Overview of Privacy and Data Protection Issues

Brandon M. Burke

Old Dominion University

CYSE 406: Cyber Law

Professor Jude Klena

26 October 2024

To: Governor of North Virginia

From: Brandon Burke

Subject: Overview of Privacy and Data Protection Issues

Date: October 26, 2024

1. Overview of Privacy and Data Protection

Privacy is a fundamental right that every person is entitled to. It refers to the right of individuals to control their personal information and the ways it is collected, used, and shared (OAIC, 2024). Concerns about personal data protection arise from the increasing volume of sensitive information being collected by businesses, governments and data brokers, often without clear consent or understanding from individuals. Additionally, this leads to unauthorized access, misuse, or exploitation of personal data as there is a lack of proper safeguards in place to protect individuals from these harms. Without adequate protection, individuals face risks such as identity theft, financial fraud, and unauthorized surveillance, which can lead to emotional distress and a loss of trust in institutions. Moreover, this can cause billions in damages which affects the economy that citizens live in.

2. Biometrics and Personally Identifiable Information (PII)

Personally Identifiable Information (PII) encompasses any data that can be used to identify an individual (U.S. Department of Labor, 2024). This can include names, addresses, social security numbers, email addresses, biometrics, etc. PII is also stored in databases that companies have. This can include usernames and passwords. Banks are a primary example. Banks hold information such as usernames, passwords, email addresses, home addresses, and social security.

PII is very valuable to attackers as this information can sell for monetary gain on dark web markets. One of the most valuable PII that threat actors can get their hands on is biometrics. Biometrics refers to unique physical or behavioral characteristics used for identification purposes. This includes fingerprints, facial recognition, iris scans, voice patterns, and the way people walk. What makes biometrics special is that it cannot be changed. Once an attacker has this information, it can be used whenever and however the attacker wants.

3. The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) was approved in 2016 and authorized on May 25, 2018 (European Union, 2024). The GDPR, instituted in the European Union (EU), is a comprehensive data protection law with key provisions including broad coverage including organizations processing personal data of individuals in the EU, irrespective of location, and encompasses EU citizens' data being processed outside the EU. Key data protection principles established by the GDPR include data minimization, purpose limitation, and accountability, all aimed at ensuring that individuals have greater control over their personal information. Processing data must also maintain confidentiality and integrity, ensuring that appropriate safeguards and security measures are in place. Additionally, the GDPR grants rights to each individual part of the EU. These rights include the right to be informed, ensuring individuals know how their data is processed. The right to access gives individuals the ability to obtain a copy of their personal data from you, as well as other supplementary information. The right to rectification which allows individuals to request that inaccurate or incomplete personal data be corrected. The right to erasure means to request the deletion of personal data from an organization. The right to restrict processing limits how an organization uses personal data. The

right to data portability which allows individuals to obtain and reuse their personal data for their own purposes across different services. The right to object means individuals can prevent or stop an organization from using their personal data. Finally, the GDPR grants rights to automated decision-making and profiling which protects against potentially harmful or discriminatory automated processes (European Union, 2024). These comprehensive rights give power to individuals to assert control over their data ensuring that their privacy is protected and respected in the growing digital age.

4. Privacy Laws in Other States

Several states have taken significant steps toward safeguarding consumer data. The most prominent being California's California Consumer Privacy Act (CCPA). The CCPA gives consumers more control over their personal information that businesses collect about them. Moreover, the CCPA regulation provides guidance on how to implement the law . This privacy act allows California consumers to have the following rights: know about the personal information a business collects about them and how it is used and shared, delete personal information collected from them (with some exceptions), opt-out of the sale or sharing of their personal information, non-discrimination for exercising their CCPA rights (Bonta, 2024). In November 2020, California voters have agreed to Proposition 24 which amends the following rights to the CCPA: correct inaccurate personal information that a business has about them, and limit the use and disclosure of sensitive personal information collected about them (Bonta, 2024). Another state with privacy protections is Virginia's Virginia Consumer Data Protection Act (VCPDA). The VCDPA governs the collection and processing of consumers' data. Similarly to the CCPA, the VCDPA allows consumers to opt out of data collection (Northam,

2021). Both acts operate under the basis of "controller" and "processor" as seen in the GDPR. The rights granted under the CCPA and VCDPA play a significant role in reducing the potential for data breaches and exfiltration of PII. When consumers can easily request the removal of their data, businesses are incentivized to limit data retention practices, which decreases the volume of information that could be compromised in a breach.

5. Recommendations

In the light of increasing public concern over privacy and data protection, I would recommend that North Virginia push to enact its own personal information and data protection law. Focusing on state-level legislation has several advantages. The first advantage is that it allows North Virginia to tailor its law to address specific needs and concerns of its citizens. By engaging with the community, lawmakers can ensure that the legislation reflects local values and priorities such as the protection of biometric data, PII, or other concerns that North Virginians may have. Additionally, state-level legislation can be enacted more quickly than federal laws. Inherently, this allows for swift actions that can help restore public confidence and demonstrate that the government is proactive in safeguarding personal information. However, there are a few drawbacks to state-level legislation. The main challenge is the risk of creating a patchwork of laws that will complicate compliance for businesses operating in multiple states. This means fatal errors can occur in business models which could impact business efficiency. On the other hand, having the Federal government to pass a law will undoubtedly ensure uniformity with business standards when it comes to privacy and the protections associated with this data. Conversely, advocating for the Federal government to create and pass a law would take a significant amount of time as lawmakers would have to consider the needs of every state. For

making a privacy law, I would recommend that you as Governor copy and ratify a law exactly GDPR almost word for word. The GDPR has worked wonders for the EU as the law results in businesses taking action to protect data it collects. In return, this causes fewer data breaches to each company. With the United States the most target country for companies holding data. Having a law exactly like the GDPR would cause less data breaches. This would mean that citizens are affected less by identity theft which is a rampant crime that occurs on a daily basis.

References

Bonta, R. (2024, March 13). *California Consumer Privacy Act (CCPA)*. State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa

European Union. (2024, April 22). *General Data Protection Regulation*. General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Northam, R. (2021, March 2). *Virginia Law*. Code of Virginia Code - Chapter 53. Consumer Data Protection Act. https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

OAIC. (2024, September 5). *What is privacy?* https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-privacy

U.S. Department of Labor. (2024). *Guidance on the Protection of Personal Identifiable Information*. https://www.dol.gov/general/ppii