The article, **Know Your Rights**, by authors, Hanni Fakhoury and Nadia Kayyali, highlights crucial information about the policies surrounding search and seizure of computers, phones, and other electronic devices. The article stresses that because of our 4th Amendment rights, individuals do not have to consent to police search without a warrant. The article states that if police knock at the door of a personal home and ask questions pertaining to an inquiry, that a response such as, “I do not want to talk to you or answer any questions without my attorney present” (Fakhoury & Kayyali, 2014) is an appropriate response. The article details all of a person’s rights from: stepping outside the door, if the police do not have a search warrant, to limiting the extent of a police search, and to obtaining advice from a lawyer before consenting to any search or answering questions. The article mentions that if the police do have a warrant it is imperative that “you should not physically interfere with them, obstruct the search or try to destroy evidence, since that can lead to your arrest” (Fakhoury & Kayyali, 2014). The article focuses on many important aspects of police search and seizure mentioning that others in your home can submit to search of articles in the home, even if they are not their own items. Overall, the point of the article is to let people know and provide understanding of their rights under the law about what is permissible and what is not, in the legality of police searching through an individual’s phone, computer or other electronic device.

The **U.S. Patriot Act** was an act voted in to law after the attacks on September 11, 2001. The act itself was voted in, to increase the safety of American citizens from terrorist attacks. The act includes many allowances in dealing with terrorism within the States and abroad. They include: allowing an increase in wiretapping, known as electronic surveillance; allowing for an increase in wiretapping for all communication devices that could be used, not just wiretapping of a certain individual; allows for a reasonable delay in notifying alleged criminals that they are under surveillance, so that more information can be obtained on criminal behavior; allows for increased access to businesses so that government agencies can pinpoint the history of an alleged criminal, this allows for a more comprehensive understanding of an alleged criminals movements; allows for all government agencies like the police, FBI, CIA, etc. to work together when looking into criminal behavior so that the process is more streamlined and information can be shared between the groups; allowing of new technologies to help investigate criminal activity;
allowing technology crimes to be assessed as being the same as a physical crime; increased penalties for those who commit terrorist crimes including increased penalties for harboring a fugitive and for all people involved in the act of the crime, but also the construction of the crime; and elimination of the statute of limitations and increased sentencing penalties (Justice.gov, N.d.). The U.S. Patriot act was voted in to protect American citizens from the threat of terrorism and has been implemented for many years inhibiting or destroying terrorist plans in the years since the September 2001 attacks.

The short film by Crash Course, [Hackers & Cyber Attacks](#) chronicles many aspects of cybersecurity. The film describes two types of hackers: white hats, who try and fix sensitive programming vulnerable to attacks and black hats, who “[may] hack for amusement and curiosity, while cybercriminals hack most often for monetary gain” (Crash Course, 2017). There are many ways that hackers can break into systems which include social engineering which is a way of coercing an individual to give up private information, phishing which is a clone of a realistic website that steals information then uses it on the real website, pretexting, and also, trojan horses which contain malicious malware aimed at stealing data or asking for a ransom (Crash Course, 2017). Besides expressing important information about types of hacks, the Crash Course video effectively communicates the global ramifications of hackers and cybersecurity. Hackers can break into water plants, electrical grids, power plants, airline flight plans, etc., and change or delete important sources of information for these companies which in turn could affect many individuals. For example, if a hacker were to break into an electrical grid database they could manipulate and cut-off power to large cities or communities within an area causing massive destruction and turmoil within these regions. Finally, the film ends with an important statement explaining why it is important to update programming on cell phones or computers to keep data attacks away from spiteful hackers, it is these updates that protect against vulnerabilities.

