With the current threat of data mining, the knowledge that the store could compile a list of pictures of its customers based on their social security numbers is scary. You begin to create not only a profile of their buying habits, but also have now added yet another node to massive amount of locational data being gathered about that person. Further, it is not difficult to extract a person's likely income, marital status, number of kids, and potentially even political persuasion from a series of purchases. By doing this, targeted marketing can take place, as can customer discrimination by buying power. The monitoring and recording of all electronic transactions is something that most people have simply come to accept; I think it's time we take a look at what is being done with this data.

Not only has technology developed but also the ability to use it has improved. Government policies are rapidly changing to adjust to the technological boom. The 2008 amendments to the Foreign Intelligence Surveillance Act, which allowed the government to conduct surveillance without warrants, were passed by the House in September 2012. This means that we are completely at the mercy of the authorities; they can listen in on our conversations, and monitor our purchases. The National Counter Terrorism Center now has authority to access data stored by other government agencies that includes flight records, exchange student hosts, casino records, and behavior patterns, all in the name of preventing terrorism. Former National Security Agency analyst William Binney admitted as much when he went public with information that the NSA and FBI have access to virtually every email in the country. The National Defense Authorization Act - allow the government to indefinitely detain people without trial through the military. Another drastic step the government has taken would be the

introduction of drones in a social setting. Drones offer intelligence collectors persistent, low-risk collection capabilities which at times have proven lethal to targets in Iraq, Afghanistan, Pakistan, and Yemen. There is increasing concern these assets may be turned on American citizens. The Air Force also keeps all video information on file for 90 days, regardless of whether a drone is flying in the U.S. or abroad.

Public Reactions to Government Surveillance

Public reaction to surveillance tends to depend highly on the question asked. A 2003 Harris survey shows this fact well. First, respondents were asked whether or not they were in favor of the increase of various surveillance measures, particularly in response to the threat of terrorism. 69% of people were in favor of closer monitoring of banking and credit card transactions, 62% favored increased camera surveillance in streets and public places, and 79.5% supported the use facial recognition technology. However, these numbers may be somewhat deceiving, because respondents to the same survey also highly valued their privacy. 96.5% of people felt it was important to be in control of who could get information about them. 91.2% said it was important to not have someone watch/listen to them without permission. Also, 77.6% of people responded that it was important to be able to go around in public without always being identified. Thus, we can conclude that people are in favor of surveillance – for everyone but themselves.

In 2001, the USA PATRIOT Act afforded American law enforcement powers of surveillance unprecedented in that country. In 2004, a Harris poll was conducted to determine the people's reaction to the increase in government, police and FBI's, authority. It was found that 76.3% of respondents were concerned about the possibility that non-violent critics of the government

would have their communications monitored, and 73.7% feared broad profiling, searching and surveillance of people based on their nationality, race or religion, exactly the possibilities that are created by increased use of modern surveillance technology. In general, once surveillance has been experienced, public support for it tends to decrease.

Ethical ramifications of Government surveillance

A common argument from the government on the topic of surveillance is “If you haven't done anything wrong, you have nothing to fear." Viewing this statement from an objective standpoint proves that it makes sense as most people are law abiding citizens whose lives wouldn’t be adversely affected through government surveillance while at the same time this surveillance makes their lives safer and more comfortable by catching terrorists. In terms of Act Utilitarianism, we can see that since the use of closed-circuit television cameras in public spaces, warrantless wiretapping, and library record checks have the potential to save lives from criminals (the greater good) and terrorists with only minimal invasion of its citizens' privacy (seemingly minor repercussions). When this action extends to things like asking citizens to carry location trackers that make the identification of criminal’s easier people would be more hesitant to look the other way since it would be invasive and the system is prone to abuse. Now consider that, given current technology, the government already has the ability to track a known target's movements to a reasonable degree, and has easy access to information such as one's purchasing habits, online activities, phone conversations, and mail. Though implementing mandatory location tracking devices for the whole population is certainly more invasive than the above, I would like to argue that these practices are a little analogous and extreme. While it may not

