

PRIVACY AS A RIGHT

Edward Snowden, a former agent of the National Security Agency (NSA), once said, “Ultimately, saying that you don’t care about privacy because you have nothing to hide is no different from saying you don’t care about freedom of speech because you have nothing to say.” Privacy is an evermore important and relevant right that is constantly being violated by companies and governments alike. Not only does privacy facilitate trusting exchanges between users, companies, citizens, and governments, but it even improves the standards for open communication. Currently, there is minimal privacy legislation in the United States, and these laws are extremely fragmented. In a few states, there is legislation, but in the other states, the legislation has died in a committee. Only six states have legislation that is actively being worked on. So far, no federal legislation has been passed that defends users’ rights over all types of data, and thus most consumer data is not protected.¹ In the European Union, however, General Data Protection Regulation (GDPR) has been passed which provides a stepping stone into a safer world. Even though there are many valid concerns with government regulation of personal freedoms, Congress should pass legislation that protects the privacy of internet users because such privacy is necessary for an open society, is a fundamental right, and creates a transparent relationship of trust between users and companies.

Statistics show that there is a growing interest in privacy legislation. In a survey of Americans by Pew Research, more than three-quarters of respondents were concerned by companies’ collection of their data. In their analysis of the data, Pew Research said, “Almost all Americans have been asked to agree to privacy policies, but fewer actually read them.” Looking at the data, only 6% of respondents said they understood how companies used their personal data, and 81% said that they see more risk than benefit in sharing their data. One more terrifying metric is that 84% percent of respondents do not feel that they are in control

¹ Thorin Klosowski, “The State of Consumer Data Privacy Laws in the US (And Why It Matters)” The New York Times, September 6, 2021, Accessed February 12, 2023, <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/>

over their data.² It is evident that users want to control their personal data and that they want to know how their data is being used. In regards to the user's knowledge of how their data is utilized, most sites in the United States are required to have a privacy policy. Currently, this privacy policy is often written in complicated legal language. Unfortunately, the complex wording of the policy leads to users avoiding the reading of it and even being confused over how their data is used.³ In the EU, this issue is alleviated by the requirement of a clear document that tells a user how their data is used.⁴ The same policy regulating this, called the GDPR, also grants users the right to take control of their data and decide who can access it. Research shows that there is public interest in privacy and that the interest is growing.

Privacy is necessary for an open society because it allows one to communicate freely, without fear of government regulation, and with software that is not defective by design. Without privacy, companies and governments can spy on users, employees, and civilians. Whistle blowers, civil rights activists, and even average civilians may have a difficult time sharing their information that could be extremely crucial to improving society as a whole.⁵ Currently, all of these people only have limited freedom to privacy. In fact, the U.S. Congress has been pressuring big tech companies for decades to install “back doors,” or a way to bypass security measures, into their products! The NSA has also been tracking and tagging user data in a huge database, and in an highly illegal, unwarranted, and unconstitutional way.⁶ This drift towards “anti-privacy” or “big brother” regulation is a dangerous move in the wrong direction. Instead, better legislation and amendments should be passed to prevent these anti-privacy regulations and injustices. Privacy regulation that

² Brooke Auxier and Lee Raine, “Key Takeaways on Americans' views about privacy, surveillance and data-sharing” Pew Research Center, November 15, 2019, Accessed February 12, 2023, <https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/>

³ Klosowski.

⁴ Ben Wolford, “What is GDPR, the EU's New Data Protection Law?” Proton AG, May 26, 2022, Accessed February 5, 2023, <https://gdpr.eu/what-is-gdpr/>.

⁵ Edward J. Snowden, *Permanent Record*, (United States: Metropolitan Books, 2019), 531-535.

⁶ Snowden, 14.

properly enacts free communication without “back doors” could stimulate an open society, allowing it to bloom and flourish.

