Levi George

Professor Chansavang

CS 30600: Computers in Society

28 September 2020

Invasions of Privacy and Violations of the Fourth Amendment by Emerging Technologies

Technology and innovation have always been a good thing for mankind. The first forms of invention were fire and bone tools, allowing us to hunt and cook our food. This innovation of cooking allowed humans to pull more nutrients out of our food, destroy deadly bacteria, and make it easier to eat. These benefits helped increase human lifespan. However, with the advent of computing technologies people have unknowingly been allowing a wealth of strangers into their homes. These strangers can be quite malicious in some cases, while in other cases they can be slightly less malicious but still invasive. Although, computers are not the first advancement to allow others into our home against our own will, nor will they be the last.

Computers steal a large amount of data, but they can also be used to stop this flow of data from your computer. Numerous methods are used in the current day to track you and store information. This can be stopped by dedicated software developers and people working within government agencies. The average person can also use certain tools to obscure their address and block software tools from accessing data that is stored by websites on their computer. In some cases, users can even block the storage of this data by browsers. However, not all tools and processes used here are 100% effective, they also are not easy to utilize in some cases. Between these tools and awareness of the following issues, people can enact change or make data mining less effective, thus deterring it. However, before someone can defend privacy, they must understand privacy and the average citizen’s right to it.

Privacy is older than many would have thought at first glance. So old, that Aristotle mused about a political life (*polis*) and a personal or domestic life (*oikos*). While most invasions of privacy would be spying on someone or listening in on their conversations (DeCew). Things changed with technology, there is an interesting trick you can perform with a cup where you place the rim of a glass against a wall and place your ear on the bottom, this allows you to listen to conversations through walls. While seemingly innocuous, it gives many people a method of invading your privacy and listening in on conversations. With the advent of the telegraph and telephone people inevitably discovered ways to splice into wires or exploit the system of communication.

One of the first known instances of the Fourth Amendment being potentially broken was Olmstead v. United States. In this case a group of federal agents wiretapped Olmstead’s phone to discover evidence regarding prohibition act violations. They did this without entering Olmstead’s own home or personal office. They accomplished the wiretapping through using the lines of a telephone company in a large basement to listen in on conversations. This wiretapping proceeded for several months until the agents felt as though they had enough evidence. Olmstead was convicted, when he tried to argue that the agents violated his fourth amendment right, the supreme court overruled and held that the agents were within the law to wiretap (Henry and Baase) (Olmstead v. U.S.).

The next instance is Katz v. United States. Agents from the Federal Bureau of Investigation used small listening devices attached to a phone booth to record his conversations with people who Charles Katz was collecting sports bets from. When he was convicted, Katz tried to argue that it was a fourth amendment violation, to no avail. When the case reached the Supreme Court, the justices presiding voted in favor of Katz. The justices ruled in his favor on account of his own expectation to have privacy in the booth. The fourth Amendment was claimed to apply only to people but not places, however, Potter Stewart stated, “But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected” (Henry and Baase).

However, the Katz story would not be the last time government officials used bugs and other devices to invade privacy. In January of 1992, Danny Lee Kyllo had his privacy invaded when agents from the Department of the Interior used thermal imaging to view the heat emitted from Kyllo’s home (Henry and Baase). This was done in order to examine heat differences under the assumption that he was growing Marijuana. The court ruled that this was an unconstitutional search since the technology was not available to the public and the police never attained a warrant to use the device for a search. Justice Scalia tried to protect privacy from future advancements by asserting the difference between “off the wall” and “through the wall” searches were inconsequential (U.S. Supreme Court, Kyllo v. United States).

While Scalia, a member of our government, tried to protect our privacy other government officials have not done the same, for their own gain. In perhaps the largest invasion of privacy and violation of the fourth amendment, U.S. President Richard Nixon’s cabinet members tried to spy on Democratic officials at the Watergate Office Building in Washington D.C. Nixon’s cabinet hired several burglars to invade and plant bugs around the Watergate complex. After the burglars were arrested, a huge scandal occurred in the Nixon administration as they attempted to cover the burglary’s connection to the cabinet. This scandal ended with Nixon’s resignation and several other members of the cabinet were convicted of various crimes (Onion). While the issue was resolved, it was because a slip up. It will be important for people to seek out issues regarding new technology and policies that can breach good privacy standards.