always be intentional, surveillance breeds control. This is the cause of most ethical issues surrounding surveillance. Surveillance creates public discomfort because the public obviously do not trust the motives of those exerting this control over them. Similarly, surveillance can be used to control and silence public dissent. The ability to revolt against an unjust controller is a necessity, but unbounded surveillance makes resistance very difficult. There is almost no question that during the 1960's American Civil Rights movement, FBI director J. Edgar Hoover used every surveillance ability within his power to harass activists, unionists and peaceniks; it is interesting to consider whether or not this movement could have been as effective had Hoover had access to all of today's surveillance tools. As surveillance technologies increase in power and functionality, so does the potential for abuse. If any organization is allowed to gather limitless information about their opponents, they will become a nearly un-resistible force; mass surveillance allows this to happen. Also the purpose for which the government collects said data is always obtuse. The European Data Protection Supervisor has acknowledged that even when two databases of information are created for specific, distinct purposes, in a phenomenon known as 'function creep' they could be combined with one another to form a third with a purpose for which the first two were not built. This non-uniqueness and immutability of information provides great potential for abuse by individuals and institutions. This archive of information could be vulnerable both from the outside and from the inside. For example, in September (2007) Benjamin Robinson, a special agent of the Department of Commerce, was indicted for using a government database called the Treasury Enforcement Communications System (TECS) for tracking the travel patterns of an ex-girlfriend and her family. Records show that he used the system illegally at least 163 times before he was caught. With the expansion of surveillance,

such abuses could become more numerous and more egregious as the amount of personal data collected increases.

People fear that allowing surreptitious surveillance in any form even of an insignificant scope could encourage the government to expand surveillance programs. This scenario, similar to a "slippery slope", cannot be dismissed as mere paranoia. For example, the use of biometric markers have increased significantly in the past several years ever since fingerprinting was encouraged in schools in the UK and US since the late 1900's. Now, the discussion has shifted towards DNA collection. British police are now pushing for the DNA collection of children who "exhibit behavior indicating they may become criminals in later life, while former New York City mayor Rudy Giuliani has encouraged the collection of DNA data of newborns. Marginalized groups in any society are a natural target for information gathering. People are frightened of the unknown; thus, minorities are frequently singled out for higher levels of observation. David Lyon notes that this is actually the way that many new surveillance technologies are introduced to society; they begin by being focused on society's weakest, most marginalized groups, and then through 'function creep' make their way into the mainstream. This is a very oppressive practice, however. When any group is singled out for scrutiny, they will inevitably be found to be in violation of some set of societal norms. Care also must be taken not to unintentionally develop a system of total surveillance; as tools combine, we form a 'soft cage.' This may be a worse scenario than the classic Big Brother, which could be called a 'hard cage'. Against Big Brother the masses can rebel, but the 'soft cage' is decentralized, convenient and very thorough.

When is surveillance appropriate?

Many different groups define appropriate bounds for surveillance in different manners. I believe that a good way to deem if government surveillance is appropriate is to make all surveillance adhere to particular guidelines. It does not have to be a law, but something along the lines of design guidelines. One particular model I found interesting was that of M.I.T professor Gary Marx, who argues that before implementing any surveillance we should evaluate the proposed methods by asking a number of questions. These questions would include: Does the surveillance cause any unwarranted physical or psychological harm? Does the surveillance violate assumptions that are made about how personal information would be treated? Does the surveillance cross a personal boundary without permission? Do individuals consent to said surveillance? Is there a human review of machine related results? Would those conducting the surveillance agree to be subjects under the same conditions extended to those they intend to survey? If the individual is treated unfairly and procedures are violated is there an appropriate way to redress the issue? Is the surveillance likely to create precedents that allow the information to be used in unlawful ways? Does the application of this tactic serve broad societal goals? Can surveillance actions be avoided? Is the information being used for personal gain?

Is government surveillance a necessary evil?

Government surveillance was started with the innocent idea of catching criminals before a crime could be committed. Surveillance was started on the basis of the never ending war with terrorism. The war we are currently engaged in is completely different from that of ten years ago. As technology has increased, so has our ability to gather valuable, often actionable, intelligence. However this move toward personal surveillance has increased the risk of smaller

crimes that on their own may be insignificant but are as bad as terrorist attacks when considered cumulatively. This necessitates the collections of citizens' conversations with potential overseas persons of interest, or even among themselves. An open society, such as the United States, ironically needs to use this technology to protect itself. This truth is naturally uncomfortable for a country with a Constitution that prevents the federal government from conducting "unreasonable searches and seizures." With the increase in terrorist attack over the past few years, people's views on how what their government can, and must, do in order to protect its citizens has been altered. However, when we hear of programs such PRISM, or the Department of Justice getting phone records of scores of citizens without any signs of suspicious activities or indications of probable cause that they might be involved in terrorist related activities, citizens needs for privacy and concern over data mining and certain "trolling" measures are warranted. The executive branch, although particularly powerful in this arena, must ensure the Congress is kept abreast of activities such as these surveillance programs. The need for enhanced intelligence activities is a necessary part of the war on terrorists, but abuse can occur without ensuring the legislative branch has awareness of aggressive tactics such as these. Working together the Legislative and the Executive can ensure that both legally and by policy that citizens' concerns with government surveillance reduce.

