Privacy

Luis Ortez

Computer Ethics 3080

Final Reflection Paper

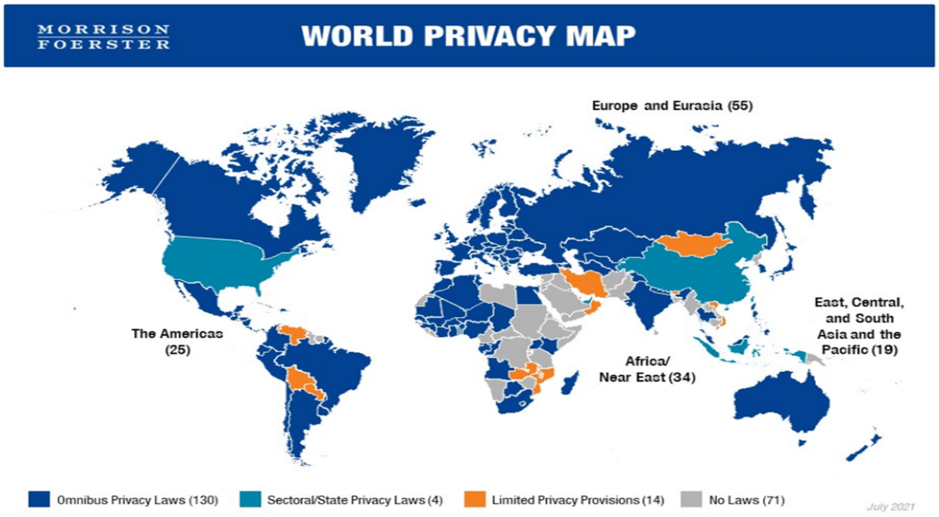
November 30, 2022

Introduction

Privacy is what every human being should have. Privacy is a right not a privilege. Some countries around the world have different opinions about it. Usually, Capitalist countries tend to give their citizens more privacy, but it depends on how the law interprets it, while communist governments tend to be more restrictive towards this issue. Talking about this issue is getting involved into many different topics, for example: Politics and social issues. But to first get started the question we need to answer is, what is privacy? Based on the oxford dictionary privacy is: "the state or condition of being free from being observed or disturbed by other people." The second question that we should ask is: Is privacy a right or a privilege? Based on the United Nations declaration its states: "Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech." As we read this quote, we can see that privacy is a right but why not every country respect that?

There are four states of privacy, these are: solitude, intimacy, anonymity and reserve. Solitude privacy is an open-source privacy analysis tool that enables you to conduct your own privacy investigations into where your private data goes once it leaves your web browser or mobile device. Intimacy privacy is keeping your personal information private. Anonymity privacy is one of the most know states of privacy, is Keeping your identity private, but not your actions, this is a way to be a witness or just commenting on someone's comment without having to give your information. This is one of the most important states of privacy. Finally, reserve privacy is to keep back or set apart.

Nearly every country has the right of privacy in their constitution. What is the importance of privacy? The lack of privacy can inhibit personal development, and freedom of thought and expression. It makes it more difficult for individuals to form and manage appropriate relationships. Why not every country on the map has these rights? Because of regimes governments for them to keep having power. Knowing what your citizens are doing, taking away this right gives you an advantage to know what they think and suppress their thoughts and security. Usually, these countries tend to be third-world countries and because of this lack of rights their citizens have fallen behind in different areas of study that help a civilization grow. Here is a map of privacy around the globe.


MORRISON FOERSTER
WORLD PRIVACY MAP
Europe and Eurasia (55)
The Americas (25)
Africa/ Near East (34)
East, Central, and South Asia and the Pacific (19)
Omnibus Privacy Laws (130)
Sectoral/State Privacy Laws (4)
Limited Privacy Provisions (14)
No Laws (71)
July 2021

As we can see in the picture above privacy is going to depend on the country you are at, every country will have different laws or no laws about privacy. Should we keep using this system? Or should we use a system for every human being on the planet? These are questions that have been asked over at the United Nations conventions about human rights, but nobody has not done anything about it. There are many different types of privacy, but there is one specifically that I want to focus on and that is, Cyber Privacy.

Cyber Privacy

Why we need Cyber Privacy? As Winston's explanation says "The definition of online privacy is the level of privacy protection an individual has while connected to the Internet. It covers the amount of online security available for personal and financial data, communications, and preferences." As we know online privacy is very important, we use the internet everyday where we place sensitive information that hackers are always going to be looking for like credit cards and personal information. We must protect from these "hackers". A hacker is a person or a thing who uses computers to gain unauthorized access to the users' data. Hackers may create programs that search for unprotected pathways into network systems and computers. Hackers may gain backdoor access by infecting a computer or system with a Trojan horse, created by hackers to acquire and steal important data without the victim noticing. Hackers are the main reasons of cybercrime.

