The Importance of Data Security and Privacy in a Threating World

Kaleb Alstott

INF 284

Author Note:

**Abstract**

 In today's world of technology that is ever growing, we have seen the rise of value in one's data. Data has come a long way from just a bunch of numbers and calculations from an app. In today's age of information, data is a necessity for companies to pursue, persuade, and rethink the idea of marketing to a crowd. With such valuable information being accessed at all times we have seen a dramatic rise in the terms of data security and data privacy over the past decade. Data security refers to the security of their data such as trying to prevent hacking or a data breach, while data privacy is defined as the trust and conscientiousness of one's data. Usually implying the trust of a company to use their app and that they will use your data to the terms and conditions applied.

With data being produced at such a fast rate across the whole world we see many laws and regulations slacking in protecting our data. We can see a real-world example that will be discussed, is the acts of Facebook and Cambridge Analytics. In this case we can see the rights of hundreds of people data being misused and wrongfully sold away. With such an exponential growth of data opening up vulnerabilities, this is causing there to be more patch work and an increased data security. As your data becomes more valued, there is an increased risk of regulating what a company or third party can use your data for. With no regulations, protections,  or enforced acts upon inappropriate use of data we will simply never be able to control and maintain a healthy balance of the digital world.

Keywords: Data security, Data privacy, Information

The Importance of Data Security and Privacy in a Threating World

In today’s day and age, we are in a world surrounded by a rapid growing field of technology. With such an exponential growth there is starting to become an issue of data being unsecured and unregulated on how it is used. After research the best way to define what data is to someone is “Your personal data, your values and interests and wishes all combine to form an overall picture ofyour identity.” (Sempf). Every button you click, every item you buy, anything you search, is all personal data that defines who you are. Ones data must be protected from being misused from third parties and other threats because of key information that your data stores such as passwords, records, transactions, etc. If we fail to protect our data rights and privacy’s, we are liable for such cyberattacks like identity theft, data breaches, hacking, phishing emails, viruses, and many more harmful attacks. With such a high valuable piece of information that many would call a resource in today’s age, we have seen a dramatic rise in the terms of data security and data privacy over the past decade. In order to understand what data security and privacy is we have to break down what happens if we don’t protect our data, why it so hard to protect our data, and finally how can we protect our data using security and privacy.

# How is data privacy and data security connected? -1

With the constant war on trying to keep up to protect and regulate our data we first must break down and understand what data security and data privacy is and how they are connected to one another. Data security can easily be broken down and defined as protecting the access of your data from unwanted or unauthorized intruders. Whereas data privacy can be defined as, one’s data that is trusted by a company or party that ensures the customer that their data is being used for the intended rights and not being wrongly used. The overall connection between these two points that link them together is the common goal of data protection. There our 5 main pillars of data security and privacy that are required which, “are summarized based on five critical metrics, including the confidentiality, availability, integrity, authentication and access control, and privacy requirements.”( Zhang, Hu, Cheng, Zhao, & Chen pg4). We can roughly break these pillars into the three main topics of confidentiality, integrity and availability. The confidentiality of one’s data refers to, the information that is being used by the right people and terms and making sure this information isn’t wrongly used or reached by intruders. Confidentiality is one of the main topics in discussing data privacy and security because this is the main aspect of being able to ensure and trust a company or customer that their data will be used for the right purposes and will be secured at all costs. The second topic that links these two terms is the integrity of one’s data, which is defined as how accurate or trustworthy your data is throughout its lifecycle. This is an important goal in data security because if your data can only be protected for a partial amount of time and isn’t consistent with limiting its risk of data breaches, then your information will have a higher risk of being interfered with or manipulated. The last common goal that data security and privacy share is availability, which is where your data has access to be available or not. This goal is similar to being consistent with the protection of your data. If your data can never be accessed properly then you won’t be able to login or use certain credentials, and vis versa, if your data is always open and not protected then you are at risk for cyberattacks. Know that we have broken down what data security and data privacy is and how they are related, we can see what problems arise if we don’t secure our data and protect our data accordingly.

* 1. **Problems that can arise in data security and privacy -1.2**

The best way to describe the risks of data security is that, “ There is an increasing need of research in technologies that can handle the vast volume of Data and make it secure efficiently. Current Technologies for securing data are slow when applied to huge amounts of data.”(Toshniwal, R (2015)). With data not being analyzed efficiently and effectively we are open for cyberattacks and risks such as ransomware, data corruption, crypto mining, hacking and much more. The risks of one or all of these attacks happening to you are could damage much more than your digital world. These attacks can cause an attacker to wipe your bank account, login to any website or social media you have access to, control files so you can’t open them, passwords to everything you have, and much worse. Simply without any data security we cannot have data privacy. If we fail to achieve the first step in securing our data, then there is no hope in trying to regulate and control the use of how are data can be used properly. The problem that can arise with data privacy is best defined as ,” If you don’t have privacy, you lose your right – indeed your ability – to be yourself, to form your very identity.”(Falkvinge). If your data cannot be privately used and controlled in the right way, then every click you have ever made in the digital world doesn’t matter, destroying who you are and what your true identity is. The risk that can come with not regulating data and your privacy in a business can cause a loss of customer trust, violation of laws against your company, loss of costumers, data leaked that can hurt your consumer, and many more threats that can cause your business or even you to go into a financial crisis. Lastly, these are all real-world issues that we have been dealing with more frequently as our technology and data grows. One of the biggest data privacy scandals that has recently happened is the actions taken place between Cambridge Analytica and Facebook. “ The discovery that Facebook gave unfettered and unauthorized access to personally identifiable information (PII) of more than 87 million unsuspecting Facebook users to the data firm Cambridge Analytica has fueled growing interests in the debate over technology’s societal impact and risks to citizens’ privacy and well-being.” ( J. Isaak and M. J. Hanna, vol. 51, no. 8, pp. 56-59). As we can see our data is still being misused and our data privacy has been broken. With millions of people’s identity taken, where can we go and what can we do to protect our data? What makes it so hard for a company or for an individual to increase data security and their privacy?