Furthermore, Government surveillance does not, on paper, violate any constitutional provision. It examines only the addressee and sender on e-mails, and telephone numbers called and called from. The Supreme Court has long held that such information is not privacy-protected by the Fourth Amendment. Apparently recognizing that constitutional argument on the NSA may not yield good results, most people are given to believe in a phenomenon like a slippery slope. They

assert that, while using sender and recipient identities for security purposes is lawful, possessing the content of the messages would enable that to be used too, unconstitutionally — despite NSA's denial that it has been done, and despite the absence of contrary evidence. While social media sites have announced that they have shared user information with the NSA, there has been no proof of data mining or the use of the content of said information. The belief that such information is being distributed is inly speculation and believing the rumors would be akin to depriving all soldiers and police officers of their guns because it is conceivable that some power-hungry president or governor could, in the future, employ armed soldiers or police to seize autocratic power. Imagined horrible doings do not supersede the reality of terrorists seeking to destroy us.

The government also has no power over how third party hosts would use surveillance information. While all official information is heavily encrypted, it is not impossible to break into. With the technological innovation in today's age, it won't be long before encryption software would be rendered hopeless. How other people use information is not in the hand of the government. In a previous example, I had stated how a government employee had used a secure system to stalk his ex-girlfriend. Accusing the system of being bad instead of the individuals using it seems to be illogical. It would be like saying: a school is completely responsible for how an individual turns out as an adult. While the school bears some responsibility, the decisions are ultimately up to its students. In this case, while the government may collect information sometimes without the consent of an individual and thus bear some responsibility as to how that information is used, it cannot be held responsible for the malicious intent of other people think

that people can manage said surveillance activities when the only other option is to leave the country vulnerable to attack.

Another important point that I think is relevant is that citizen's privacy should be protected first and foremost by themselves. If they have something to hide then don't post it on Facebook or put it in an email. Government surveillance does not extend to tapping all phone lines and wiretapping every conversation. If there is something incredibly personal that you wish to say then talk to that person face to face or call them. Privacy is our personal choice and I believe it is something we have taken for granted until recently. Rather than blaming the government for learning something about us that we didn't want known, shouldn't that person first make an effort to hide that thing themselves? I understand that something's are beyond control but I believe getting some control back into our lives depends on us. While I believe that the government should increase its citizens awareness about the methods used in surveillance and people involved should be made aware of their situation, I do not believe that the entire system is flaws or in this case "evil". I believe government surveillance is very much just a necessary evil.

My Solutions

In general, I believe that government surveillance can be made ethical and overall more appealing to people by adopting some of the options listed below:

- There exist reasonable and publically accessible records that tell us when such surveillance has occurred.

- **Limiting Governments' Authority to Collect Personal Information:** Governments should put sensible limitations on their ability to compel service providers to disclose user data that balance their need for the data in limited circumstances. In addition, governments should limit surveillance to specific, known users for lawful purposes, and should not undertake mass data collection of Internet communications.
- **Develop a system of accountability:** Intelligence agencies seeking to collect or compel the production of information should do so under a clear legal framework in which executive powers are subject to strong checks and balances. There should be a set of rules, not necessarily laws but a quality check system with a set of preconditions that have to be met for said surveillance to be allowed. Reviewing courts should be independent and include an adversarial process, and governments should allow important rulings of law to be made public in a timely manner so that the courts are accountable to an informed citizenry.
- **Transparency About Government Demands:** Transparency is essential to a debate over governments' surveillance powers and the scope of programs that are administered under those powers. Governments should allow companies to publish the number and nature of government demands for user information. In addition, governments should also promptly disclose this data publicly. We have already taken the first few steps towards this transparency, the most obvious example would be NSA giving Google, Facebook and other major companies permission to release reports now including how many requests for the data of its members it has received from the government, how many total users were affected, and what percentage of those receive a response from the

company. There has also been a change to the Foreign Intelligence Surveillance Act to the same effect. The curtains haven't been pulled back completely but it's a start.

- **Encourage information flow:** The ability of data to flow or be accessed across borders is essential to a thriving 21st century global economy. Governments should permit the transfer of data and should not inhibit access by companies or individuals to lawfully available information that is stored outside of the country.
- **Prioritizing reticence in situation involving Government surveillance:** This matter is not an easy one to solve and transparency in policies might take a long time to implement, thus having patience with the system is a must. Reticence requires a deliberate evaluation of what we say, how we say it, and to whom it is said. If we care about reclaiming privacy, then we can all start by reconsidering what we post online and how we write emails, considering when and to whom they are sent. Once we accept that privacy is not something we are granted by default but something that we must collectively work to uphold, we can begin to redefine the boundary between public and private.

