In Electronic Frontier Foundation’s article [Know Your Rights](written by Hanni Fakhoury and Nadia Kayyali), they provide a guide to protection against unreasonable searches of personal digital devices. In the first section, they explain when authorities are legally allowed to search your personal devices. Under most circumstances, the police need a valid warrant to search or seize your devices. However, if you verbally consent to a search, they do not need a warrant. Furthermore, they can ask your partner, roommate, guest, etc. for consent to search our personal devices (if you are not present); the ensuing legalities are a bit of a grey area, but if the police “reasonably believe the third person has control over the thing to be searched,” then they can legally proceed with the search. If you are arrested by the police, they can generally search all items on your person without a warrant; however, they cannot legally search the digital contents of your devices without a warrant. The exception to this rule is if the police have reason to believe that crucial digital evidence on your device is in danger of being erased, they can legally search the digital information on your personal device.

In Electronic Frontier Foundation’s article [Mandatory Data Retention](they discuss mandatory data retention rules and their consequences to data privacy. In many countries, governmental agencies are advocating legislation that requires Internet Service Providers (ISPs) and telecommunication providers to track and document the data and activity of public users online and through telecommunication. Oftentimes, this legislation is coupled with legal arrangements that enable governmental investigators to access the documented data and activity of. The majority of internet service and telecommunication providers assign users a unique internet protocol (IP) address, which changes regularly. IP addresses contain many pieces of information, namely location. These proposed mandatory data retention laws require internet service providers to document IP addresses for a specified period of time. This documentation of IP addresses enables governmental agencies to potentially identify an individual at a specific time with a given IP address. Clearly, this proposed legislation could significantly harm the privacy and data security of online and telecommunications users.

In her video [Cybersecurity: Crash Course Computer Science #31](Carrie Anne explains the basics of cybersecurity. She defines cybersecurity as “a set of techniques to protect the secrecy, integrity, and availability of computer systems and data against threats.” Secrecy is upheld if only authorized persons are able to read or access computer systems and/or data. Integrity is upheld if only authorized person are able to use or modify data and/or computer systems. Availability is upheld if only authorized person are able to access their data and/or computer systems. In order to achieve cybersecurity, security designers typically define a threat model -- which profiles the characteristics and capabilities of a potential cyber-attacker. Threat models allow preparation against specific threats, instead of exhaustively preparing against broad, general threats. In order to ensure that access is given only to the appropriate people, systems authentication -- “the process by which a
computer understands who it’s interacting with.” Authentication methods include requiring a password, requiring a physical key, and biometric identification (fingerprint scanning, iris scanning).

Keylogging is the process of recording various activities on a computer. A keylogger is a piece of hardware or software program that is able to record computer activity in real time. In his article, Why Keylogging Software Should Be on Your Radar, Bradley Mitchell explains the basics of keylogging. A keylogger typically has the following capabilities: recording all keyboard keys pressed by the user, documenting all passwords entered by the user, capturing screenshots at regular intervals, taking copies of emails sent by the user, documenting URLs visited on web browsers by the user, making a list of applications that were run by the user, recording logs of all instant messaging sessions, and automatically sending reports containing this information (by email, FTP, or HTTP). The majority of keyloggers of store the data they collect on the local hard drive of the computer, but others automatically send the data to a remote computer or even a remote web server. Furthermore, malicious keylogging software is almost always very hard to detect; the software hides its presence by such methods as being installed in hidden or disguised directories or hiding or disguising the software from the operating system task list.

In Electronic Frontier Foundation’s article Cyber Security Legislation, they discuss various cybersecurity laws and their consequences. In 2014, the Cyber Intelligence Sharing and Protection Act (CISA) and the Cybersecurity Information Sharing Act (CISA) were introduced in Congress. Although these bills are intended (or at least under the guise of intention) to promote and improve cybersecurity, they also enable corporations to share more personal user data with the government or private companies. Along with other similar legislation, these bills are usually written sufficiently broadly to allow internet and telecommunication providers to track, document, and share personal emails, text messages, and other digital communication with governmental agencies. The definitions of the bills tend to be vague and non-specific: the bills enable actions to be taken to protect against “improper” modification of data and to ensure “timely” access to information. An important consequence of these bills is that they enable governmental agencies to investigate subjects (crimes or otherwise) unrelated to cybersecurity threats.

In her 2014 TED Talk Hackers: The Internet’s Immune System, Keren Elazari talks about a side of hacking and cybersecurity not often under the spotlight: the benefits provided by hackers. For instance, in 2010, New Zealand programmer Barnaby Jack devised a way to make ATMs limitlessly output money. However, instead of using his knowledge for criminal activity, Jack publicized his research, allowing ATM designers to fix and improve ATM security. His view on cybersecurity was exemplified by a quote of his: “Sometimes, you have to demo a threat to spark a solution.” Elezari agrees with this view on cybersecurity. She believes that hackers are “the immune system for this information age.” Although hackers often cause harm, they also find problems and weak points in software or systems -- allowing the repair of these problems and improvement the systems. Using various examples, including the actions of international hacktivist group Anonymous, Elazari points out that hackers have a significant amount of power and influence. She says that “hackers are a force for social, political, and military influence.”
Hi Luke,

It was interesting reading your summary of the first article, The 'Fair Use' Rule. In my last chapter case research, I read about fair use as a legal defense: in the case of Oracle vs. Google, Google used fair use as a defense against Oracle's claims of copyright infringement regarding their Java application programming interfaces. Here's one of the sources I used if you're interested: A Brief History of Oracle vs. Google. However, it seems to me that this concept of fair use is a bit of a legal grey area. You mentioned that fair use is generally applicable when using a copyrighted work for "education, parody, criticism, news, or commentary." I definitely agree that fair use is applicable for education and news. The only category I don't agree with is parody. In my opinion, I don't think that using a copyrighted work for parody should be fair use since parodying is directly processing the work itself; I think that you should have to first get the permission of the owner of the work before being able to make a parody. But, clearly that is not the legal standard at the moment. Are there any of those categories that you yourself don't agree with?

I also liked what you wrote in your last paragraph (about the TED talk The Surveillance Device You Carry Around All Day. I liked how you pointed out that most people carry around their phones with them almost everywhere. I think that the location tracking of people with mobile phones that these companies are capable of is virtually the same as if people had some sort of physical tracking device on them at all times. Viewing it in this way really puts the entire situation in a different light. I read an article by the Electronic Frontier Foundation Mandatory Data Retention that describes similar ideas and problems. This article was my favorite article this week, and it explains how certain mandatory data retention laws require internet service and telecommunication providers to record the IP addresses of their users and to allow governmental agencies to access this information. As you said in your paragraph, this tracking allows the pinpointing of individuals' locations by whoever has access to their IP addresses. Clearly, this is a significant invasion of privacy.

It was really interesting reading what you had to say!

--Shanti