The Importance of Online Data Privacy

by Raymond Wray

With the advent of the internet in the 1980s, the world changed forever. If an average individual from just one hundred years ago was transported into modern society, he would probably be astonished at the concept of a global web of information that can be instantly accessed almost anywhere at any time. This displaced individual would be even more perplexed when they learned of the lack of caution that people use when entering their own information into this web. Our online habits would likely be viewed as the equivalent of someone standing in a town square and screaming their deepest secrets. Yet, society has become increasingly dependent on the digital world. Billions of people access the internet every day, and an unimaginable amount of information is processed every second. Because of the increasingly universal nature of the internet and the dangers it poses, it is more important than ever to be cautious of how personal data is handled.

Online data collection by corporations is undoubtedly one of the strongest catalysts of irresponsible information handling. Social media companies in particular have spurred a huge increase in the probability that information posted on the internet will not stay private. As recently as 2021, more than half a billion Facebook users had their profile data lifted from the site and posted publicly (Bowman). Perhaps just as notably, Facebook had no intention of even notifying its users of this breach because of "…the fact that the information was publicly available and that it was not an issue that users could fix themselves" (Bowman). This data breach is more than enough cause for concern, but the response from Facebook itself should be just as disturbing. In an ideal world, corporations should be fully transparent with their clientele. The fact that Facebook didn’t prioritize notifying its users of this massive invasion of privacy is proof that social media companies don’t necessarily have the best interests of their users in mind.

It could be argued that the importance of Facebook’s data leaks is lessened because most young people nowadays would rather use other social media sites. Unfortunately, the danger of exploitation is just as present elsewhere. For example, TikTok is undoubtedly one of the most popular apps in 2022, but there have been repeated calls to remove it from app stores because it “poses an unacceptable national security risk due to its extensive data harvesting … combined with Beijing's apparently unchecked access to that sensitive data" (Umawing). The average person, regardless of age, more than likely has either a Facebook or TikTok account. Therefore, the risk of data leaks encompasses a huge demographic of social media users. Data protection should not be neglected just because someone uses one social media site instead of another.

Even when faced with an event like Facebook’s 2021 data breach and the vulnerabilities of TikTok, skeptics may insist information obtained from social media is probably not that useful. After all, how much harm could possibly be done with just a relationship status, gender, or birthdate? This assertion can be addressed by a rather simple quote from a 2018 Consumer Reports article. Justin Brookman, the director of privacy and technology policy for Consumers Union, points out “…information can also be used to crack account security information or scam you and your friends” (St. John). In other words, social media users shouldn’t be lulled into a false sense of security. Even if Social Security numbers and banking information isn’t being posted for everyone to see, other less specific data can still be used as important clues in the effort to access truly personal details.

The threat that social media poses to information security should be obvious, but financial sites have also proven to be sources of extensive data leaks. While this age of constant interconnectivity makes social media almost a necessity, some people choose to abstain from these popular platforms because they recognize the inherent dangers. In this case, the question that must be posed is whether or not the personal data of these digital “black sheep” is any safer than those who post their entire life story on the internet. The answer is yes, but not by as large of a margin as one might think. The increasingly rare path of no social media is a commendable decision, but it creates vulnerabilities in other areas. Those who are unfamiliar with the internet may be more susceptible to spam calls and emails. Unfamiliarity with hacking tricks such as phishing, combined with a general blindness to internet culture, can considerably hinder anyone’s ability to keep their online data secure. However, the dagger in the heart of the older population’s information security lies in their finances.

Those who do not use social media at all are likely older, which means those people are more likely to be conscious of their money. Anyone with financial aptitude is almost certainly monitoring their credit score through agencies such as Equifax, TransUnion, and Experian. Unfortunately, these credit reporting agencies are vulnerable to data breaches as well. Before Facebook’s leaks in 2021, Equifax suffered a major data breach in 2017 that exposed the financial information of 147 million Americans. Mariam Baksh, a Nextgov senior correspondent who reports on federal cybersecurity, gave more detail about the Equifax incident. In her report, Baksh mentions that the U.S. Justice Department “charged four members of the Chinese Public Liberation Army with responsibility for what it says is the largest theft of personally identifiable information—and trade secrets—by a state-sponsored actor” (Baksh). In that same report, former FBI Deputy Director David Bodich was quoted saying, “…the Equifax hack fits a disturbing and unacceptable pattern of state-sponsored computer intrusions and thefts by China…" (Baksh). This concentrated hacking effort is a clear sign that personal information on the internet is not only open to exploitation, but it is valued by criminals and foreign nations.

There is a critical parallel that must be examined between the Equifax hack of 2017 and the Facebook data breach of 2021. Equifax's CEO learned of his company's hack at the end of July 2017, but this knowledge was not disclosed publicly until months later on September 7 (Moyer). In fact, it took a considerable amount of time for the data leak to reach all of the appropriate people just within Equifax itself. It was reported that Equifax's former chief executive "waited nearly three weeks to tell the company's board of directors about the now infamous data breach" (Moyer). Although Facebook and Equifax both suffered some of the largest data leaks in history, both hesitated to immediately disclose these events to the public. This lack of immediate transparency is a telltale sign that these companies often prioritize themselves over protecting their userbases and the vast amount of data they possess.

