Attachment #26

ACLU, 5/2/19 letter and attachment

ACLU
AMERICAN CIVIL LIBERTIES UNION
Rhode Island

128 Dorrance Street, Suite 400
Providence, RI 02903
Phone: (401) 831-7171
Fax: (401) 831-7175
www.riaclu.org
info@riaclu.org

TESTIMONY ON THE PROPOSED PACKAGE OF LEGISLATION PUT FORTH BY THE RHODE ISLAND ONLINE DATA TRANSPARENCY AND PRIVACY PROTECTION COMMISSION
May 2, 2019

The ACLU appreciates the opportunity to provide commentary on the proposed package of legislation being evaluated today by the commission. As we have noted previously, we believe that effective legislation must prioritize the protections of consumers over the profits of the tech industry. We would like to focus our testimony on two of the three pieces of legislation, the "Model Student Online Personal Information Protection Act" and the "Rhode Island Right-to-Know Data Transparency and Privacy Protection Act." Additionally, we have attached copies of the commentary which was given to the commission on the "Consumer Personal Data Protection Act of 2019" earlier in the session by Timothy Edgar from Brown University.

In February, we expressed considerable concerns regarding a draft of the student privacy bill which we believed would weaken the protections that existing law provides. In light of the most recent draft which we have examined, we would like to reiterate and expand upon these concerns. Not only do our initial thoughts about the legislation stand, but we find that this new model bill is significantly weaker and would allow the tech industry broad-reaching access to, and use of, student data under the guise of protecting it. For the convenience of the committee, we have attached a copy of our previous testimony detailing these specific concerns with updated page and section numbers to reflect the new bill draft.

Our National office also apprised us that this specific model bill has a history of being the tech industry's response to campaigns calling for comprehensive improvement of statutory data privacy protections. This bill began popping up a few years ago in response to multi-state campaigns, supported by the ACLU, which would have considerably restricted commercial access to students' online information. We have also been advised that this "model" bill has been uniformly rejected by every state in which it has been introduced because of its flagrant prioritization of industry over consumer needs.

One particularly concerning aspect of this new draft is the allowance for operators to use "recommendation engines," which capture consumer data in order to provide relevant and individual product recommendations. Section (d) on page 5 opens the door for large companies to use student data to promote their products across multiple industries. Imagine Amazon working in the education space and using student data to "educationally" promote good food choices from Whole Foods, or an educational app which recommends additional study materials for a fee to students who consistently answer questions wrong; these are the scenarios that this bill allows, and that it is designed to allow. We urge that the commission reject this legislation from consideration for introduction.

We have also attached for the consideration of the committee a copy of our proposed amendments to the current student data privacy statute, Chapter 16-104, which would enhance protections against security breaches and provide for deletion of student data under specific circumstances.

The "Rhode Island Right-to-Know Data Transparency and Privacy Protection Act" we find to be comprehensive and focused on the rights of the consumer. However, we believe with one significant amendment and a few smaller changes, its purpose could be more fully achieved.

This bill notes under its legislative findings that a critical component of consumer transparency is the ability for consumers to have access to effective "opt-in" and "opt-out" strategies. Yet, it does not require the implementation of an opt-in option on behalf of the consumers. In the realm of data privacy, opt-in procedures, as opposed to opt-out procedures, are significantly more transparent and intentional. While opt-out procedures place the burden on the consumers themselves, and in some cases may not adequately inform the consumer of the ability to opt-out, opt-in procedures give consumers the opportunity to deliberately decide the fate of their personal data, and, as such, allow a substantial amount of autonomy in the potential marketing of data.

To better fulfill its legislative findings, we believe that it would be appropriate to include language which would guarantee an opt-in option for consumers. We have attached suggested language to strengthen this aspect of the bill, and we hope that the commission will favorably consider it. We also included a proposed definition of "opt-in consent" to be added under "Definitions."

Three additional minor amendments to this bill would make it inclusive of the full spectrum of service providers that collect data and the process of data marketing. Under the definition of "Operator" on page 4, we propose including the language "or any other communications, utility, or information service" following the word "service" on line 6. Cable companies and information service providers are similar to the other listed companies in their method of collecting data, and we see no reason to exclude them from the provisions of this bill.

We also encourage the inclusion of "Biometric information" in the bill under the list of personally identifiable information. Finally, we have also attached suggested amendments to the definition of "Disclose" on page three which would strengthen the language regarding permitted disclosure and provide for deletion of data after it has been disclosed for its specified purpose.

This commission has the opportunity to make Rhode Island a leader in the national conversation around consumer and data privacy. We believe that with the review of our suggestions, Rhode Island can emerge on the forefront of comprehensive laws which effectively protect consumers. Thank you for your consideration.

TITLE 16
Education

Chapter 16-104
Student Data-Cloud Computing

Section 16-104-1

§ 16-104-1. Student data-cloud computing.

16-104-2. Definitions.

(a) For the purposes of this chapter:

(1) "Cloud computing service" means a service that enables convenient on-demand network access to a shared pool of configurable computing resources to provide a student, teacher, or staff member account-based productivity applications such as email, document storage, and document editing that can be rapidly provisioned and released with minimal management effort or cloud computing service provider interaction.

