Attachment #15

Timothy Edgar Memorandum (2/13/19)

WATSON INSTITUTE
FOR INTERNATIONAL STUDIES
BROWN UNIVERSITY

To: Steven Brown
Executive Director
ACLU of Rhode Island

From: Timothy H. Edgar
Academic Director for Law and Policy, Executive Master of Cybersecurity
Senior Fellow, Watson Institute for International and Public Affairs
Brown University[1]

Date: February 13, 2019

Re: Notes on proposed legislation from Rhode Island Online Data Transparency and Privacy Protection Commission

At your request, I have reviewed a package of proposed legislation from the Rhode Island Online Data Transparency and Privacy Protection Commission (the "Commission."). Based on a preliminary review, I have included some commentary on each of the bills.

We are facing a major digital privacy crisis in the United States, and Rhode Island can be on the forefront of legislating solutions for it. Cybercrime and cyber insecurity threaten the long-term prosperity of the United States. Strong state privacy and data breach laws are an important lever to encourage better cybersecurity practices.

Rhode Island should be giving companies with shoddy security practices no excuses to postpone upgrading their cybersecurity. We should put companies that are doing the right thing at an advantage and send a signal that Rhode Island will fight for the cybersecurity of its residents.

California and Massachusetts have been leaders in this area, by engaging with privacy advocates and those who fight for consumer protection. Rhode Island can be a leader as well.

I include substantive comments for each bill, and would be happy to discuss my comments with members of the commission.

[1] Institutional affiliation is listed for identification purposes only.

WATSON INSTITUTE
FOR INTERNATIONAL STUDIES
BROWN UNIVERSITY

699 – Relating to Commercial Law, "The Data Security Breach Notification Act"

While the intent is appreciated, the overall concern is that this proposed bill could be a step backward for privacy in Rhode Island.

By offering inadequate protections for privacy in a world full of data thieves, cyber criminals, and state-sponsored hackers, the bill could unintentionally favor short-term business interests of companies over the privacy interests of Rhode Island residents.

The definition of "breach of security" at 6-48.1-2(2) contains some concerning loopholes.

- The bill uses a standard of "substantial risk of identity theft or fraud against a resident of the state" as a threshold for "breach of security." This could harm security. A breach is a breach and should not be limited by a "risk" or "harm" standard. The risks of harm from security breaches are often uncertain. A breach of personal or otherwise sensitive information should be the standard for reporting.

- The bill exempts unauthorized, but "good faith," acquisitions of personal information for "lawful purposes" as potential breaches, unless there is "unauthorized use." This is a vague and potentially dangerous exemption. An unauthorized acquisition of personal data is a warning sign that the entities involved do not have adequate security controls or data policies in place, regardless of whether the data was used improperly.

- "Encrypted" is defined as a process using a 128-bit key. Legislation should not be technology-specific in this way. Whether encryption is secure cannot be defined solely by key length; key length tells us nothing about security unless we know what cryptographic system is actually being used. For example, in 2016 the National Security Agency (NSA) recommended against using 128-bit keys (AES) for the government's Top Secret systems, requiring a key of at least 256 bits. That does not mean 128-bit keys under AES are never good enough; it depends on the risk and should not be specifically legislated. Legislation should use a more general term like "state of the art," and this should be left for courts to define based on current scientific standards, not further defined by legislation or regulation. It is unrealistic to expect the RI Department of Business Regulation to be able to keep up to date with encryption standards.

- Defining "personal information" by categories of direct identifiers could have substantial and adverse consequences. The list of direct identifiers is also too brief, excluding a host of common identifiers. It is also a mistake to exclude publicly available information, as previously-obscure public records provide a host of detailed information that could (especially when aggregated) be useful to identity thieves and other criminals. Personally identifiable information should be defined as *any information that is linked or could be linked, together with other information, to identify a person.* It cannot be reduced to a list. As early as 2000 – almost two decades ago – it was shown that 87% of the U.S. population can be identified by date of birth, gender and zip code.[2] Since then, there has been continuing research showing the many ways in which allegedly anonymized data is not secure.
- The "substitute notice" provisions are inadequate. "I don't have contact information" should not be a catch-all excuse for a failure to do due diligence to provide notice of a data breach.