1. **Why is our data so hard to protect -2.**

Our data as time goes on will continue to grow and be more valuable. We are living in the age of information meaning information can be, “ available instant access to knowledge that would have been difficult or impossible to find previously.”(Contributor, *The New Information Age* 2011). With this type of information at our fingertips we are able to produce data, leave cookie trails, and leave behind a digital trace that lets companies know who you are. There are three main issues that arise that makes data security and privacy so hard today and that is the exponential growth, cost of maintaining the data privacy, and open vulnerabilities. With such an exponential growth of “ more than 1.7 megabytes of new data is created every second”(*The 5 Biggest Challenges in Global Data Privacy and Protection*2020) we are still trying to look for new ways to analyze so much more data because we are using old technology to analyze millions and billions of data records still today. With lack of updated technology there is a higher risk of data breaches and data encryption due to how it is nearly impossible to keep track and run as much data as we are producing at this rate. The second issue that arises is how much it costs to run and maintain data privacy, and at worst if you were to get breached how much it costs to recover and build your business back. “In fact, the Ponemon Institute found that the total average cost of a breach cost in 2017 was $3.62 million. What’s more is that there is a 30% chance for an organization to experience a data breach over the next two years.”(*The 5 Biggest Challenges in Global Data Privacy and Protection*2020). As we can see with such a high amount of money that can be lost through a data hack it is almost impossible to rest or comeback from such a dramatic loss of money. With the two variables of an unlimited amount of data being produced and the cost of future damages we see how trying to secure and regulate our data is becoming harder every day. The last and final reason why data security and data privacy is so hard to protect is due to open vulnerability’s. “ According to CVE, a definitive source for information security vulnerabilities reported that nearly 15,000 disclosed vulnerabilities surfaced in 2017. This is more than 56% more than 2016 total vulnerabilities.” (*The 5 Biggest Challenges in Global Data Privacy and Protection*2020). With hundreds of patch works needed to fix all of these open vulnerabilities we can see the stress and the extra needed help in order to work on and maintain a safe low risk network. Combining all three of these variables we can see how with so much data it is becoming harder for one to regulate and secure data from high risks of these cyberattacks.

1. **How to protect our data today -3**

With all of our data today being so vulnerable yet worth so much value, it seems to be impossible to protect your identity. In order to protect your data and give you the best chance of limiting cyberattacks there is multiple things one can do. One of many being encrypting your data. Encrypting your data can help you prevent cyberattacks because you are putting a unique password on your email, social media websites, or anything that adds value to your data and identity in the digital world. The next step out of many that you can take would be is backing your data up frequently and ensuring your device at all times is up to date with at least anti-malware protection. Backing up your data can help you revisit old data that may have been infected or lost at a certain time helping you ensure that you will never lose access to important data. Having any type of security is better than none and this is where downloading an anti-malware protection can help. “Having an anti-malware protection can help defend against computer spyware, worms, viruses, and many more protecting your data. “(*101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Safe in 2020,* 2020). Nationally we need to add a focus on updating and staying up to date in laws and regulations with our data and how it is used. A “harder”, or more of a consequence is needed to be presented when harming with one’s data is on the line. With such a valuable piece of information that is growing as we speak; we need to step up and take an action in our role of data that we are leaving behind.

1. **Conclusion -4**

In conclusion, we can see the similarities and differences between what data security and data privacy is and how they are connected. With our data being so valuable in an age of technological growth we need to find better ways in ensuring our data is as safe as possible. With our data giving so much information and defining our identity in a digital word we need to increase our data security and make sure that our data is being used properly in order to keep our data and our identities secure. With such a great risk of data falling into the wrong hands or being missed used, we have to step up and play a role in the digital world and what we are leaving behind. With data defining who we are in the digital world, we need to take a step in the right direction and start to limit the risk of these cybercrimes as they continue to grow. You never know when you could be the next victim of miss used data.

References

101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Safe in 2020. (2020, September 30). Retrieved November 09, 2020, from https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

The 5 Biggest Challenges in Global Data Privacy and Protection. (2020, August 18). Retrieved November 09, 2020, from https://cipher.com/blog/the-5-biggest-challenges-in-global-data-privacy-and-protection/

Contributor. (2011, April 10). The New Information Age. Retrieved November 09, 2020, from https://techcrunch.com/2011/04/10/the-new-information-age/?guccounter=1

Falkvinge, R. (2020, August 26). Without privacy, you lose your ability to have an identity of your own. Retrieved November 09, 2020, from <https://www.privateinternetaccess.com/blog/without-privacy-you-lose-your-right-to-an-identity/>

J. Isaak and M. J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy

Protection," in Computer, vol. 51, no. 8, pp. 56-59, August 2018, doi:

10.1109/MC.2018.3191268.

Sempf, J. (2020, November 02). The age of information: What makes your data so valuable? Retrieved November 08, 2020, from <https://www.hornetsecurity.com/us/security-information-us/data-value/>

Toshniwal, R., Dastidar, K. G., & Nath, A. (2015). Big data security issues and

challenges. *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*, *2*(2).

Zhang, J., Hu, F., Cheng, X., Zhao, Y., & Chen, B. (2018, March 29). Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. Retrieved November 08, 2020, from https://ieeexplore.ieee.org/abstract/document/8327600