Attachment #5

Report to Vermont General Assembly on Data Privacy, 12/15/18

REPORT TO VERMONT GENERAL ASSEMBLY ON DATA PRIVACY
December 15, 2018

Prepared by the Vermont Office of the Attorney General

I. INTRODUCTION

The General Assembly has asked the Attorney General, in consultation with the Public Service Department, to make recommendations on the following issues:

1. Adoption of regulations concerning telecommunications privacy and whether to model such rules after the FCC's 2016 Privacy Order, WC Docket No. 16-106, FCC 16-148, adopted Oct. 27, 2016. The request for this recommendation was made in Act 66 of 2017.
2. Whether Vermont should designate a Chief Privacy Officer, and what the responsibilities of that Officer would be. This request was made in Act 171 of 2018.
3. Whether to regulate businesses that handle the data of consumers with whom they have a direct relationship, as requested in Act 171.
4. Any other privacy recommendations that are reasonable and warranted.

Vermont is not alone in considering regulation in this area. While the federal government has been slow to respond to data privacy concerns, various states have generated legislation responsive to such concerns. Vermont made a significant addition to these efforts last year with the Data Broker Registration Act and the Data Broker Data Security Act, 9 V.S.A. §§ 2446-47 (collectively the "Data Broker Regulations").

Today's technology enables data collection by businesses, organizations, and governments that creates concerns for consumer privacy. Though data collection has many benefits to our economy, security, and general welfare, we believe that a balance must be struck between these benefits and the expected right of individual privacy.

"Privacy" as used in this report concerns the information that businesses and others collect about individuals, how they collect that information, how much control individuals have over the collection, with whom the data is shared, and to what purposes the data is used. The "consent" consumers provide for use of our data is sometimes uninformed and can often feel coerced. It has become a challenging reality that participating in the modern information economy is often predicated on the sharing of private data.

This report makes two kinds of recommendations: those to adopt now and those to consider in the future after monitoring developments elsewhere:

A. Recommended Action Steps:

These are reasonable, incremental steps that Vermont may adopt now to enhance the data privacy of Vermonters.

1. The State of Vermont should designate a Chief Privacy Officer with resources sufficient to carry out the mission of that office;
2. The State of Vermont should conduct a privacy audit;
3. The General Assembly should adopt a law modeled on California's Student Online Personal Protection Act (SOPIPA), Cal. SB 1177, California Education Code 49073.1;
4. The Security Breach Notice Act should be amended to expand the scope of Personally Identifiable Information ("PII") applicable to the Act;
and
5. The General Assembly should consider amending the various definitions relating to personal information in order to harmonize them.

B. Defer Action:

For the following issues, Vermont should continue monitoring to determine how they are working in other states and federally.

6. The General Assembly should defer implementing privacy protections for customers of Internet Service Providers, including possible adoption of the FCC's 2016 Privacy Order;
7. The General Assembly should defer implementing laws similar to the California Consumer Privacy Act of 2018;
8. The General Assembly should defer implementing laws similar to the European Union's General Data Protection Regulation (GDPR); and
9. It would be premature to make additional changes to the Data Broker Regulations without first observing how the law works in practice and whether changes are warranted.

II. BACKGROUND

The Attorney General's Office has heard from Vermonters and others on this topic in a number of ways, including at public hearings, through written comments, through the Consumer Assistance Program (CAP), and by the hundreds of data breaches reported to the Attorney General's Office each year in accordance with the Vermont Security Breach Notice Act. Legislative testimony and related conversations have also informed this report.

Public hearings on this topic began last year when the Attorney General's Office and Department of Financial Regulation held twelve hours of public hearings specific to data brokers in Burlington. During those meetings privacy questions and issues were raised. Also, several Vermont legislators, with members of the executive branch and the Attorney General's Office, engaged in a well-attended listening tour, which included public hearings in Springfield and Barton on Nov. 9, 2017 and Manchester Center and Burlington on Nov. 14, 2017. The result was a report to the General Assembly and a first-of-its-kind law, Act 171 of 2018, to regulate data brokers who profit from consumer information. As part of this legislation and other enacted bills, the legislature requested that the Attorney General's Office partner with other agencies to provide recommendations with regards to protecting Vermonters' privacy. The

Attorney General's Office formed a Privacy Working Group in coordination with the Department of Public Service to investigate the above-mentioned questions.