(2) "Cloud computing service provider" means an entity other than a public elementary or secondary school that operates a cloud computing service.

(3) "Process" means to use, access, manipulate, scan, modify, transform, disclose, store, transmit, transfer, retain, aggregate, or dispose of student data.

(4) "Student data" means any information in any media or format created or provided:

(i) By a student; or

(ii) By a school board employee about a student in the course of using a cloud computing service, including the student's name, email address, postal address, email message, documents, unique identifiers, and metadata.

16-104-3. Cloud Computing Services.

(a) Notwithstanding any general or special law to the contrary, any person who provides a cloud computing service to an educational institution operating within the state shall process data of a student enrolled in kindergarten through twelfth (12th) grade for the sole purpose of providing the cloud computing service to the educational institution and shall not process such data for any commercial purposes, including, but not limited to, advertising purposed that benefit the cloud computing service provider.

(b) The cloud computing service shall:

(1) establish, implement, and maintain appropriate security measures, consistent with best current practices, to protect the student data that the cloud computing service sends, receives, stores, and transmits in conjunction with the service provided educational institutions in the state;

(2) establish and implement policies and procedures for responding to data breaches involving the unauthorized acquisition of or access to any student data collected by the cloud computing service. Such policies and procedures, at a minimum, shall:

(i) require notice be provided by the cloud computing service provider to any and all affected parties, including educational institutions and cloud computing service student users and their parents or legal guardians, within thirty (30) days of the discovery of the breach;

(ii) require the notice to include a description of the categories of student data that were, or were reasonably believed to have been, accessed or acquired by an unauthorized person; and

(iii) satisfy all other applicable breach notification standards established under state or federal law; and

(3) Permanently delete all student data collected by the cloud computing service within ninety (90) days of the termination of the student user's account, or upon request by the student user, the student user's parent or legal guardian, or the student user's educational institution.

16-104-4. Limitations on Use. Evidence or information obtained or collected in violation of this chapter shall be promptly deleted or destroyed and shall not be admissible in any civil or criminal trial or legal proceeding, disciplinary action, or administrative hearing, or used by an educational institution for any other purpose.

16-104-5. Penalties. In any civil action alleging a violation of this chapter, the court may award to a prevailing party declaratory and injunctive relief, damages, and reasonable attorneys' fees and costs.

PROPOSED CHANGES TO SECTION 6-48.1-4 "Information sharing practices.", page 5-6

(a) An operator of a commercial website or online service or any other communications, utility, or information service that collects, stores and sells or Discloses Personally Identifiable Information ~~through the internet~~ about individual customers residing in this state who use or visit its commercial website or online service shall, in ~~its customer agreement or incorporated addendum or in another~~ conspicuous location on its website or online service platform where similar notices are customarily posted:

(1) Identify all Personally Identifiable Information that the operator collects through the website or online service about individual customers who use or visit its commercial website or online service; and

(2) Identify all Third Partiers to whom the operator may Disclose Personally Identifiable Information if permission by the customer to which it pertains provides permission to do so.

(b) An operator may only Disclose Personally Identifiable Information identified in Part (a)(2) of this subsection if it obtains prior Opt-In Consent from the customer to which it pertains, who may revoke that consent at any time.

(1) An operator shall employ a mechanism for customers to grant, deny, or withdraw consent that is easy to use, clear, conspicuous, comprehensible, not misleading, persistently available through all methods the operator gives customers for account management, in the language primarily used to conduct business with the customer, and made available to the Customer for no additional cost.

(2) A customer's grant, denial, or withdrawal or consent shall be given effect promptly and remain in effect until the Customer revokes or limits the grant, denial, or withdrawal of consent.

(c) An operator shall not:

(1) Refuse to serve a customer who does not provide consent under this subsection; or

(2) Charge a customer a higher price or offer a customer a discount or another benefit based on the customer's decision to provide or not provide consent.

PROPOSED CHANGES TO SECTION 6-48.1-3 "Definitions."

Amend Definition of "Disclose" on page 3 to include:

(3) "Disclose" means to disclose, sell, release, transfer, share, trade, disseminate, make available, or otherwise communicate orally, in writing, or by electronic means or any other means to any individual or Third Party. "Disclose" does not include the following:

(i) Disclosure to an affiliate.

(ii) Disclosure of Personally Identifiable Information by any entity to a Third Part under a written contract authorizing the Third Party to utilize the Personally Identifiable Information to perform services exclusively on behalf of and for the benefit of the disclosing entity, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, or similar services, but only if:

(A) The contract prohibits the Third Party from using the Personally Identifiable Information for any reason other than performing the specified service or services on behalf of such entity and from Disclosing any such Personally Identifiable Information to additional Third Parties;

(B) Any data that is shared or otherwise disclosed is deleted and destroyed by the Third Party after the specified services are fully performed; and

(C) The entity effectively enforces these prohibitions.

Add after the definition of "Operator" on page 4, a definition for "Opt-In Consent":

(5) "Opt-In Consent" means affirmative, express customer approval for the requested Disclosure of that customer's Personal Identifiable Information after the customer is provided with information set forth in Section 6-48.1-4(A).