The duty to report data breaches at 6-48.1-4 is inadequate.

- The legislation provides no time limit for notice of a data breach, instead providing that notice must be provided "as soon as practicable and without unreasonable delay." There should be a realistic, but short, time limit for notice.

The obligation to comply with RI law should be independent of federal laws and regulations

- The legislation provides at 6-48.1-6 that compliance with applicable federal laws and regulations regarding a data breach exempts businesses or entities from compliance with the Rhode Island data breach law. However, there is no general federal data breach law. Sector-specific federal laws and regulations may provide lax or no standards for reporting of data breaches. This is why state data breach laws are necessary. Complying with federal laws and regulations should not exempt businesses from complying with state data breach reporting laws.

[2] L. Sweeney, Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000.

Penalties are inadequate and should be clarified.

- The penalties provided in 6-48.1-7 ($5,000 maximum per violation, and $10,000 per violation for violating a court order) are low enough that they could seriously undermine the legislation. If a "violation" is a security breach event, a company may prefer to simply ignore the law and pay the fine as part of a cost of doing business. This has been common practice among some bad actors in the technology world, including very large companies (like Facebook) that can afford to ignore fines. The law should also be clarified as to whether a "violation" is a single security breach event, or whether each record that is breached counts as a separate violation (which would obviously result in the fines being much higher). For large technology or other firms with sensitive data, a better approach would be to permit fines that are large enough to create incentives for compliance; the maximum fines could be set at a dollar amount that is high enough to provide appropriate deterrence or as some percentage of the total revenue of a company, whichever is larger. This is the approach taken by the European General Data Protection Regulation (GDPR), which provides maximum fines of up to 20 million euros or 4% of annual company turnover, whichever is higher, for the most egregious violations.

The private right of action should include equitable relief.

- The private right of action at 6-48.1-8 is a good idea to supplement enforcement of the act, given the limited resources available to the RI attorney general's office. However, the effectiveness of this remedy is undercut by denying equitable relief in private suits for enforcement of the act. Plaintiffs may be more interested in ensuring against future harms from shoddy security practices than they are in compensation. The courts should be empowered to provide such remedies.

"Rhode Island Right-to-Know Data Transparency and Privacy Protection Act"

- The legislative findings are well-drafted and affirm important privacy principles.

- The definition of "personally identifiable information" in 6-48.1-3 is far superior to the definition in the data breach bill, and is a good starting place for what that bill should require. While it lists categories of personally identifiable information and includes examples of direct identifiers in each

category, these lists are is far more inclusive and the bill is careful to note that the lists of identifiers are merely illustrative, not exclusive.

- Some of the exemptions are overbroad. Tax-exempt organizations include major entities (universities, etc.) and should not be exempt entirely from the bill. "Statistical information and aggregate customer data" should not be exempt entirely from the bill, as this information can often be readily re-identified and may pose privacy risks.

"LC 702 - Office of Information Technology and Security"

- The establishment of this office would be a good step for Rhode Island. The office should be careful to use a process that ensures systems have security goals and outcomes, and that these goals and outcomes are measurable. The federal government's approach to public IT management under the Federal Information Security Management Act (FISMA) has been criticized in the past for taking a checklist-based approach to security that measures compliance, not security. The Obama administration made a strong effort to reform FISMA to make it more effective. Rhode Island should reference this experience.

"Biometric Information Privacy Act"

- Obvious biometrics, such as photographs, are excluded. Facial recognition technology continues to advance and pose a major threat to privacy. While newsgathering, personal photos, and other issues pose obvious complications that may require some carefully-drafted exemptions, entities that collect photographs should not simply be let off the hook from all regulation under the bill.