Privacy is a fundamental right that is supported by the GDPR and mutually supports the Bill of Rights. Currently, U.S. regulators have chosen to only prioritize the privacy of three specific data classes: healthcare, financial, and children.⁷ However, privacy is an all-encompassing right just like the right to free speech, religion, and press. This right is being violated in numerous ways today. Companies are mishandling data, as observed in the Facebook and Cambridge Analytica scandal, and governments are spying on civilians, such as the NSA surveillance revealed by Edward Snowden. Privacy regulations are the way to minimize this problem. In a way, the Fourth Amendment to the constitution already grants this right by preventing unreasonable searches and seizures, and the GDPR already discourages companies from misusing data,⁸ but this preexisting regulation is still not enough. However, big tech organizations such as Facebook and Google still attempt to unlawfully collect data. Some companies are still willing to pay the fine imposed upon them by the GDPR, and the Fourth Amendment is unable to be enforced because the collection is considered to be confidential.⁹ On the other hand, some organizations, such as the Electronic Frontier Foundation (EFF) and Mozilla, fight for user’s rights and call for privacy-respecting legislation. In some cases, the EFF has even fought in court on consumers’ behalf. Companies like these help offset the lack of legislation to protect users’ rights. Strict privacy laws need to be passed that force governments and companies alike into compliance that is auditable and to make them recognize privacy as a right.

If properly regulated, a transparent relationship of trust between users and companies allows one to share information with confidence in how the information is being

⁷ Theresa Payton and Ted Claypoole, *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*. (United Kingdom: Rowman & Littlefield, 2014), 229

⁸ Wolford

⁹ Payton and Claypoole, 230.

used. In today's society, many people share their information in the blink of an eye, with no concern and no regard to how their data is being processed because it is necessary for everyday life.¹⁰ However, this only makes up some population of the internet, and there are still those who are wary of how their data is handled. The GDPR already requires that companies share with users how they process their data in a "concise, transparent, intelligible and easily accessible form, using clear and plain language."¹¹ The U.S. as a whole does not have a similar policy yet. However, some states, like California, that help protect users' rights in their states. This document explaining the use of data is backed by law in the European Union,¹² and allows users to grant companies the right to their data with confidence. These users can even make companies delete their data or temporarily pause the collection of their data,¹³ maximizing users' control over their data. Since it is legally binding, users can know with certainty that their data is being processed according to those terms. This transparency can even be enhanced by an open source license which allows users themselves to audit the code using their data. Because of this control, users may be more likely to trust companies with their information. Privacy legislation greatly benefits users and companies by facilitating trusting relationships.

By looking at the benefits of privacy legislation, one can conclude that legislators should pass laws that protect internet users' privacy since privacy connects an open society, is a fundamental right, and creates a transparent relationship of trust between users and other entities. Privacy allows all to confidently communicate without fear of malicious actors, be they governments and corporations or hackers, to intercept personal information. Without privacy, those fighting for good in society could meet roadblock after roadblock on their quests to unlock key information. Privacy legislation is already supported by existing articles,

¹⁰ Marc Goodman, *Future Crimes: Everything is Connected, Everything is Vulnerable, and What We Can Do About It?*, (United States: Doubleday, 2015), 89

¹¹ Wolford

¹² Wolford

¹³ Wolford

laws, and amendments, such as the GDPR in the EU and the Fourth Amendment. New legislation will help further the mission for user rights and safety. Finally, privacy legislation regulates and enforces the preexisting user agreements such as privacy policies. Such legislation will expand users' rights and limit companies' overreach. In conclusion, politicians should make efforts to pass these privacy laws to protect users, both now and in the future.

Bibliography

- Axier, Brook and Lee Rainie. "Key takeaways on Americans' views about privacy, surveillance and data-sharing" Pew Research Center. November 15, 2019. Accessed February 12, 2023. <https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/>.
- Goodman, Marc. *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do about It*. United States: Doubleday, 2015.
- Klosowski, Throin. "The State of Consumer Data Privacy Laws in the US (And Why It Matters)." *The New York Times*, September 6, 2021. Accessed February 5, 2023. <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/>.
- Payton, Theresa, and Ted Claypoole. *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*. United Kingdom: Rowman & Littlefield, January 16, 2014.
- Snowden, Edward J. *Permanent Record*. United States: Metropolitan Books, 2019.
- Tapscott, Don, Alex Tapscott. "Why Transparency and Privacy Should Go Hand in Hand." HuffPost. May 25, 2011. Accessed February 5, 2023. https://www.huffpost.com/entry/why-transparency-and-priv_b_643221.
- Wolford, Ben. "What Is GDPR, the EU's New Data Protection Law?" Proton AG. May 26, 2022. Accessed February 5, 2023. <https://gdpr.eu/what-is-gdpr/>.