Cybercrime is one of the most quickly evolving sorts of crime in our society today, and it has also become a major issue because it does a great deal of damage and impacts us in several ways. But what is cybercrime? Cybercrime is distinguished from traditional crime by its severity. According to reports, this crime is committed via an electronic medium, which eliminates the need for reading, and in secret. Some of the cyberspace-related crimes include cyber fraud, defamation, cyberstalking, harassment, IPR theft, data hostage, cyber warring, phishing, e-mail bombing, cyber war, and unlawful surveillance. Cybercrime is being underrated, we must put more focus on This global issue and start doing a change.

Being a victim of cybercrime can have long-lasting effects. Criminals send phishing emails posing as a bank or other financial institution and requesting sensitive information. If you disclose this information to the criminal, they may be able to access your bank and credit accounts, as well as open new accounts and damage your credit record. Those who are victims of password theft are an additional method or consequence. Every day, more than 1.5 million individuals fall victim to cybercrime, which can vary from the loss of simple passwords to extensive financial fraud. Each year, cybercrime damages the global economy by more than $110 billion, on average costing each victim $197. As customers become more aware of traditional attack tactics, cybercriminals have developed new techniques that combine mobile devices and social media to keep their victims susceptible.

Film piracy is another consequence of cybercrime in our society that must be addressed by copyright laws. This indicates that movies are cloned onto fresh disks and made to appear authentic. The result is that the visuals of these films are diminished, and the presumed standard and style of the film are altered. This tarnishes the reputation of the entertainment sector that produced the film, and the corporation stands to lose a substantial amount of money. Lastly, I'd want to suggest how this cybercrime should be addressed and, if possible, stopped. Applying patches and other software fixes as soon as they become available is one of the most effective methods for preventing computer intrusions. Updating your computer regularly stops hackers from exploiting software flaws that they may otherwise use to get access to your system. While keeping your computer up to date will not prevent all attacks, it will make it much more difficult for hackers to get access to your system, block many simple and automated efforts, and maybe dissuade a less determined attacker from searching for a more vulnerable system. Modern versions of Microsoft Windows and other popular software may be configured to download and install updates automatically, eliminating the need to manually check for updates. Using "auto-update" features in your software is an excellent starting point for maintaining internet security. Also, keep in mind that a freshly obtained computer may not have adequate security for your needs. Focus not just on getting your home computer to function, but also on getting it to function securely. Configuring typical Internet applications, such as your web browser and email client, is one of the most important aspects to focus on. For instance, the security settings in your Web browser, such as Internet Explorer, Fire Fox, Yahoo, and Google Chrome will determine what happens when you visit Web sites on the Internet; the strictest security settings will give you the most control over what occurs online but may distract some users with a barrage of questions ("This may not be secure; are you sure you want this?") or the inability to do what they want.