The Privacy Working Group held three hearings to consider legislative proposals to address these emergent issues at the following times and locations:

- Monday, August 6, 2018: 9 a.m. – 12 p.m., 29 Church St., Burlington
- Tuesday, September 25, 2018: 1 p.m. – 4 p.m., 118 Prospect St., White River Junction
- Thursday, November 15, 2018: 5:30 p.m. – 8:30 p.m., 109 State St., Montpelier, VT

All three hearings generated robust conversations with input from members of the public and interested parties. Themes of conversation included how to fit Vermont into the federal landscape of regulations; how to protect choice and transparency around use of consumer information; and how to balance consumer privacy with economic growth. Six different organizations submitted prepared testimony at the hearings in addition to the open discussions. Others submitted written comments directly to the Attorney General's office.

III. RECOMMENDED ACTION STEPS

A. Designation of a Chief Privacy Officer

We recommend that the General Assembly create the position of Chief Privacy Officer (CPO). Several states have established a CPO position, a practice which has also been growing more common in the business community over the past decade. The first state to have a CPO was West Virginia, a small rural state like Vermont. A CPO typically has four main responsibilities:

1. Ensuring that the State complies with privacy obligations and protects the privacy of its citizens, which includes training State employees, reviewing contracts to ensure that vendors are protecting citizen data, and considering the privacy implications of new programs and technologies;
2. Providing education and outreach to help the citizenry better protect themselves;
3. Advocating within the executive and legislative branches as to further protections for Vermonters, including amending existing law and recommending areas where data need not be collected; and
4. Serving as an ombudsman to hear citizen concerns regarding privacy issues.

Notably, one of the largest collectors of Vermonters' data is the State of Vermont. The State is also a provider of data to businesses and other third-parties, including data brokers. The State is required to make this information available by state and federal statute, and in keeping with our duty of transparency as implemented by the Public Records Act. The State must balance its obligations of openness with making sure that citizens' data is not being used inappropriately, is only collected when necessary, and is disposed of securely when no longer needed. This may in some cases require amending existing laws or proposing new regulation. Currently, there is no

single individual who is accountable for balancing these competing interests within the halls of government.

The task of enforcing privacy laws as they apply to the businesses in Vermont rests with the Attorney General and has not typically been one of the roles of a CPO in other states. Law enforcement and compliance are sometimes conflicting roles, and we recommend that they not be housed within the same entity.

Importantly, a CPO position cannot simply be an additional title for a current employee. It is a complex position that requires dedicated staff and resources to carry out its mission. It could be housed in the Vermont State Archives and Records Administration in the Secretary of State's Office, with the Secretary of the Administration, the Auditor, or report directly to the Governor.

B. Conduct a Privacy Audit

As a consequence of the privacy hearings and legislative testimony, we know it is important to Vermonters that the State of Vermont appropriately handle citizen data. An audit would ensure that the government is handling citizen data securely, provide vital information to policymakers to determine whether our laws need adjusting, and shine a light on the State's processes.

This could be a role assigned to a Chief Privacy Officer, but given the urgency of this issue, we recommend that the General Assembly mandate an immediate privacy audit in order to determine:

- Which State subdivisions are collecting sensitive data;
- What data is being collected;
- How the data is used;
- Whether the data is publicly available or not; and
- Who is obtaining public data about our citizens from the State.

In the absence of a Chief Privacy Officer, this task might be assigned to officers with specific interest or expertise in this matter, such as the Chief Records Officer, and/or Chief Data Officer. However, to ensure a timely and fulsome audit, resources must be made available to accomplish this task.

C. Adopt SOPIPA

On January 1, 2016, California's Student Online Personal Protection Act (SOPIPA) went into effect. This law applies to websites, applications, and online services that focus on K-12 students, what is sometimes referred to as the "Ed Tech" industry. Ed Tech companies collect a lot of student data, and this law requires that businesses that collect student data use it to the benefit of the students, and not for other purposes.

