PUBL363 Policy Brief

Privacy in Cyberspace

Mehul Sen

May 2021

1 Introduction

As published by Joseph Johnson on statista.com, the average daily time spent online by internet users worldwide in 2021 is around 155 minutes on a mobile device and 37 minutes on a computer (Johnson, 2021). The internet has had a major impact on how humans interact with each other. With the emergence of digital technologies like online forums, instant messaging, and social networking, humans spend a lot of their time online, accessing websites and sharing data. This shared data contains important information about the individual generating that data. This can be anything from their hobbies and interests to their jobs and source of income. An Individual's data defines that individual's role on the internet. This is also the reason why tech companies and organizations collect some of this data and use it for targeted advertisements and generating user statistics. Finding a balance between privacy and data regulation is becoming increasingly important in today's cyberspace. Coming up with effective privacy laws that take into consideration the ever-changing technical landscape as well as the security perspective into consideration is very important and should not be overlooked.

2 Audience

The government is capable of changing how data gets collected by companies. They have the power to pass and modify bills that limit the data collected by companies as well as the government. We have already seen this in work with Europe's Data Protection Law. Even though the General Data Protection Regulation is far from an ideal law, it does provide people with greater control over their data. As described by Alison Cool, the "right to be forgotten" aspect of this law allows citizens to force companies to erase some of their data allowing them to regain ownership of their online identity (Cool, 2018). The General Data Protection Rule(GDPR) proved that having laws and legal frameworks in place which govern privacy and control data collection prove to be effective and useful. Policymakers and courts can learn from the mistakes made while creating the GDPR and build on them to create "empirically grounded and practical rules" that help ensure the privacy of individuals.

3 The Privacy Problem

Privacy is an important aspect of our day-to-day lives; it is something that gets generally overlooked by people when accepting the terms and conditions agreement. However, Privacy is much more important than people assume it to be. The right to privacy intersects with many human rights such as freedom of expression, the right to seek, receive and impart information, and freedom of association and assembly. It prevents large groups from using individual's data for their personal goals. This was the case in the Cambridge Analytica Scandal where their organization unlawfully used personal data to find and 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 an individual to share anything and everything that they wish to share with the world without the fear of being monitored and tracked. This allows individuals to freely engage in conversations regarding various topics including politics, giving them the ability to share their opinions with the world with or without the world linking their ideas back to them as an individual. Privacy allows people to put on the façade of being a nameless faceless user online. What they choose to do with this ability depends on each person behind the façade.

A world without privacy would be an authoritarian world. Absolute power would lie with the people controlling access to individual data. Able to foresee their every move, their motives, and the ability to get into their minds. This would allow them to shape the world in whichever way it seems fit. People would be criticized for any opinion that stands out of the norm, their personal life and their online life will no longer be restricted to them, every action they take would be monitored and recorded. From past historical events, we know for certain that complete authoritarian rule does not work. To form trust and promote growth as well as protecting the rights given to citizens, privacy has to be maintained.

4 Privacy vs Security

Even though privacy is an important aspect of governance, complete and total anonymity is also not a viable option. 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 other's 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 while conducting the attack. This makes it very difficult for the authorities and the defenders to kick them out of the network as well as making sure that they stay out once detected. Having weaker privacy gives way for a potentially stronger security and it is up to the governments and policymakers themselves 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 so that it is easier for the government to be able to track everything and trace it back to individuals thus maintaining the idea of accountability.

The government however is not the only player that benefits from a lack of privacy, private companies, and advertisers also profit from the collection of data being shared online. This data is then used by companies like Facebook and Google to build profiles or "digital dossiers" on each accessing their resources (Gross & Acquisti, 2005). These dossiers allow these organizations to build up targeted advertisements, focusing on presenting individuals with products that they believe would have the highest chances of being sold. Targeted advertisers do not benefit from increased data privacy laws since with the increase in data regulations, their access to detailed dossiers dwindles and this severely affects their business model. Apart from advertising, companies also store this user data to improve their current services as well as providing detailed statistics on the services that they provide. Privacy is also put at risk when this collected user data is shared among organizations and between the private companies themselves and the government. An example of this would be telecommunication companies sharing user data with the governments to facilitate their intelligence.

The idea of privateering security as described by Florian Egloff, where pri-

vate companies actively participate in defensive capabilities which also include offensive security brings up privacy issues (Egloff, 2015). Private companies are victims of the majority of cyber-attacks. Due to this, they can no longer be reliant on the government alone to act against the attacker. Aside from focusing on improving their defensive capabilities, companies are also looking into ways in which they can quickly attack their attackers. For example, if a company, let us assume A decides to incorporate offensive security capabilities within their network. When they are then 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 of offensive security such as Cyber Deception, Disruption, and Preemption which have been discussed thoroughly by NAS in their book At the Nexus of Cybersecurity and Public Policy (Wolff, 2017). Offensive security, while sounding great theoretically 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 simply defining every attack on a system as malicious, now the context behind that attack also starts being considered when defining an attack to be acceptable or not. Josephine Wolff outlines the risks that are brought on by offensive security very well.

This idea of hacking back the attackers perfectly summarizes the issues we face today with privacy. On one hand, it is the privacy of the companies and the user data that they store itself, that needs to be protected from the attacker. However, on the other hand, while using offensive security, companies attempt to get information on their attackers, be it using beacons that pingback 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, to do that, it can break the very privacy laws that the organization

was protecting in the first place. This leads us to carefully consider the risks and possibilities associated with privacy before taking any actions.

5 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 being 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 as well as better risk assessments (Dubrova, 2018). 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 there are more than a couple of perspectives that need to be considered. The implementation of a strong well-defined policy that is made collaborating with all fields of this ecosystem, including representatives from the government, 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

Cool, A. (2018, May 15). *Europe's data protection law is a big, confusing mess.* Retrieved from `https://www.almendron.com/tribuna/europes-data-protection-law-is-a-big-confusing-mess/` (Name - Cambridge Analytica; European Parliament; European Union; Facebook Inc; Copyright - Copyright 2018 The New York Times Company; Last updated - 2020-07-14)

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

Egloff, F. (2015). *Cybersecurity and the age of privateering: A historical analogy.*

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. 71–80). New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/1102199.1102214 doi: 10.1145/1102199.1102214

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

Wolff, J. (2017, Oct). *Attack of the hack back.* Slate. Retrieved from https://slate.com/technology/2017/10/hacking-back-the-worst-idea-in-cybersecurity-rises-again.html