Computers, like small bugs and recording devices, have made the problem even more virulent, with GPS and the IP Protocol being used to tag web surfers and gather information regarding them. A good example is in the 2012 case of *U.S. v. Jones*. Where the police used a GPS tracker that they had attached to his car to follow his whereabouts near constantly. The police had used proper channels to secure a warrant for using the GPS device. However, Jones won the court case since the Justices of the court reasoned that Jones’ car was his personal effect. Additionally, the basis of expecting privacy as a means for determining Fourth Amendment violations is at play here. A few of the Justices on the Supreme court have determined that the expectation of privacy is the key to the Fourth Amendment (United States’ Supreme Court, United States v. Jones).

The most recent form of invasion comes from a most beloved pass-time for many people. Social Media sites like Facebook and Instagram are constantly tracking people. People unknowingly expose a large amount of information to everyone on the internet. This information can be spread very quickly across the internet, especially images that are explicit or embarrassing in nature. An excellent example are photos that celebrities and government officials dislike, they are attacked with fervor. In fact, Beyoncé, had several bad photos taken during her performance at the Super Bowl, when her publicist desired their removal from a BuzzFeed post, BuzzFeed reposted them. Another example is Chinese President Xi Jinping, when people drew comparisons between the Chinese President and Winnie the Pooh, China proceeded to ban the Intellectual Property within the Chinese borders. Earlier this year, after a skirmish that led to the deaths of several Indian soldiers in the Ladakh region, Indian tweeters began using the #WinniethePooh tag. The same thing happens to people all the time, once they post a picture it sometimes remains on the internet for years (Sullivan, Rory).

Risks to you do not stop at self-exposure on Facebook; Facebook also analyzes your posts and pictures to gather information. They see what ads you click on as well; they determine once you’ve clicked on an ad on Facebook and where it led you, then they save this information. Another major way that Facebook records your information is through other web articles. Even when you don’t have a Facebook account, they still track you through these web articles. Whenever a web page has a Facebook pixel, or just a Facebook-based comment section with a Like button the user can be tracked across multiple websites. Even if you refuse to utilize the Pixel’s features, Facebook still gets information on you. Facebook has information regarding all people stored in their databases for the sole purpose of building advertising models, they are trying to determine how to get you to buy products and improve Facebook earnings (St. John, Allen).

Continuing the Facebook discussion, the Pixel is simply a small image file that a website will request. This pixel allows for data to be gathered, all sorts of activity on a site can be examined with the pixel. This can collect information regarding products you have clicked on or added to virtual shopping carts. However, web developers control what data is collected and when it is transmitted to Facebook. If you are logged into Facebook on your preferred browser, then Facebook will collect data on everything you do and will know most of the websites you visit. Even without a Facebook account, a database can be compiled associated with your IP address (The address of your computer). All the data they collect regarding you, can be associated with your router’s virtual name. (St. John, Allen).

As robotics and computing has evolved this has given rise to the Internet of Things. This concept is the inter-connectedness of devices with embedded computers. So, if your fridge has a display on it, then it is a computer that can be accessed by other computers. The same goes for your phone, TV, and even car. This also includes drones and other robots that are produced commercially. This offers substantial amounts of ease or entertainment in the case of drones and micro-computers in home appliances. However, at the same time people unknowingly endorse and purchase these things that allow invaders to gain access to their home through the embedded computers. There are a variety of things consumers can do to limit this data collection, however in many cases the total elimination is only possible through not using the devices.

Drones can be used to investigate a house or building from the air and through windows. Their small form factor also makes it difficult to detect with radar, unless it is specially equipped. While laws have been established to protect against drone usage, they are primarily focused at government agencies and companies (Drone Use and Privacy…). However, arms should not be raised against drones, numerous times they aren’t invading your privacy but in the case that they are, you should contact the police. Attacking or shooting down drones can be harmful to legitimate efforts and uses of drones; one instance involved a drone being used to search for a lost dog (Kiger, Patrick).

Drones allow external viewing into your home, but appliances with minicomputers can allow people to view inside your home or discover your actions. Appliances like your fridge can monitor the frequency with which you open it and in some cases the contents, they even offer recipe search capabilities. This information can be used against you in some cases, people can collect the information about what you consume and see what times you are most active. A talented hacker could discover your major times of activity and use that to stage a home invasion. Without proper safety features on certain appliances like an oven or fridge, the software could be accessed, and the hardware could be overclocked to cause damage or destruction to the appliance or the even the home (Mookyu, Park).

