Sam Zandiasadabadi

Professor Tomasevich

CSC 300GW

10 December 2022

Paper 1 Revision: Online Privacy & its Importance

Privacy is a human right that everybody is entitled to. However, things can get difficult in the digital world. Every website, online article, and even social media platforms are responsible to keep the information of their users private. And the failure to do so might have heavy consequences for both the users and the people responsible for keeping the data safe. In the same way, we have the right to privacy in everyday life, we do on the internet as well. However, it is a lot more complicated than it might seem! If we are in the background of a photo taken in public, do we have ownership of the photo? Can the person responsible for taking the photo publish it online without our permission? Can we take legal action against the publication of the photo? These are all questions, or perhaps topics that we will address by the end of this essay.

There are many vague definitions as to what online privacy means. While some argue that it is not being tracked when using a webpage, others argue that it is more about being comfortable with the content you share online knowing that only your target audience will be able to see it. Depending on each person and the scenario in hand, both statements can be true or false, but neither are necessarily wrong. For the most part, the most common definition of “online privacy” is the level of privacy protection a person connected to the internet has. One might be all alone in a room while scrolling through Facebook, or Instagram. While this person technically has privacy in the sense that there is nobody else in the room to bother, distract, or watch over them, there could be numerous ways in which the person’s privacy can be distorted. An inappropriate or unwanted advertisement can pop up and distract the person without their permission. They might see a comment or a post about someone whom they no longer wish to be in contact with. And quite possibly, the worst situation of them all, a stranger can send them an unwanted and rude message that they did not want to read.

In addition to being exposed to unwanted messages and advertisements, being connected to the internet can bring in other dangers and unpleasant outcomes. Almost every web page or application that exists asks for the rights to track, use, and download the activity details and information of their users. Some sites sell this information to other websites or companies, who will then use the gathered data to contact these people about promotional products. However, things can get a lot worse if valuable information such as credit card numbers, or social security numbers are exposed online. This information can be used to purchase things under a person's name, and they would be responsible for paying them off or facing legal issues in case of serious misconduct. This is why online privacy is extremely important since it gives people control over their identity and personal information. If they are to no longer have control over their personal and sensitive information, then almost anyone can duplicate or manipulate their identity to serve their intentions, whether good or bad.

The internet is constantly changing and evolving every day. According to "internetlivestats.com," a website designed to calculate on average how much activity and traffic the major platforms online experience. About ten thousand new tweets are being posted on Twitter every second. About a hundred-and-six-thousand Google searches and ninety-seven-thousand views are generated on YouTube per second. With this much traffic online, how can we ensure that our privacy remains intact? The answer is to be more cautious. Every time a person joins a new social media platform before they can create their account, they have to agree to the terms and conditions that the company has set for its users. If they choose to agree to these terms, then they have essentially granted the company to track certain data in order to better shape and update their platform. This can either be the terms or items they search for online or the type of discussions that they choose to interact with. For the most part, these are all legal and have no evil intentions or bad outcomes. However, even once a person has agreed to the terms in which what data would be tracked, there are still steps that can be taken in order to better preserve their online privacy.

While some are very protective of their online privacy to the point where they refuse to sign up for social media accounts or share any information about themselves online, others do not care as much and refuse to take precautionary and necessary steps to ensure their privacy online. One of the reasonings for this is that they have a false sense of security that makes them believe they are safe from having their personal information stolen. They also feel comfortable and willing to share details with people whom they know on social media believing that the receiving end of the message is the person that they trust. However, unfortunately, this is not always the case.

As well as having a false sense of security, some believe that in the case of a leakage, they would be unscathed and nothing would happen to them. This is because once they sign up for a social media platform, they believe that they only give their first and last name, or an email account, any of which they are okay with being made public because it is not anything blatantly secretive or of much importance to others. However, the truth is that in this case, their email could then become a target since it is now out there for people to see. In the case of their email getting hacked, then more personal information that would actually be needed to remain private could leak and cause all sorts of problems for a person. In other words, leaking will not just affect one specific thing. Everything is connected in the online world, and if one thing gets exposed, then it opens up the way for more information to be discovered.

Lastly, another reason that I have come across when dealing with people that do not care much about their privacy online, is the fact that they simply fail to see or do not care much about the fact that their information gets leaked. This ties in with the previous case when people fail to see how everything ties in with each other, however, this is worse in the sense that they believe their information is useless compared to many other people's information that has also been leaked is useless and unimportant. They believe that their data would be useless to anyone else so they do not take steps to protect their data or are careless with what they share with others online. However, much similar to the previous case, this can have massive consequences as well.

Data leaks and online privacy issues are extremely common and no one is completely safe from them. In 2019, news broke out that many users of the social media application, WhatsApp, including certain government officials around the world were victims of hacking and data leakage. According to Christopher Bing, and Raphael Satter, in their article "Government officials around the globe targeted for hacking through WhatsApp," WhatsApp filed a lawsuit against the NSO Group, an Israeli hacking tool developer, claiming that the hacker had exploited a security flaw in WhatsApp's servers that led into the hacking of over fourteen-hundred users' cellphones between April 29, 2019, and May 10, 2019. While there is practically no way to completely prevent and stop data leakage or damages to online privacy, there are simple but effective steps that can be taken to further strengthen and protect our online privacy. Committing to sharing less online, using unique passwords, reading all user agreements before signing up for a service, blocking search engines from tracking our data, disabling ad and data trafficking, and using a VPN (Virtual Private Network) while surfing through the internet can all result in better protection of our online privacy.

