Data Privacy Memo for the Governor of North Virginia

Robert S. Timmons

Old Dominion University

CYSE 406: Cyber Law

Professor Jude Klena

October 2nd, 2024

Privacy Memorandum for the Governor

To: The Governor of North Virginia
From: Robert Sullivan Timmons
Subject: Privacy for the Citizens of North Virginia
Date: October 2nd, 2024

Governor,

The citizens of our great state have expressed concerns about the lack of data privacy and protection laws in North Virginia and have demanded action to these pressing matters. With the ever-present internet and the rise of IoT devices, data is being collected on a monumental scale. As the amount of data and data types on the internet increases, so does the likelihood of a breach. In 2023 alone, there were around 2,365 cyberattacks, effecting over 340 million people. On top of this, last year witnessed the most data breaches ever, having over a 72% increase from 2021, the former record holder. (St John, 2024) It is imperative to react to this growing issue; to secure and ensure the confidentiality and integrity of our citizen's data. This memorandum will brief you on privacy in the information age, personally identifiable information (PII), the issues pertaining to data protection, and how it is affecting our citizens. With this understanding, possible solutions will be provided, using examples from other state's legislation, as well as other country's rulings on data privacy for their citizens, the private sector, and government institutions. Governor, it is essential that action is taken to protect our citizenry's most prized possession, their privacy.

Privacy is not a new concept to governments and their citizens, the ability to be left alone and not interfered with has been debated at length in court. With the advent of the internet however, the definition has quickly evolved and matured. According to the International

Association of Privacy Professionals, “Information privacy is the right to have some control over how your personal information is collected and used.” (Iapp, 2024) On the internet, information is as valuable as gold. Monolithic internet companies have been founded on collecting and selling online information to the highest bidder. Recently, Facebook has been caught collecting individual information, packaging it as usable data, and selling access to thousands of companies. This information is then in turn utilized to advertise products, monitor individuals, or conduct research. Collecting data on such a massive scale may seem harmless but can have devastating consequences.

Personally identifiable information, or PII, is some of the most sought-after data by companies and various actors on the internet. This information can include full names, personal addresses, birthdays, and other data points that are unique to the individual. If this data were somehow stolen from these large corporations, nefarious actors could leverage it to open bank accounts, commit identify fraud, or more easily scam individuals through phishing attacks. For example, Yahoo, one of the top search engines, discovered a breach of one of their PII databases, which contained over 3 billion passwords, full names, birthdates, phone numbers, and emails. (Stempel, 2017) As technology has progressed, other, even more personal data has found its way onto the internet and into the hands of malevolent hackers. Biometric data is increasingly used in the commercial, health, and banking sectors for greater authentication and identification of customers, patients, and employees alike. Information like facial structure, tone of voice, and fingerprints are just a few pieces of data collected by advanced biometric scanners. Like all data on the internet, this data has found its way into the hands of malevolent hackers. In the case of Suprema, a British biometrics company, it was discovered to have their entire database exposed to the internet. Reported by the guardian, “The researchers had access to over 27.8 million

records, and 23 gigabytes worth of data including admin panels, dashboards, fingerprint data, facial recognition data, face photos of users, unencrypted users and passwords…" (Reed, 2019) When this information is not properly protected by sound government regulation, it becomes only a matter of time exposures occur, and innocent individuals are at risk of impersonation or scams.

In response to these vulnerabilities, other countries and government entities have invoked legislation and regulations to combat these data threats to their citizens. Most notably, the European Union unveiled the GDPR, known formally as the General Data Protection Regulation. Enacted in 2018, the GDPR aims to be the all-encompassing regulation that protects citizen data within the EU. Many of the stipulations directly pertain to the collection, storage, and disposal of personally identifiable information, such as IP addresses, cookies, full names, addresses, government identification, and photographs, just to name a few. GDPR protections apply to all member states within the EU, as well as companies that operate within the union's borders. Meaning, even if a corporation is headquartered halfway across the globe and offers some form of service, even if not for monetary gain, their policies must be complaint with the GDPR. (Stanciu, 2024) Guided by seven core tenets, the sweeping regulations ensure confidentiality of data, integrity of data, accountability for companies, and data minimization. Data minimization is a particularly fascinating objective, as it instructs entities that they can only hold onto data for certain time periods with user permission. In the case of Yahoo, if these procedures were implemented, there could've been reduced impact as less data would've been available. The GDPR's regulations have been a positive step forward in cyberspace, providing tangible frameworks for government and commercial entities alike to keep an individual's data safe.