The most malicious form of privacy invasion comes from attempts to protect people. Since cameras are a key component of home security and security in general, they are used frequently. Cameras are also easy to access if left improperly defended. This can expose people at their most vulnerable point; in their own homes. However, many countries have littered their cities with cameras to observe crimes and bad behavior. Cities in the U.K. and most of China use a massive number of cameras to observe citizens and track crime. However, in some cases it has been shown that the cameras don’t always prevent crime. China has a bad habit of spying on its citizens and it uses the cameras to do that. In the future, states like China will use every piece of technology possible to claim control over their citizens (Hoar, William).

The United Kingdom has displayed a large amount of care in this realm. They have installed cameras in major thoroughfares, parking garages, and along active streets. These cameras do achieve some of their intended effects in the U.K. There are decreases in vehicle related crime and other petty crimes and some people do feel safer with the cameras observing them. However, they do not provide a total deterrence, violent crimes are remained mostly unchanged. In addition to the alleviation of some crime, U.K. agencies allow citizens to put in petitions or applications to have recordings of them removed, ensuring a more privacy friendly stance on surveillance (Sheldon, Barrie). The U.K.’s actions with surveillance technology is an excellent example of what good privacy policies look like, building policy that allows legitimate use of a technology while also protecting citizens of a government.

Every company will use technology to get an edge over the consumer and to get them to buy some product. New technologies are arising that expose sensitive information about people to companies. The use of DNA analyzing services such as 23andMe reveal the genealogy of the users. This contains information such as heritage and can even reveal susceptibility of certain people to diseases and disorders. In turn the lack of protection for DNA and other genetic data would allow the same companies who offer the service to sell the data. This means that insurance companies can discriminate against you for being pre-disposed to certain illnesses (Brodwin, Erin). This aspect of privacy is more up to debate; however, it should be thought of that if the contents of our thoughts is our own, then so should the contents of our body. People can’t just come up to you and look in your mouth, and medical care providers can’t force you to undergo care. So, the logical step is that people don’t get to view the contents of your DNA without your consent. However, this is only the start of technology that could invade the privacy of others. cars which drive themselves and computers that work on the atomic level can all be causes for great concern.

Self-Driving Cars analyze the things that a camera on the front of the car sees. From there it uses a sophisticated machine that learns from use. This machine is a computer that has a Neural Network or A.I. on it. This machine will use constraints that it has been given to analyze what it sees to make decisions about how to drive and what courses of action to take. While the A.I. is innocuous, the GPS is more concerning. It offers a method of tracking the drivers and in some cases can record every place a driver has visited. How then should someone protect against GPS trackers on cars, or even those that are on phones? Additionally, hacking of cars is a concern, a single vulnerability could allow bad actors to invade the car’s systems and shutdown anything from airflow to even the engine and the brakes (Navetta, David).

Another important aspect of self-driving cars is how they work and make decisions for the driver. While not directly related to privacy, it is still important to consider other safety issues regarding the way these systems are built. In the case of an accident, should a self-driving car protect the lives of its passengers or the lives of those on the road (Navetta, David)? While a car can be found to have several inadequacies in its security, what if something thought to be protected, was actually indefensible? What if methods of protection that are implemented in computers no longer worked? Quantum computing has the mathematical power to break through most types of encryption.

Quantum computing seems fascinating, it is the logical conclusion of shrinking form factors for our processing machines. Computers used to take up entire warehouses and weigh tons, however continued advancement in computing technology and materials engineering allowed for the creation of the smallest computers. Computers now are small enough to fit in someone’s back pocket and still has the capability to run advanced computations and even run graphically demanding games. Next, it would make sense to go even smaller, to the size of atoms. Instead of using the typical bits that computers do, Quantum computers make use of Qubits that can achieve several different states through superposition. Where does this become a threat?