So far, we know that online privacy is extremely important, and if breached can have harsh consequences. While exposed credit cards or social security numbers online can have terrible outcomes, they are not the only times when things can go wrong. Many of our cell phones include applications that assess and track our location and show it to others to see. An example of this is the Snapchat feature that allows users to share their locations with their friends and family. However, at the time of its creation, not everyone was aware of this fact. In the article "Police warns teens and parents about Snapchat location-sharing," the author Felicia Gans states how the police worries that "Snapchat's playful, easy-to-use appeal to children and teens could lead to an abuse of the new Snap Map feature by those who want to hurt them." (Gans, par. 3). Now Snapchat has made it very clear that this feature exists. However, at the time of the incident, there were people whose location was exposed without their consent. Not because Snapchat wanted to take advantage of them, or put them in harm's way, but because the new update failed to properly announce and state the new feature.

Even when the users are informed of the new changes made in the terms and services of a social media platform, that does not guarantee the users' safety and privacy. Not too long ago, datasets from Facebook were exposed to the internet in April 2019. According to reports by UpGuard, a third-party risk and attack surface management company, in their article "Losing Face: Two More Cases of Third-Party Facebook App Data Exposure", the personal information of well over five hundred million users had been leaked online. These personal information included Facebook ids, account names, and phone numbers. While on the surface, this might not seem like a huge issue, this can be very problematic, since this gives ill-intentioned people on the internet to have access to this information, and allows them to use that to cover their tracks.

Even though there have been many efforts to reduce and manage the traffic of data that is stored online, there are still ways in which sensitive information can find its way into the hands of the wrong people. The invention of data clouds has helped with securing and storing data more efficiently. However, it also allows those with solid coding skills and bad intentions to use their skill and find access to these data. One can hope that with the constant evolution of technology, there will become a day when we have developed and implemented security systems that completely shut off unauthorized users from ever accessing information that they have no business looking for. But the truth is that, as technology improves, and we get to learn more and more about computers and how we can use them, there will always be ways in which these security systems can be breached or compromised, and this allows hackers and unethical workers to keep on leaking personal information. Not only the publication of these personal data will violate the rights of the victims, but it also puts them in dangerous positions where all sorts of illegal activities can get tied to their name, even if they are fully innocent.

An example of this could be the story of the IT professional, Kenneth Gibson, who worked for a software company from 2012 to 2017. Throughout his time working at his job, he stole data from the customers of the company that he worked for. Gibson would use his skills and the stolen data to keep on creating fake PayPal accounts in the name of those people, and kept on wiring and transferring money into those accounts. During this time, Gibson made around $3.5 million dollars. He was eventually caught when using an ATM, since one of the checks he was depositing matched the name of another user which triggered a security response that eventually led to his downfall and arrest.

Lack of online privacy will always be a huge issue as long as we continue to make progress with technology and science. Each day, new algorithms and ideas are introduced and created that endanger our rights to privacy. Keeping one's online privacy allows us to be in control of our identity. If we are not in control of our own identity, then somebody else can take advantage of that and try to manipulate our persona for their own personal gain. There are no definitive ways in which we can protect our privacy, but some practices definitely give us a better chance and put us in a better position. Since a good portion of life and necessary data are now available on the internet and can be found online, it is important to ensure that everyone can have access to them without forsaking or being stripped of their privacy. This is why the Supreme Court made a ruling to enforce stronger protection for the amount of private information that is being posted and stored online.

So to answer the questions asked at the beginning; there are no right answers. A person is allowed to post a picture that they have taken in public unless it is against the constitution or laws of a certain place. If someone is not happy with being in the background of a photo, they can politely ask the owner of the photo to not publish the said picture. However, if the owner of the photo is adamant about posting the photo online, then there is not much that can be done in that situation. Unless the picture is inappropriate, graphic, belittling, or demeaning towards the person, there is not much that can be done to remove the photo. You can take this matter to the court, but if there is nothing morally wrong with the photo, then it cannot be taken down without the owner's consent. Ultimately, online privacy is extremely important and needs to be taken seriously since it gives a person control over their identity.

Works Cited

1 second - internet live stats. (n.d.). Retrieved September 26, 2022, from https://www.internetlivestats.com/one-second/#youtube-band

Bing, C., & Satter, R. (2019, October 31). *Exclusive: Government officials around the globe targeted for hacking through WhatsApp - Sources*. Reuters. Retrieved September 26, 2022, from https://www.reuters.com/article/us-facebook-cyber-whatsapp-nsogroup/exclusive-whatsapp-hacked-to-spy-on-top-government-officials-at-us-allies-sources-idUSKBN1XA27H

Gans, F. (2017, July 9). *Police warn teens and parents about Snapchat location-sharing - The Boston Globe*. BostonGlobe.com. Retrieved September 26, 2022, from https://www.bostonglobe.com/metro/2017/07/09/police-warn-teens-and-parents-about-snapchat-location-sharing/VXric6XsOCDsVmPDhKCbhJ/story.html

How to protect your privacy online (with 10 examples). Aura. (n.d.). Retrieved September 26, 2022, from https://www.aura.com/learn/how-to-protect-your-privacy-online

Losing face: Two more cases of third-party Facebook App Data exposure: Upguard. RSS. (n.d.). Retrieved December 10, 2022, from https://www.upguard.com/breaches/facebook-user-data-leak

Reno Man sentenced to four years in prison for creating over 8,000 fraudulent online accounts with stolen identities to commit $3.5 million fraud scheme. The United States Department of Justice. (2018, July 30). Retrieved December 10, 2022, from https://www.justice.gov/usao-nv/pr/reno-man-sentenced-four-years-prison-creating-over-8000-fraudulent-online-accounts-stolen

Rogers, P. R. (2021, April 30). *Supreme Court ruling adds privacy protection for the Digital age*. GovTech. Retrieved September 26, 2022, from https://www.govtech.com/public-safety/supreme-court-ruling-adds-privacy-protection-for-the-digital-age.html