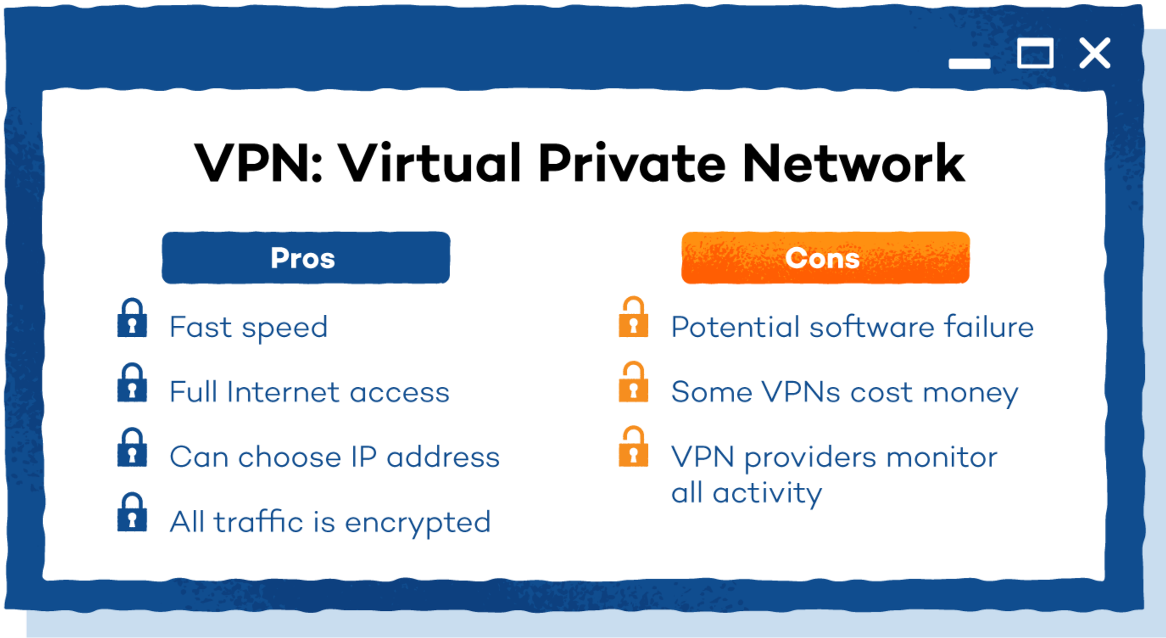
Avoidance of Privacy Attacks

The "Help" section of your software or the vendor's website frequently may assist you in modifying security and privacy settings without requiring specialized knowledge. If you are unsure how to set up it, ask a trusted friend or contact the vendor directly. Choosing a difficult-to-guess password is the first step in keeping passwords safe and out of the wrong hands. Strong passwords consist of a minimum of eight characters and a combination of letters, numbers, and symbols. Avoid using your login name, sensitive information such as your last name, or words from a dictionary as your password. Utilize incredibly robust and unique passwords when it comes to online banking. Maintain the security of your passwords and avoid using the same password for every online account. At a minimum, passwords should be updated every 90 days. This can help limit the amount of harm someone with access to your account can cause. If you uncover something questionable about one of your online accounts, you should change your password immediately. Use passwords that are both strong and unique when it comes to online banking. This can help limit the harm that someone with access to your account can cause. If you detect something suspicious with one of your online accounts, one of the first things you should do is change your password.

The use of VPNs can also protect you if you are connected to a public internet router. “A virtual private network (VPN) is a technology that improves your online security and privacy. When using a commercial VPN service, you connect to a server run by a VPN provider via an encrypted connection. In other words, all data transferred between your computer and the VPN server is scrambled so that no one else can read it.” (National Cybersecurity Alliance). This explains the use of a VPN, but a VPN is not an antivirus, while they will protect your IP and encrypt your internet history, but that is as much as they can do. They won't keep you safe, for instance, if you visit phishing websites or download compromised files.

Keep you information to yourself. Yes, this is your privacy do not share any of your personal information with anyone. Most of the attacks we received is because we have shared the information, sometimes we ourselves are our worst enemy. Do not answer Scam Calls, these are the worst these people are trying to get money from you, now it has gotten easier to identify them. Just do not answer a call, the government or any other person will reach out to you via mail not your phone, unless if they have told you that will reach out to you via phone.

These are just some ways to try and avoid sharing your personal information. As shown below these are the advantages and disadvantages of using VPNs, but they will help you to have more security for your online information.



VPN: Virtual Private Network

Pros	Cons
Fast speed	Potential software failure
Full Internet access	Some VPNs cost money
Can choose IP address	VPN providers monitor all activity
All traffic is encrypted	

Personal Privacy

Our personal Privacy is one of our most important rights as Americans. We have the right to control our personal data and make sure who is shared with. Personal privacy can be as well as establishing boundaries with our family, friends, coworkers, and significant others. Our electronic devices are part of our privacy, putting passwords in these devices mean that you do not want anybody to go thru your personal information and is also a way of security in case it gets stolen.

We as Americans, do we have the right to privacy? The short answer is no. The U.S Constitution does not contain no express right of privacy. But it depends to how I started this reflection; it depends on how the law is being interpreted. There have been some Supreme court cases that have problems regarding the right of privacy. For example: Meyer v. Nebraska (1923), Pierce v. Society of Sisters (1925), and Griswold v. Connecticut (1965). In these cases, the U.S Supreme Court interpreted what the law states about privacy rights depending on if parents were allowed to teach their children their foreign languages to the usage of selling condoms. The law states that every American is allowed to keep their business to themselves but if it's affecting another person the government or any other authority has the right to intervene.

Conclusion

In conclusion these is a reflection about privacy. Making sure about our rights and how to have security on our daily lives. Privacy is a right not a privilege.

Sources

1. Winston & Strawn LLP. "What is the Definition of Online Privacy?". 2022. https://www.winston.com/en/legal-glossary/online-privacy.html#:~:text=The%20definition%20of%20online%20privacy%20is%20the%20level%20of%20privacy,data%2C%20communications%2C%20and%20preferences.
2. Exploring Constitutional Conflicts. "The Right of Privacy". 2022. http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html
3. National Cybersecurity Alliance. "The Importance of using VPNs". March 29, 2016. https://staysafeonline.org/online-safety-privacy-basics/the-importance-of-using-a-vpn/
4. Peter Swire. " Alan Westin's Legacy of Privacy and Freedom". 2022. https://iapp.org/news/a/alan-westins-legacy-of-privacy-and-freedom/
5. Oxford Dictionary. https://www.oed.com/