Quantum computing offers a way to break the last line of defense between your private information and what you look at on the internet from people who could use this against you. Quantum computing makes encryption obsolete, encryption being the method of encoding to make any information you send or receive incomprehensible to anyone who gets their hands on the information. This means that with quantum computers, your information could easily be decrypted and then viewed. Everything you look at and everything you send appears before those who are using the quantum computer to break into it. This is a situation which is a hard one to decipher. People have a variety of paths before them to deal with quantum computers, they could outlaw quantum computing, put heavy restrictions on quantum computers, or quantum computers could lead to even more robust methods of encryption that protect against decryption. (Tucker, Patrick).

These examples serve to display the need for proactivity in legal matters and matters of personal rights. Citizens in the U.S. could get their representatives to enact privacy policies like those in the U.K., providing adequate usage of some technology and protect citizens. The first step would be for people to act on these issues. There are various ways for people to protect themselves and bring the issues to the attention of people in office like governors and mayors. However, there are also methods of spoiling the efforts of data trackers and social media. It also helps for people to be aware of these issues, spreading awareness is one of the biggest methods of gaining advocacy for a movement. However, the biggest thing that anyone can do to start defending their privacy is to know that they deserve it and know what their rights are, otherwise people can take advantage of that lack of knowledge.

One of the most effective methods to protect against things like invasions of privacy is to pursue legal action, it can be applied almost universally to entities both large and small. In the past, issues with invasions of privacy have been solved through legal action and taking things to the supreme court. This can be seen in situations like Katz v. U.S. and Olmstead v. U.S. It is important to also become involved in your community and communicate your concerns with your local legislator. Numerous petitions have succeeded in forcing government officials to acknowledge some issue within the community. The best way to promote a petition and change within in some community is through continuous advocation and spreading awareness of some issue.

Understanding how computers work can make the vulnerability that people experience at their hand clearer. This understanding and awareness allows people to elect how to arm themselves against these threats to privacy and security. This means someone could take to their local legislator or elect to hide themselves through other means involving computers. Since everyone has different backgrounds, they can apply their own different views to a problem and solve or improve the problems. This idea can be seen in the Japanese train system, when faced with loud trains, the engineers were stumped. One day, one of the engineers who was an avid bird watcher had an epiphany after watching an owl float effortlessly and quietly down from its perch to catch an unsuspecting prey.

In fact, numerous people have devised ways to ruin the data or stop the flow of data between consumers and the companies that collect that data. There are numerous plug-ins for browsers to block trackers that would send data from your computer based on your searches. There are browsers, software, operating systems, and methods of working on the internet for you to obscure your location and searches. The most basic methods involve abstaining; however, this isn’t practical since so much of our world is based online. Additionally, the less familiar you are with computers and the less experience you have, then the worse off you may be. One of the biggest ways to prevent attacks is to know when and how you can be attacked.

Browsers like Brave, Tor, and FireFox all have features that provide safety from invasions of privacy. Tor, is a software that instead of sending information directly from your computer to a server, will route it through a series of computers and then send it to the server. This hides your IP address (your computer’s identifier), which in turn can obscure your current location from people who would want to see this and find you. However, by logging into your Facebook, Instagram, or other accounts will make it clear who you are to external viewers, it will ruin your security. This and many other tools can provide you with several layers of security and protect you from people who would try to find you or track your data.

Brave and Firefox both feature tracker blocks to prevent cookies, ad trackers, and other services from collecting data on you. Additionally, they are slightly faster and less resource intensive that Internet Explorer and Google Chrome. There are even search engines that you can use along with these browsers to prevent trackers from getting your data. DuckDuckGo is the premier search engine to block trackers and avoid giving data to companies like Yahoo or Google. This is all surface level though, there are more ways to avoid detection online using different operating systems and avoiding certain web surfing habits.

For tech savvy people, there are a myriad of methods to avoid leaking data. The major method is to change the operating system you use. Two operating systems that can help you avoid detection while surfing the web are Tails and Kali Linux. While there are many others that can help with security, these two are the most popular. Tails enforces several principles in its design; Amnesia, Encrypted Persistent Storage, Open-source, and utilizes Tor. Tails in essence forgets everything you do when you turn it off, will save some files onto the hardware you start it from, and this is only a few of the things. If you are particularly interested in security then Kali Linux offers a similar set of tools that also allow for privacy, however it also offers tools for penetration testing, which can be used to determine how safe you are from hackers or other bad actors.