For example, SOPIPA prohibits Ed Tech businesses from:

- Using student information to engage in targeted advertising;
- Creating profiles of students for any purpose other than school purposes;
- Selling student information; or
- Disclosing student information for purposes unrelated to the student's K-12 education.

The law also requires that Ed Tech businesses maintain data security standards and delete data if requested by the school or district. We recommend that Vermont's approach to SOPIPA include parents in this area.

Currently at least seven states have SOPIPA-like laws: Arizona, California, Illinois, Maine, Nebraska, New Hampshire, and Texas. Due to the market size of these states, many businesses are already in compliance with SOPIPA; therefore, Vermont's enacting a SOPIPA law would not require many businesses to significantly alter their behavior. Enaction would ensure SOPIPA's best practices were officially adopted in Vermont and provide Vermont with enforcement authority.

The proposal to adopt SOPIPA was discussed at length in all three of the privacy hearings, and no stakeholder – from industry or consumer groups – raised opposition to the idea.[1]

D. Update the Security Breach Notice Act

Vermont's Security Breach Notice Act, 9 V.S.A. § 2435, last underwent significant amendments in 2012. The Security Breach Notice Act requires businesses that experience a security breach to provide notice to the Office of the Attorney General or Department of Financial Regulation, and to consumers whose data is involved in a security breach. The Act applies to any business that collects data about a Vermont resident, but limits what constitutes a "Security Breach" to breaches involving "Personally Identifiable Information (PII)."

PII addresses a fairly narrow set of data, specifically:

"[A]n individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:

> (i) Social Security number;
>
> (ii) motor vehicle operator's license number or nondriver identification card number;
>
> (iii) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;

[1] However, it may be important for lawmakers to hear from so-called "EdTech" companies since it is unclear if any advocates represented them specifically during the public hearing process.

(iv) account passwords or personal identification numbers or other access codes for a financial account.[2]

This is essentially the definition of PII that was set forth in the first Security Breach Notice Act, adopted by California in 2002. Over time as we have gained more experience with security breaches, and the types of data that are being targeted has expanded, many states have expanded their definitions of PII. In light of these changes, we recommend that Vermont update the scope of data that requires security breach notification. Specifically, the definition of PII should be expanded to include all, or some combination of:

1. Biometric information, such as finger prints, facial recognition data, and other information;[3]
2. Genetic information;[4]
3. Health information;[5]
4. Login credentials, meaning usernames and passwords, which are often used across different websites, making a consumer vulnerable whenever a password is stolen;[6] and
5. Passport numbers.[7]

E. Review and Consider Harmonizing Data Definitions

Several of Vermont's laws that regulate handling of data define the data at issue in different ways. For example, these laws sometimes refer to "Personally Identifiable Information," "Personal Information," "Brokered Personal Information," or other definitions. It is possible that the different definitions are necessary to serve the purposes of the laws in which they are used, but there may be value in determining whether the various definitions can be harmonized, for purposes of simplicity in compliance. Lawmakers should request legislative council review the various statutory definitions and consider potential benefits or drawbacks of attempting to create a uniform standard definition.

IV. DEFER CONSIDERATION OF NEW PRIVACY REGULATIONS

A. ISP Privacy

In October 2016, the Federal Communications Commission issued Order FCC 16-148, which would have increased privacy protections for customers of Broadband Internet Access Service (BIAS) Providers. Many consumers use BIAS Providers for access to the Internet and must necessarily provide BIAS Providers with access to the data sent through their services. The

---

[2] 9 V.S.A. 2430(5)

[3] Required in Colorado, Delaware, Illinois, Iowa, Louisiana, Maryland, Nebraska, New Mexico, North Carolina, Oregon, South Dakota, and Wisconsin.

[4] Required in Delaware and Wisconsin.

[5] Required in Alabama, Arizona, Arkansas, California, Colorado, Delaware, Florida, Illinois, Maryland, Missouri, Montana, Nevada, New Hampshire, Oregon, South Dakota, Virginia, Wyoming, and Texas.