Though this memo has discussed more international policies enacted to protect data privacy, there are some laws closer to home states have implemented. According to Bloomberg, there have been over 20 US states who have employed data protection and handling laws, with this number on the rise. Most notably, the states of California and Oregon have passed stringent regulations, named the California Privacy Rights Act (CPRA) and the Oregon Consumer Privacy Act (OCPA) respectively. California's CPRA applies mainly to companies who meet a certain criterion, such as how much data they collected overall, how much business they get from California, and other stipulations. The CPRA empowers individuals to take more control of their data, forcing companies to ask users for permission to use their data, disclose to individuals of what data they have upon request, the ability to correct and alter data stored, and opt out of any data collecting scheme. (Trustarc, 2024) CPRA's unique wording mandates companies to give explicit, well-defined descriptions of how a user's data will be used and disclose any information they have, lest they face legal consequences. The OCPA takes this a step further, and in many respects, is considered one of the most severe and sweeping data privacy regulations. Within the law, there is an explicit definition of privacy, what it entails, and what rights the individual have. As seen with the CPRA, you can receive copies of data kept by organizations, can request for edits, and deletion of information. Going a step further, the OCPA stretches to organizations that receive data secondhandedly from other businesses. On top of this, businesses that deal with 25k Oregonians a year, or receive 25% of their business from Oregon must comply with the OCPA. (Or.DOJ, 2024) This is half of what California requires. States across the union have begun acting against aggressive data collection, and with more time, it appears mores states with have similar or more extreme measures like California and Oregon.

As detailed earlier in this memo, data protections geared toward privacy are essential in the information era, as the individual is continually at risk. There have been debates between moving for the federal government to draft a comprehensive solution, or let the states decide among themselves. The federal government could produce a sweeping regulatory suite that would apply to all states, regardless of their current laws. Though this can be extremely helpful, the state of North Virginia shouldn't rest on its laurels and wait for the federal government. The federal government takes time, between bringing bills to the floor, negotiations, debates; the house of representatives and senate will take time to home in on the details. Worst of all, the bill could get stuck in committee, and no resolution could be agreed upon. If our state drafts its own data protection policy, there will be more flexibility, as we're not dealing with different parts of the country and there will be less red tape and procedure to follow. To build on this, we can customize it to our own liking, there is a chance that the federal government, whose representatives may have donors in the tech industry, don't go far enough in their regulation, as to not rock the boat with their donors. In the digital age, you cannot rely on your data not being important. Data is collected on massive scales, packaged, analyzed, and sold to the highest bidder. It is crucial we create a comprehensive data protection policy that meets our unique needs and requirements.

References

The rise of Ashburn: Data Center capital of the world - crowley media group. Crowley Media Group LLC. (2023, January 22). https://crowleymediagroup.com/resources/ashburn-data-center-capital-of-the-world/#:~:text=Ashburn%2C%20Virginia%2C%20is%20a%20small,well%20as%20many%20tech%20companies.

King, D. (2024, April 8). *Is Virginia's tech industry prepared for the next cyberattack? • virginia Mercury*. Virginia Mercury. https://virginiamercury.com/2024/04/08/is-virginias-tech-industry-prepared-for-the-next-cyberattack/

Reed, B. (2019, August 14). *Major breach found in biometrics system used by banks, UK police and defence firms*. The Guardian. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

Zilber, A. (2024, January 19). *Facebook users' personal data sent to thousands of companies : Study*. New York Post. https://nypost.com/2024/01/18/business/facebook-users-data-sent-to-thousands-of-companies-study/

What is privacy. What is Privacy. (2024). https://iapp.org/about/what-is-privacy/#:~:text=Broadly%20speaking%2C%20privacy%20is%20the,information%20is%20collected%20and%20used.

St John, M. (2024, April 17). *Cybersecurity stats: Facts and figures you should know*. Forbes. https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/#:~:text=Cybersecurity%20Fast%20Facts,in%202023%2C%20with%20343%2C338%2C964%20victims.&text=2023%20saw%20a%2072%25%20increase,the%20previous%20all%2Dtime%20record.

Stanciu, T. (2024, January 11). *What is GDPR? summary of the General Data Protection Regulation*. Termly. https://termly.io/resources/articles/what-is-gdpr/

Trustarc. (2024). *Summary of the california privacy rights act (CPRA) main rules*. TrustArc. https://trustarc.com/resource/california-privacy-rights-act-cpra-main-rules-summary/

Oregon DOJ. (2024, October 1). *Consumer privacy*. Oregon Department of Justice. https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/privacy/

Stempel, J. (2017, October). *Yahoo says all three billion accounts hacked in 2013 Data Theft | Reuters*. Reuters. https://www.reuters.com/article/technology/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82NV/