If you are serious about being secure, then the biggest thing you can do is to avoid social media. Websites, like Facebook and Instagram all track you, additionally apps like TikTok can actively get data on you while you use it. Forming an alternative identity can also work to obscure your identity on the internet, although this is as easy as just not using your real name one websites but abstaining from using Facebook is better than lying to Facebook about your identity. Other ways to protect yourself from invasions of privacy or data leaks is to use password managers, VPNs, encryption and to minimize how much you use location features on your phone or computer. While a lot of technological innovations seem convenient and fun, things like Alexa and refrigerators with onboard computers pose a major risk, so it can often be better to avoid them to have a more secure network.

While many people take it on themselves to protect themselves from online threats, they can’t always avoid threats that work on a systemic and application without avoiding these systems. While this may seem easy, it should not be the responsibility of the people to avoid invasions of privacy and threats to their security. It should lie on the developers and people who work on these systems to produce secure and non-invasive programs. It doesn’t make sense for a chef to give you a half cooked and half spiced meal, so why should developers give insecure and invasive systems to users. However, not all developers think this way and in some cases developers are little fish in a big pond and can’t make meaningful changes. Developers who do have power over the development life cycle can use tools and methods that improve security and restrict access to your system by big data companies.

In many cases developers who work on projects for companies like Google, Facebook, and even government agencies may have little agency themselves. Developers will have no right or power to fight against bad practices occurring in the workplace. Edward Snowden was one developer who witnessed invasions of privacy and data being stored regarding citizens in order to root out possible terrorists. Edward could not stand for this and leaked information about the NSA’s actions in order to make these actions known to the public. After this he had to flee the country for Russia, but Wikileaks arose as a counter to poor privacy practices in companies and agencies. Wikileaks allows developers and workers to leak information onto a widely available service for all to see.

While seemingly useful cookies and other trackers offer third parties a window into the lives of your consumer’s lives and their interests. These cookies can be used to build up a data profile on users. This profile is then used to send ads that are targeted to users on the internet or through mail. These ads are lucrative and innocuous but collect data unbeknownst to users, violating their right to privacy and control of information about themselves. Some websites avoid this by notifying users and using opt-in or opt-out policies of data collection. The best way to serve your users is to avoid using these trackers or make it obvious how they are being used. Best practices include how to design your applications and software, but they also include how to structure the system for security.

Developers have an unprecedented amount of data available to them. Most computers these days come with a myriad of tools and devices built-in to them. The average phone has a camera, accelerometer, gyroscope, and even GPS all packaged within it’s small form-factor. Many developers believe that Responsive Web Design is a necessity for developing robust and powerful applications that can make money. However, this serves as a security risk, when applications have access to some part of a phone’s hardware, they expose it in order to use it. If the application using the hardware has some weakness or flaw and it is hacked or penetrated, then all the things that the application could access is now accessible by the bad actor who has hacked the application. The bad actor could now view files, locations, web history, and possibly even other application data.

To solve this issue, it is important to code safely and securely. There are many classes that teach this to students, but it is also important to use valid coding conventions and best practices. A system that is not robust could become vulnerable through weaknesses or glitches that a bad actor tests for exposure. Additionally, it is important to avoid jumping on technology bandwagons. When new systems or programming frameworks arise, they almost always have some weakness in them. Using these frameworks can also produce glitches and loopholes for hackers to break through. In many cases secure coding is not made known to programmers or in some cases is not taught. I can recount a web development class that did not teach semantic or secure coding, both industry standards for programming and key to making accessible software or websites.

This gives rise to another issue which must be solved in order to produce competent developers who create secure systems. Standards must be expressed and taught to young students of programming. Creating a more secure world starts with teaching security concepts to users. This doesn’t even apply to just software developers and programmers. Security concepts can be taught to everyone, ranging from safe web surfing to safe programming. This is the only course of action that can produce a safer internet, students only need be given the knowledge to protect themselves. When our education system teaches students about safe sex, safe driving, and how to live healthily then why not teach students about safe web surfing?

Humans are beings of sacrifice, with the ease of our lives that has been achieved

through technology we are sacrificing our liberty to privacy. However, it is entirely up to us how

much privacy we give away for these benefits. We must fight, tooth and nail, in the legal realm

and from our own home to defend ourselves against the government. We must take steps to secure our anonymity online whether it be against companies who sell information about you or people who might wish to stalk you. We must teach students about how to program and surf the web safely in order to protect the privacy that we all deserve. To quote Benjamin Franklin; “He who would trade liberty for some temporary security, deserves neither liberty nor security.”