- Affirmative, opt-in consent is the correct standard for collecting biometric information, but the bill undercuts this standard by providing that "a person's signature or a click in an online check box" automatically counts as opt-in consent. Clicking "I accept" or signing a lengthy form does not ensure that there is true, voluntary consent, as should be required for collecting a biometric identifier.

- The exemption for collection of medical information is overbroad. While it makes sense to ensure that health care providers are not subject to unnecessary new burdens, DNA information is particularly sensitive and health care providers should not be left entirely out of the bill.

- Companies should not be allowed to collect biometric identifiers without consent simply because they are doing so for a "security purpose." This undermines the intent of the bill.

- Likewise, financial transactions should not be exempted entirely from the bill. If banks want to collect biometrics, they should be required to obtain consent and to provide alternate methods to authenticate transactions for those who wish to opt out.

- There are exemptions for collecting biometrics without consent that are overbroad and could compromise the purpose of the bill. These include the exemptions 1) for collecting biometrics in accordance with "purposes authorized and conducted pursuant to state or federal law" and 2) for collection by "third-party data storage providers." These should be narrowed and clarified or eliminated.

"RD700a – The Consumer Personal Data Protection Act of 2019"

This is modeled on a Vermont law. While the intent of this legislation is good, there are loopholes which could undermine its effectiveness. Rhode Island should fix these loopholes.

- Again, the definition of covered information in 64.48-1-3(1) ("brokered personal information") should be revised. While the bill does include a "catch-all" in addition to direct identifiers, the standard is too narrow (requiring the information to "allow a reasonable person to identify the consumer with reasonable certainty") and excludes publicly available information. (See discussion above about how exposure of previously obscure publicly available information can pose privacy risks).

- The definition of "data broker" in 64.48-1-3(4) is also too narrow, excluding any business which has a direct relationship, *even a past relationship*, from the bill. A data broker could easily purchase a business (even a failing business) solely for its personal data and evade regulation under the bill by claiming a relationship with the people in that business's databases. The exemption also ignores that data brokers may also operate other businesses that do have direct relationships with many customers (e.g., Lexis-Nexis). A major financial institution or digital services company (like Facebook) could offer data broker services while apparently avoiding responsibility under the act. It is hard to

see what purpose such a narrow definition serves, since the main responsibility the act imposes – implementing an information security program – is a prudent step that any business with sensitive personal information should be undertaking anyway, regardless of whether they have a direct relationship with individuals.

- The definition of "data broker security breach" should not exempt employees or agents of the data broker who are acting in "good faith." An "agent" might include any number of third-party companies with which a data broker has a relationship. Even "good faith" breaches of security could have significant unforeseen consequences.

- The definition of "personally identifiable information" is far too narrow, excludes a great deal of sensitive information, and should certainly include publicly available information. See discussion above.

- The law should, at a minimum, affirmatively require data brokers to make available easy-to-use opt-out mechanisms, and should not be limited to requiring data brokers simply to disclose opt-out policies if they have them. This provision might even be used by a data broker's lawyer to undermine an argument that a data broker is already required by existing law to provide an opt-out.

- The penalty for failure to register (maximum of $10,000 per year) may be inadequate as applied to some large technology companies that will decide they can ignore the law and pay the fine as a cost of doing business if they are caught. A more effective method would be to link the maximum fine to a company's gross revenue (see discussion above).

"Public Utilities and Carriers – Student online personal information protection."

- The exemption for use of private K-12 student information should be available only if the researcher has complied with ethical guidelines, including (as applicable) the human subject research guidelines and review by an institution review board (IRB).

- There should not be exemptions for use of so-called "deidentified" student data. Many attempts to deidentify data have failed, leading to allegedly deidentified or anonymized data to be easily linked to a person. Legislation should not encourage this risky practice.

- Additional concerns about this proposal, in light of its conflict with current state law, are included separately.