Conclusion

Most people don't live out their lives without a secret or two. Unfortunately, modern surveillance is making it more and more difficult to keep one's actions away from watchful eyes; those without protection from the system will all be forced to live under public scrutiny. Surveillance is becoming more and more sinister; for instance, the city of Gotham, New York has begun to move towards hidden or disguised surveillance cameras. People will no longer know if they are under the city's watchful eye, and thus will have to be permanently in

line with social norms. Surveillance technologies exist, and will forever continue to evolve. The only thing that keeps society from a state of total surveillance is the goodwill of those in control of the systems. Surveillance is not inherently malevolent; in the proper hands, it can be a very enabling tool. The issue should not be that we are being watched; it should how we are being watched. Government surveillance is not a violation of the constitution and I think that it should be allowed to continue given it meets certain conditions. These conditions are solely to make accepting surveillance more comfortable to the people and thereby more efficient to the government. I believe that by employing some of the solutions listed above like transparency in government policies, adherence to particular rules when performing surveillance activities, encouraging the flow of information and developing a certain reticence toward government surveillance would make the surveillance easier to deal with. In all honesty, the government will never shut down surveillance activities, if people make too much of a fuss, the government will just build in more back doors and stoop to less ostentatious methods of observation. I would rather the government provide us with just enough to know we are being placed under surveillance and in what way. I believe it is within any person's rights to demand a reason for surveillance. Thus surveillance can be wielded as a weapon or a boon, depending on how it is used. The government has taken the first few steps towards making surveillance more transparent, I think we, as citizens, should take the next step by protecting the things we don't want others to see by not putting it on social networking sites, or present the information in any way the government can track. We are ensured our privacy and we should definitely trust in the government but at the same time remaining vigilant is always a good option.

Sources

1. Greenwald, Glenn, Laura Poitras, and Ewen MacAskill. "Edward Snowden: US Surveillance 'not Something I'm Willing to Live Under'" *The Guardian*. Guardian News and Media, 09 July 2013. Web. 28 Feb. 2014.
   Link: http://www.theguardian.com/world/2013/jul/08/edward-snowden-surveillance-excess-interview

2. Soghoian, Christopher. "Christopher Soghoian:Government Surveillance - This Is Just the Beginning." *Christopher Soghoian: Government Surveillance*. Ted Talks, Aug. 2013. Web. 10 Mar. 2014.
   Link:
   http://www.ted.com/talks/christopher_soghoian_government_surveillance_this_is_just_the_beginning

3. Soghoian, Christopher. "Privacy at Risk: The New Government Surveillance and the Fourth Amendment." *Google Books*. N.p., n.d. Web. 03 Apr. 2014.
   Link:
   http://books.google.com/books?id=aUCKWTEDCTMC&printsec=frontcover&dq=government+surveillance+privacy&hl=en&sa=X&ei=ARs9U_O5HIvJsQT7m4H4Cg&ved=0CEQQ6AEwAA#v=onepage&q=government%20surveillance%20privacy&f=false

4. "Liberty, Privacy & Surveillance." *American Library Association*. American Library Association, n.d. Web. 03 Apr. 2014.
Link: http://www.ala.org/advocacy/privacyconfidentiality

5. "Domestic Surveillance Techniques - Our Data Collection Program." *Domestic Surveillance Techniques - Our Data Collection Program*. NSA, n.d. Web. 2 Apr. 2014.
Link: http://nsa.gov1.info/surveillance/

6. "Tech Giants, Telcos Get OK to Release Stats on NSA Spying | Threat Level | WIRED." *Wired.com*. Conde Nast Digital, 25 Jan. 0014. Web. 01 Apr. 2014.
Link: http://www.wired.com/2014/01/nsa-public-spying-data/

7. "From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance." *Pace Law*. Pace Law, Winter 2011. Web. Apr. 2014.
Link: http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=f3df19f0-04b2-4a35-ad17-65ce06364221%40sessionmgr113&vid=2&hid=114

8. "How 9/11 Turned the U.S. Government into Spies: A Brief History of Domestic Surveillance." *TakePart*. N.p., n.d. Web. 03 Apr. 2014.
Link: http://www.takepart.com/article/2013/09/11/9/11-patriot-act-and-history-nsa-spying

9. "Timeline of NSA Domestic Spying | Electronic Frontier Foundation." *Electronic Frontier Foundation*. N.p., n.d. Web. 01 Apr. 2014.

   Link: https://www.eff.org/nsa-spying/timeline

10. "The Ethics (or Not) of Massive Government Surveillance." *The Ethics (or Not) of Massive Government Surveillance. Stanford University*, n.d Web 02 April 2014

    Link: http://cs.stanford.edu/people/erobots/cs181/projects/ethics-of-surveillance/ethics.html

11. Lyon, D. (1994) The Electronic Eye: The Rise of the Surveillance Society, University of Minnesota Press.

12. Thoreau, H.D. (1849) On the Duty of Civil Disobedience, online at http://eserver.org/thoreau/civil.html, accessed 04.15.2014