[6] Required in Arkansas, California, Florida, Illinois, Missouri, Montana, Nevada, North Dakota, Oregon, Rhode Island, and Texas.

[7] Required in Alabama, Arizona, Colorado, Delaware, Florida, Louisiana, Maryland, and Oregon.

Order would have required BIAS Providers to provide consumers with reasonable notice of their privacy policies and to obtain opt-in consent before sharing certain customer information like web browsing data and other private information with third-parties like advertisers.

In March 2017, the US Congress overturned the FCC Order. In Act 66 of 2017, the Vermont General Assembly asked the Attorney General, in consultation with the Department of Public Service, to issue a recommendation as to whether Vermont should adopt telecommunications privacy regulations and whether to model such rules after the FCC Order.

We have heard compelling testimony for and against the adoption of such regulation and from advocates and industry organizations. We also heard testimony that only the largest BIAS providers are seeking to share this data, and that the smaller providers, of which there are several in Vermont, do not have the capacity to monetize customer data. Therefore, some speculate that adopting BIAS regulation could help level the playing field between local ISP providers and the large national companies, while protecting consumers, without placing a high burden on BIAS Providers. However, we do not have enough data or testimony from local ISP's to make a determination on this point.

One industry advocate repeatedly stated that ISPs do not sell data. Consumer advocates countered that the major ISPs have acquired ad networks, and so while it may be accurate that they don't currently "sell" the data, ISPs certainly monetize data internally through ad networks.

No state has adopted Broadband Privacy regulations like the FCC Order to date.[8] The reasoning for this has been attributed to one or more of the following:

- Desire for a uniform national approach;
- Desire for a general standard applicable to all businesses, not just ISP's;
- Strength of the industry trade groups who oppose such measures.

Therefore, in keeping with our recommendations that this year the legislature should focus on bringing Vermont up to speed with existing protections rather than being a first-mover in new protections, our recommendation is that the State wait and see what happens in other states this year, before taking action on this issue.

B. California Privacy Protection Act

Earlier this year California adopted a significant new privacy regulation that limits how businesses can use personal data. This law goes into effect in 2020.

[8] The National Conference of State Legislatures (NCSL) has tracked specific state action or inaction regarding ISP Privacy Legislation, available at: http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers.aspx

In May 2018, the European Union adopted the General Data Protection Regulation (GDPR), which is a far more restrictive privacy regulation than anything that exists in the United States.

We believe that GDPR may ultimately provide many positive developments for consumers and likely represents an overdue correction to the previously unregulated approach to data collection and use. However, given that GDPR is new, and the California law will likely be amended before it goes into effect, we recommend the legislature monitor these developments and consider action in the future depending on outcomes for consumers and the private sector.

C. Changes to Data Broker Regulations, Including Whether to Extend Regulation to Businesses with a Direct Relationship with Consumers

In Act 171 of 2018, the General Assembly asked us to make a recommendation regarding amendments to the recently adopted Data Broker Regulations.

The Data Broker Regulations define what it is to be a "data broker," require data brokers to register annually with the Secretary of State, require data brokers to maintain minimum data security standards, and make it illegal for anyone to acquire certain personal data through fraud or for the purpose of stalking, harassment, fraud, identity theft, or illegal discrimination. This regulation goes into effect on January 1, 2019.

We have received requests to expand this law to apply to entities with a direct relationship with the consumers whose data is handled. We have also received requests to require that data brokers be required to have credentialing practices so that they do not share data with nefarious actors. Finally, we have received requests that in the event of a data broker security breach, notice be provided directly to consumers, instead of merely listing the fact of such breaches in the registry of data breaches.

Because the Data Broker Regulations have not yet gone into effect, we believe that it is premature to make a recommendation in this area. We will continue to monitor the effect of the new data broker law.

V. CONCLUSION

As technology, and data usage in particular, becomes more thoroughly integrated into our lives and our economy, government should act to proactively balance the need for consumer protection and a robust marketplace. Vermont's first step is to adopt the data privacy steps that have proved successful elsewhere. Meanwhile, other initiatives on the vanguard should be monitored and considered for future action.