Privacy in Cyberspace

PUBL363 - Policy Brief - Mehul Sen

Introduction

According to an article published by Joseph Johnson on statista.com, internet users worldwide spend an average of 155 minutes daily on a mobile device and 37 minutes on a computer in 2021[5]. The internet has revolutionized how humans interact with each other. With the advent of various digital technologies such as online forums, instant messaging, and social networking, people spend a considerable amount of time online, accessing websites and sharing information. This shared data contains crucial details about an individual's interests, hobbies, jobs, and income sources. An individual's data defines their role on the internet. This is why tech companies and organizations collect some of this data and use it for targeted advertisements and user statistics. Striking a balance between privacy and data regulation is becoming increasingly critical in today's cyberspace. It is essential to develop effective privacy laws that consider the ever-changing technical landscape and security perspective. This should not be overlooked.

Audience

The government has the power to regulate how companies collect data. They can pass and modify laws that limit the data collected by both companies and the government. For instance, Europe's Data Protection Law is an example of this power in action. Although the General Data Protection Regulation may not be perfect, it does give people greater control over their data. According to Alison Cool, the law's right to be forgotten aspect enables individuals to compel companies to erase some of their data, which helps them regain ownership of their online identity[1]. The effectiveness of the GDPR shows that having legal frameworks in place to govern privacy and data collection is useful. Policymakers and courts can learn from the GDPR's shortcomings and use them to create practical and empirically grounded rules that safeguard individuals' privacy.

The Privacy Problem

Privacy is a crucial aspect of our daily lives that people tend to overlook while accepting terms and conditions agreements. However, privacy is much more important than people assume it to be. It intersects with various human rights such as freedom of expression, the right to seek, receive and impart information, and freedom of association and assembly. Privacy prevents large groups from using individuals' data for their personal gain, as seen in the Cambridge Analytica Scandal where the organization unlawfully used personal data to influence voters of a particular party by showing them targeted political ads.

Privacy also ensures freedom of speech and thought. An individual's privacy allows them to share anything and everything they wish to share with the world without the fear of being monitored and tracked. This allows individuals to engage in conversations regarding various topics including politics, giving them the ability to share their opinions with the world without being linked back to them as an individual. Privacy allows people to put on the facade of being a nameless faceless user online, and what they choose to do with this ability depends on each person behind the facade.

A world without privacy would be an authoritarian world, where absolute power would lie with those controlling access to individual data. They would be able to foresee every move, motive, and get into people's minds, shaping the world in whichever way they want. People would be criticized for any opinion that stands out of the norm, their personal and online life would no longer be private, and every action they take would be monitored and recorded. History has shown that complete authoritarian rule does not work. To form trust, promote growth, and protect the rights of citizens, privacy must be maintained.

Privacy vs Security

Even though privacy is an essential aspect of governance, complete and total anonymity is also not viable. Without any governance or privacy, people are no longer obligated to follow laws and rules outlined in the past. They can no longer be kept accountable for their actions and may harm others, taking away others' rights and privileges. This applies equally in the digital world; black hat hackers and individuals with malicious intent often hide themselves using proxies and encryptions. Using these techniques, they can effectively render themselves invisible, completely hiding their location or information about the device they use during the attack. This makes it very difficult for the authorities and the defenders to kick them out of the network and ensure they stay out once detected. Having weaker privacy gives way to more robust security, and it is up to the governments and policymakers to ensure how much privacy is provided to the citizens. Certain countries, like Russia and China, have very little to no digital privacy for their citizens. Their online activities get tracked and monitored. Encryption and VPN technologies are prohibited, making it easier for the government to track everything and trace it back to individuals, thus maintaining the idea of accountability.