Works Cited

Brodwin, Erin. “After you spit into a tube for a DNA test like 23andMe, experts say you shouldn’t assume your data will stay private forever.” *Business Insider.* Feb. 16, 2019. <https://www.businessinsider.com/privacy-security-risks-genetic-testing-23andme-ancestry-dna-2019-2>. Accessed Nov 11, 2020

DeCew, Judith, “Privacy”, the Stanford Encyclopedia of Philosophy Archive. Spring 2015 Edition. May 14, 2002. <https://plato.stanford.edu/archives/spr2015/entries/privacy/> Accessed Nov. 7 2020.

Deflem, Mathieu, and Shannon McDonough. “The Fear of Counterterrorism: Surveillance and Civil Liberties Since 9/11.” Society, vol. 52, no. 1, Feb. 2015, pp. 70–79. EBSCOhost, doi:10.1007/s12115-014-9855-1.

“Drone Use and Privacy Presidential Memorandum on Domestic Use of Unmanned Aircraft Systems.” Congressional Digest, vol. 95, no. 6, June 2016, pp. 5–32. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=115424885&site=ehost-live&scope=site.

Henry, Timothy, and Baase, Sara. *A Gift of Fire*. New York, Pearson, 2018.

Hoar, William P. “China Imposes Digital Dictatorship, Spreads Surveillance Tech.” New American (08856540), vol. 35, no. 11, June 2019, pp. 41–43. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=136687363&site=ehost-live&scope=site.

Kiger, Patrick. “Think a Drone is Spying on You? Here’s What to Do.” *Science How Stuff Works.* Aug 13, 2019. <https://science.howstuffworks.com/drone-spying.htm>. Accessed Nov 12, 2020.

Navetta, David and Et. Al. “Privacy and Security Issues in Autonomous Cars”. *Cyber Defense Magazine.* Oct 24, 2019. <https://www.cyberdefensemagazine.com/privacy-and-security/>. Accessed Nov 11, 2020.

Onion, Amanda and Missy Sullivan, Matt Mullen. “Watergate Scandal”. *History Channel*. Sep 25, 2019. <https://www.history.com/topics/1970s/watergate>. Accessed Nov. 7 2020.

Park, Mookyu, et al. “Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective.” Sensors (14248220), vol. 19, no. 9, May 2019, p. 2148. EBSCOhost, doi:10.3390/s19092148.

Sheldon, Barrie. “Camera Surveillance within the UK: Enhancing Public Safety or a Social Threat?” International Review of Law, Computers & Technology, vol. 25, no. 3, Nov. 2011, pp. 193–203. EBSCOhost, doi:10.1080/13600869.2011.617494.

St. John, Allen. “How Facebook Tracks You, Even When You’re Not on Facebook”. *Consumer Reports*. Apr. 11, 2018. <https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook/>. Accessed Nov. 7 2020.

Sullivan, Rory. “Indians mock Xi Kinping with Winnie the Pooh after deadly border clash with China.*” Independent*. Jun. 19 2020. <https://www.independent.co.uk/news/world/asia/india-china-xi-winnie-pooh-border-clash-a9575516.html>. Accessed Nov. 7 2020.

Tucker, Patrick. “What Quantum Computing Means for National Security.” Futurist, vol. 44, no. 4, July 2010, pp. 6–7. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=51010414&site=ehost-live&scope=site.

United States’ Supreme Court. *Katz v. United States.* Dec. 18, 1967. Legal Information Institute, Cornell U Law School, <https://www.law.cornell.edu/supremecourt/text/389/347>.

United States’ Supreme Court. *Olmstead v. United States.* Jun. 4, 1928. Legal Information Institute, Cornell U Law School, <https://www.law.cornell.edu/supremecourt/text/277/438>.

United States’ Supreme Court. *Kyllo v. United States.* Jun. 11, 2001. Legal Information Institute, Cornell U Law School, <https://www.law.cornell.edu/supremecourt/text/99-8508>.

United States’ Supreme Court. *United States v. Jones*. Jan. 23 2012. Legal Information Institute, Cornell U Law School, <https://www.law.cornell.edu/supremecourt/text/10-1259>. Accessed Nov. 7 2020.