

Online Privacy

The internet is a vast, infinite space filled with unlimited opportunities to invoke any desire within one's creative mind. One could even say it is the digital expansion of reality that we as humans express ourselves in a different plane of existence. With this existence it's important to note that many people expect the basic rights of a person who lives within a society (like that of the United States of America) to be transferred over to the digital realm. One of these basics rights is the right to privacy. The things a person conducts behind closed doors are private and so the deeds they conduct on their own personal machine or browser should also be conducted privately if they wish to have it done like so. However, this is not always the case. Especially in today's day and age, a teenager, even kids from what I've witnessed, are able to acquire your personal private information with ease. Personal information is the equivalent of gold on the internet, as it can grant access to things that are not meant to be easily given access to. Your name, age, address, hobbies, goals and aspirations, physical characteristics, are all considered personal information that can be used against you in different ways.

In an article written by Lemi Baruh, titled "Online Privacy Concerns and Privacy Management: A Meta-Analytical Review.", I learned that there are multiple forms of data extraction, and the reasons behind the desperate need for data and why it's so valuable. Any information that is gathered on you, is analyzed and perhaps sold by platforms and social

medias to their affiliates and partners. Chances are if you were born within the last 30 years, prior to your consciousness of it, you already existed on the internet and there was a compilation of data about you somewhere out there already without your knowledge. A lot of information may seem miniscule and unimportant, such as information like your place of study, or your favorite animal. These platforms can collect, process, and profile all that data into statistics that are ready to be sold. Some of the data is not specifically personal to you, but it counts you as an added statistic to a population. By agreeing to the terms and conditions of a website when you sign up or register to use their services, you might be agreeing to sharing your data with people you might not want to share it with. Along with including yourself as a statistic in a larger whole population. A lot of the information that you share that you initially may think is private between you and the platform may be something like your geo location. Services like Snapchat and Facebook request this data from you in order to improve their software. But at the same time, you don't know what those companies are doing with that information after they extract it from you. After all it is a live feed of your location, you don't just get to pick and choose when you share that information. Once the "Allow" button is pressed, that application or service has full access to your location. You can always turn this off in the settings later, but while it's on you may never know what exactly is being done with that information that you choose to share with the platform, willingly or unwillingly. Baruh lists a series of variables along with their included measures, one of which is the "Online service use/intention to use online services" variable, and its included measure included "location-based services" which means to whatever extent the service may require, they are able to work with that information and data however they like.

In another article by Hongliang Chen, titled “Securing Online Privacy: An Empirical Test...”, they discuss how the internet is becoming a “major avenue for the business transactions of corporate users and other individuals”. Keep in mind this article is about 4 years old, discussing information from a few years before its time. Yet, E-commerce sales have steadily been increasing up until and even after the publication date of this article. Especially this last year with the introduction of the Coronavirus, people have opted much more often towards online shopping and shipping compared to the usual walk in, buy what you need, walk out method that we’ve been used to our whole lives. Though with the introduction of new business styles and methods, comes with the introduction of new internet scams and fraud acts to claim more victims. Chen claims that in 2014 the reported financial loss of Internet scams amounted to more than “\$800 Million” in 2014 alone. A lot of the methods used by scammers and other criminals is abled by the leak of private information and data that is willingly left unsecure by people who don’t take their privacy seriously or share information that they are shooting themselves in the foot within the long run.

Susanne Barth and Menno De Jong wrote an article titled, “The Privacy Paradox...” that touches on the bare minimum people actually do to cover their online privacy. The privacy paradox as they discuss deeply goes like this; a user may show that they’re very concerned about their online privacy, but they undertake very little precaution to protect their personal data. The truth behind privacy is problematic because most people who want to use a platform to reach an audience must agree to a list of terms and conditions provided by said platform. For instance, if a public figure wants to reach out to a wide audience on Facebook or Twitter, they must agree to the terms and conditions. These terms and conditions may or may not use the information you provide them with and sell/share it with 3rd parties. Some information may not be as important as

others, for instance your birthday and general appearance description. But what if someone wants to know what your wife looks like, or your children? That picture that was posted of you and your family is now easily accessible to that person and whatever other organization wishes to find that information. In order to avoid this information being leaked to the public, the best way is to abstain from the use of social media. Though the other paradox stays existent, where if you wish to reach out to a larger audience, you must agree to these terms and conditions of parts of your privacy being widely available to the public online.

To sum up everything that has been stated so far, privacy is a very delicate subject in the eyes of the online community. It can easily be broken and although people tend to regard it as something that is very crucial to keep safe, they often do not reciprocate that attitude within their actions. In order to really practice proper privacy, you must take caution in what you choose to share online. Even if privacy is guaranteed by the platform, that information that is lobbed onto the internet is there forever. Even in past circumstances, platforms like “Snapchat” claim to erase your data and information and pictures once you send them, but police files have shown that if needed, the police can request that information from Snapchat to be received and analyzed in order to be used against the user. This was in their terms and conditions at the time of release. It’s also important to note that information posted by others can also be used against you even if you don’t use social media. Information about your devices, from which you have previously logged on to social media, can share your location, operating system, device settings, and even information on your browser history and keywords entered to searches can all be shared with 3rd parties. Not only can others profit off of your lack of online security, but you put yourself and your close ones at risk of leaking their privacy as well. So, if you don’t take the privacy issue seriously, you could face mild or even serious repercussions one way or another. It’s true that

being transparent is good if you have nothing to hide, but at the same time you don't want your life to be like a glass wall for everyone to peer in and see what all your business is about.

References

- Baruh, Lemi, et al. "Online Privacy Concerns and Privacy Management: A Meta-Analytical Review." *Journal of Communication*, vol. 67, no. 1, 2017, pp. 26–53., doi:10.1111/jcom.12276.
- Chen, Hongliang, et al. "Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors." *Computers in Human Behavior*, vol. 70, 2017, pp. 291–302., doi:10.1016/j.chb.2017.01.003.
- Barth, Susanne, and Menno D.T De Jong. "The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review." *Telematics and Informatics*, vol. 34, no. 7, 2017, pp. 1038–1058., doi:10.1016/j.tele.2017.04.013.