The government, however, is one of many players that benefit from a lack of privacy; private companies and advertisers also profit from the collection of data being shared online. Companies like Facebook and Google then use this data to build proles or digital dossiers on each accessing their resources[4]. These dossiers allow these organizations to build up targeted advertisements, presenting individuals with products they believe would have the highest chances of being sold. Advertisers do not benefit from increased data privacy laws since, with the increase in data regulations, their access to detailed dossiers dwindles, severely affecting their business model. Apart from advertising, companies also store this user data to improve their current services and provide detailed statistics on the services they provide. Privacy is also at risk when this collected user data is shared among organizations, private companies, and government. An example would be telecommunication companies sharing user data with the governments to facilitate their intelligence.

The idea of privateering security, as described by Florian Eglo, where private companies actively participate in defensive capabilities, including ensuring security, brings up privacy issues[3]. Private companies are victims of the majority of cyber-attacks. Due to this, they can no longer rely on the government alone to act against the attacker. Aside from focusing on improving their defensive capabilities, companies are also looking into ways to attack their attackers quickly. For example, if a company, let us assume A, decides to incorporate to ensure security capabilities within their network. When they are attacked by party B, Offensive security allows A to attack B back to get more information about B. Private companies are starting to use different variations to ensure security, such as Cyber Deception, Disruption, and Preemption, which NAS discussed thoroughly in their book At the Nexus of Cybersecurity and Public Policy[6]. While sounding great theoretically, offensive security has its own set of issues that need to be considered. The ability to attack your hackers in cyberspace changes our definition of attacks and malicious users. Instead of defining every attack on a system as malicious, the context behind that attack also starts to be

considered when defining an attack as acceptable. Josephine Wolff outlines the risks brought on by offensive security very well.

This idea of hacking back the attackers perfectly summarizes the issues we face today with privacy. On the one hand, the privacy of the companies and the user data that they store themselves needs to be protected from attackers. However, on the other hand, while using offensive security, companies attempt to get information on their attackers, be it using beacons that ping back to the company servers when stolen, or certain backdoors that are opened on B's side allowing A to retrieve their stolen data. Privacy can be compromised under the pretense of maintaining security and ensuring the attackers get punished; however, it can break the very privacy laws that the organization was protecting in the first place. This leads us to consider the risks and possibilities associated with privacy before taking action.

Solution

Implementing stable and effective privacy protocols brings us back to implementing policies and passing laws like GDPR. Even though they have many drawbacks, some of which are that it is staggeringly complex. We know that it works. It provides a sense of trust between both the client and the companies aggregating their data. GDPR also allowed for better decision-making and risk assessments[2]. Policymakers should take extensive feedback from GDPR itself and further improve on its drawbacks. It is evident that dealing with data privacy is complicated, and more than a couple of perspectives need to be considered. The implementation of a firm, well-defined policy that collaborates with all fields of this ecosystem, including representatives from the government and the private sector, and keeping in mind the data privacy for citizens and consumers using services offered by companies could give rise to legal frameworks and privacy laws that are effective.

References

[1] Cool, A. (2018, May 15). Europes data protection law is a big, confusing mess. Retrieved from https://www.almendron.com/tribuna/europes-data-protection-law-is-a-big-confusing-mess/

[2] Dubrova, D. (2018, Apr). The App Solutions. Retrieved from https://theappsolutions.com/blog/development/gdpr-challenges-and-benefits/#:~:text=ThemostobviousbenefitofGDPRistrust,theirtrustworthinessintheeyesoftheusers.

[3] Eglo , F. (2015). Cybersecurity and the age of privateering: A historical analogy

[4] Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In Proceedings of the 2005 acm workshop on privacy in the electronic society (p. 7180). New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/1102199.1102214 doi: 10.1145/1102199.1102214

[5] Johnson, J. (2021, Jan). Daily time spent online by device 2021. Retrieved from https://www.statista.com/statistics/319732/daily-time-spent-online-device/

[6] Wolff , J. (2017, Oct). Attack of the hack back. Slate. Re trieved from https://slate.com/technology/2017/10/hacking-back-the-worst-idea-in-cybersecurity-rises-again.htm