The hacking threat I chose to learn about, Ransomware, is covered in this article, [Ransomware: A Growing Threat To SMES](#) by Qinyu Liao. Many SME (small to medium enterprise) businesses “still consider spam the number one security risk to their business. While spam is a nuisance, threats such as spyware, phishing and crimeware can pose a greater threat to a firm’s livelihood” (Liao, N.d). Ransomware covers a spectrum of cyberattacks including trojan horses, worms, and spyware, but the reason that Ransomware differs from these other forms of cyberattacks is because, “[the hijacker] Impos[es] serious threats to information assets protection, ransomware victimizes internet users by hijacking user files, encrypting them and then demanding payment in
exchange for the decryption key” (Liao, N.d.). While ransomeware uses well-known cyberattacking vulnerabilities, the difference here is that they expect cash or payment for relinquishment of the stolen information. The cyber-attacker will encrypt the files within the computer system, so that they are unreadable, leaving the victim without any access to the information they need. Once the victim realized they cannot access their information the cyber-attacker will request a ransom to release the files back to the organization. All SME businesses must protect themselves from these kinds of vulnerabilities. According to the article written by Liao, “we will probably get to the point where we are not able to reverse the encryption, as the length of ransomware encryption keys are pushing the boundaries of modern cryptography” (N.d).

The Electronic Frontier Foundation, (EFF) wrote an article, Cyber Security Legislation that examines the two bills, Intelligence Sharing and Protection Act (CISPA) and the Cybersecurity Information Sharing Act, that have been passed. The Acts, introduce legislature that “grant companies broad legal immunity to share more information with the government and private companies” (EFF, Nd.). The goal is so that companies can give information over to government and companies when they feel that a cyber threat hack is seen to be a detrimental to them. However, the bill is extremely vague in what defines an actual attack. EFF writes, “CISPA does not define exactly how far a company can go, leaving it open to the possibility of abuse (N.d). This could mean that private emails and texts could fall within legally obtainable electronic sharing, even though U.S. citizens are supposed to have certain privacy rights within the constitution. The biggest problem with these Acts is that the government could then use any information, even information unrelated to the supposed threat attack, whichever way they deem suitable (EFF, N.d).

The TED talk, Hire the Hackers! presented by Misha Glenny explores the topic of cybersecurity and discusses a different way of approaching this multi-billion dollar industry. Glenny says, “we are at the beginning of a mighty struggle for control of the internet. The web links everything...” (TED Global, 2011). Companies, governments, and individuals cannot escape the impossible greatness of the internet, nor the detrimental aspects of the dark-side of internet hackers. Glenny’s counter offer to the cost of cyber security, is to instead recruit and/or higher the cyber hackers who are disrupting the online system. Glenny shows six instances where the men convicted of hacking were young teenagers, some with certain disabilities, like Aspersers, who all shared the common characteristics of complete understanding of the cyber world (TED Global, 2011). Instead, as he points out, most of these cyber criminals are placed in prison for numerous years, when they could be helping fight the battle for cyber security. Glenny mentions multiple countries that have already implemented the plan to recruit these young hackers before they are arrested and after their prison centers to work with
governments and companies to improve their internet security (TED Global, 2011). Considering the information I found in the article, *Ransomware: A Growing Threat To SMES* by Qinyu Liao, where it is discussed that cybersecurity might reach a threshold that cannot combat cyber hackers, that it may be in the best interest of all, to go directly to the source and hire these young people to implement design techniques that create a safer internet.

**Reply to another student’s thread:**

Catherine-

I really enjoyed reading all of your discussion post subjects. It is interesting to me the different ideas that can be pulled out of the same article and written about. I also, wrote about the *U.S. Patriot Act* mostly because I was hoping to understand the Act better. The different policies that were enforced under this act, seemed to be very legit. However, I have been hearing for years that the Patriot Act was unconstitutional. I found this interesting article, *The Ethics of Government Surveillance*, discusses some of the ethical issues surrounding the governments access to wiretapping and surveillance of an individual or group. It highlights the issue that in the wrong hands, the power it affords could be used for great harm. Although, people want to believe that our government officials are without dangerous desires, the truth is that all humans are vulnerable to weakness. The article proposes the idea that the Patriot Act may be ethically sound based off “utilitarianism [which] uses the ends to justify the means. If a certain decision results in the most positive outcome for the largest number of stakeholders, regardless of what the decision entails, it is ethically justified” (Dan, 2013). However, many find that the Patriot Act gives the government too much access to personal data and privacy of United States citizens. My vote is still in question. I understand the motivation behind the Patriot act, but I still expect my government to give me the privacy afforded under the constitution. My biggest worry, is that it could be used for harm. For example, look at all of the data searches we have had to do for this class in the last few weeks, each student in this class may be subject to some sort of surveillance because of our searches. I can’t say for sure, but it could be deemed "suspicious", which seems strange to me.

Kristina