The common theme of data theft between social media and financial sites is vital to consider because it helps encapsulate the far-reaching nature of the threat, but even that does not paint the full picture. An individual citizen can be affected by a lack of data privacy, even the national security of an entire country can likewise be compromised. However, it is a mistake to believe the exploitation of data always occurs from the outside in, or always originates from an easily combatable source. An organized effort from a foreign nation to illegally gather data, or hacking attempts from someone as close as a next-door neighbor is fairly easy to rally against. Criminals we can point our fingers toward are easier to defeat because they are tangible threats, but exploitation from less specific sources also exists. Malicious use of personal data has expanded to a world-wide scale that can be difficult to counter due to the complicity of international laws and relations. This far-reaching and less specific manipulation can make defending online privacy even more difficult than it already is.

Although his motivations can be debated, Edward Snowden entered the public eye in 2013 when he released classified information about global surveillance from his time in the CIA and NSA. Despite denials from the companies in question, Snowden unveiled evidence that the NSA has global surveillance programs in place which utilize "collaboration with tech companies like YouTube, Skype, Google, and Apple" (West). Snowden's revelations should generate a sense of great alarm in anyone who accesses the internet. The exploitation of online data is not confined to a few vigilantes or even just a few countries, it is a global effort undertaken by some of the most powerful organizations that have ever existed.

Spying through online data can be twisted to seem beneficial, and on some levels it can aid law enforcement, but look no further than George Orwell's novel *Nineteen Eighty-Four* to see the potential end result of mass surveillance. In the novel, Orwell predicts a dystopian reality where an individual's every move is monitored by government entities. The protagonist laments that he has to live "…in the assumption that every sound you made was overheard, and, except in darkness, every moment scrutinized" (Orwell 3). It may seem unbelievable that we could ever reach the point that Orwell describes, but we cannot truly know how data collection may ultimately shape civilization. The internet and the ability to gather data on a global scale is still an extremely new tool that society has in its possession. Either way, the facts that Snowden provided to the world in 2013 about global surveillance programs show that Orwell's predictions in 1949 hold considerable merit.

The risks associated with entering personal information on the internet will only increase, but there are also benefits to mass data collection. As the internet ages, it is natural that more and more data will enter into the digital world and the likelihood of data exploitation will be greater. On the other hand, the continual profiling and analysis of online data has the potential to lead to exceptional breakthroughs. The synthesis of healthcare data, for example, has many benefits. Data collection of healthcare records enables the analysis of “large datasets from thousands of patients, identifying clusters and correlation between datasets, as well as developing predictive models” (Batko). Without this type of analysis, it could take healthcare professionals much longer to notice trends and reach conclusions on effective treatments. Simply being able to maintain an online database of medical information instead of keeping manual records for every patient is reason enough to value the internet’s capabilities.

When considering the dangers of online data security, it is important to stay optimistic instead of getting bogged down in the negativity of possible exploitation. Many factors such as social media, crony capitalism driving corporations, hackers from foreign nations, and global surveillance showcase the importance of why data privacy matters. Nevertheless, society has advanced exponentially in the past few decades. Online data collection has played a pivotal role in our ability to socially network and analyze information on levels we have never experienced before. In spite of the risks, the internet remains an incredible and revolutionary tool that opens gateways to all sorts of opportunities. As we move forward with this tool in our collective grasp, we must simultaneously be vigilant of risks and ensure that online data collection is used to the benefit of humanity as a whole.

Works Cited

Baksh, Mariam. “Chinese Military Officers Hacked Equifax, Justice Department Says.” *Defense One*, 10 Feb. 2020, https://www.defenseone.com/technology/2020/02/chinese-military-officers-hacked-equifax-justice-department-says/163013/. Accessed 14 Nov. 2022.

Batko, Kornelia, and Andrzej Ślęzak. “The Use of Big Data Analytics in Healthcare.” *Journal of Big Data*, U.S. National Library of Medicine, 6 Jan. 2022, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8733917/. Accessed 16 Nov. 2022.

Bowman, Emma. “After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users.” *NPR*, 10 Apr. 2021, https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users. Accessed 14 Nov. 2022.

Moyer, Liz. “Equifax's Then-CEO Waited Three Weeks to Inform Board of Massive Data Breach, Testimony Says.” *CNBC*, 3 Oct. 2017, https://www.cnbc.com/2017/10/02/equifaxs-then-ceo-waited-three-weeks-to-inform-board-of-massive-data-breach-testimony-says.html. Accessed 16 Nov. 2022.

Orwell, George. *Nineteen Eighty-Four*. Secker & Warburg, 1949.

St. John, Allen. “Here's What Makes the Facebook Data Breach so Harmful.” *Consumer Reports*, 12 Oct. 2018, https://www.consumerreports.org/digital-security/what-makes-the-facebook-data-breach-so-harmful-a8227559641/. Accessed 14 Nov. 2022.

Umawing, Jovi “TikTok Is ‘Unacceptable Security Risk’ and Should Be Removed from App Stores, Says FCC.” *Malwarebytes*, 5 July 2022, https://www.malwarebytes.com/blog/news/2022/07/tiktok-is-unacceptable-security-risk-and-should-be-removed-from-app-stores-says-fcc. Accessed 16 Nov. 2022.

West, Angus. “17 Disturbing Things Snowden Has Taught Us (so Far).” *The World*, 9 July 2013, https://theworld.org/stories/2013-07-09/17-disturbing-things-snowden-has-taught-us-so-far. Accessed 14 Nov. 2022.