NECTA
New England Cable & Telecommunications Association, Inc.
Ten Forbes Road • Suite 440W • Braintree, MA 02184
TEL: 781.843.3418 • FAX: 781.849.6267

NECTA Comments to Vermont Privacy Working Group

November 15, 2018

Examples of legislation that would address student data privacy (child protection focused)

The recently enacted Illinois Student Online Personal Protection Act, 815 ILCS 505/2Z, is a good model from which to develop student data privacy legislation. This law prohibits operators of websites, mobile apps, and other online services and applications from (1) knowingly engaging in targeted advertising, if such advertising is based on any information that the operator has acquired because of the use of that operator's site, application or service for K through 12 school purposes; (2) using information created or collected by the operator's site, service or application to create a profile about a student, except when such information is used for K through 12 purposes; (3) selling or renting a student's information; or (4) disclosing certain information, except for specified purposes. These prohibitions apply only to operators with actual knowledge that the site, service, or application is used primarily for K through 12 purposes and was designed and marketed for K through 12 purposes. The Attorney General enforces the Act.

Example of a state government data disposal requirement (this requirement exists on the books in Vermont but government is currently exempt from the statute)

Multiple states have enacted laws that impose data disposal obligations on state governmental entities. For instance, Massachusetts law establishes a set of "minimum standards for proper disposal of records containing personal information," applicable not only to private "person[s]" but also to state and local "agenc[ies]." Mass. Gen. Laws Ch. 93I, §§ 1, 2. Massachusetts's statute provides, among other things, that "paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed," and that "electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed." *Id.* § 2.

Other states have enacted statutes establishing an affirmative duty for agencies to dispose of data in certain circumstances. Michigan law, for example, requires that "a person or agency that maintains a database that includes personal information regarding multiple individuals shall destroy any data that contain personal information concerning an individual when that data is removed from the database and the person or agency is not retaining the data elsewhere for another purpose not prohibited by state or federal law." Mich. Comp. Laws § 445.72a. *See* also this link from the National Conference of State Legislatures -- http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx -- which indicates that at least 32 states and Puerto Rico have enacted laws that require entities to destroy, dispose, or otherwise make personal information unreadable or undecipherable. The summary chart on this website also indicates whether each state law applies to businesses and/or government.

NECTA
New England Cable & Telecommunications Association, Inc.
New England Cable & Telecommunications Association, Inc.
Ten Forbes Road • Suite 440W • Braintree, MA 02184
TEL: 781.843.3418 • FAX: 781.849.6267

The current federal framework that regulates privacy

Robust federal frameworks already exist for protecting consumer privacy. The Federal Trade Commission (FTC) also oversees a comprehensive and technology-neutral federal framework for protecting consumer privacy. Under its Section 5 authority to prevent "unfair and deceptive acts and practices," the FTC has established clear guideposts for ensuring privacy online, based on the core principles of transparency, choice/consent, and privacy-by-design. In addition to this Section 5 oversight, the FTC enforces a wide array of other federal privacy statutes, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and many more. Over the years, the FTC has brought more than 500 cases protecting the privacy and security of consumer information, including many enforcement actions in the Internet arena. Through its active enforcement efforts, the FTC has been successful in stopping violations of consumers' privacy, preventing future violations, entering into consent decrees obligating companies to implement comprehensive privacy and data security programs, and obtaining significant monetary penalties where appropriate.

And beyond the FTC, other federal privacy laws apply to protect collection, use, and disclosure of personal information in particular industry sectors, such as Sections 338 and 631 of the Communications Act for satellite and cable operator video providers, Section 222 of the Communications Act for voice telecommunications carriers, the Family Educational Rights and Privacy Act for protecting student records, the Electronic Communications Privacy Act, the CAN-SPAM Act for email marketing, the Gramm Leach Bliley Act for financial privacy, among others.

What federal legislation might look like on privacy

Federal legislation should create a national, technology-neutral privacy regime that includes robust, enforceable standards and applies uniformly to all entities in the online ecosystem. Congress should take a balanced approach, providing both strong consumer protection *and* sufficient flexibility to allow companies to innovate and grow. Finally, federal legislation should preempt state privacy laws, promoting greater consistency for consumers and certainty for industry. A state-by-state approach creates a patchwork of differing rules and regulations that is confusing to consumers.

Brief overview of CA privacy law and GDPR while highlighting the hurdles for compliance including financial burdens of compliance

In the privacy context, the California legislature recently passed the California Consumer Privacy Act of 2018 and its "clean up" bill SB 1121 (collectively, the CCPA). The CCPA imposes numerous costly burdens that will require businesses to make substantial changes to their data collection, use, and disclosure mechanisms, while providing consumers with little additional privacy protections beyond what is already provided under the FTC's privacy framework. For example, the CCPA requires specific notice to consumers on every Internet web

NECTA
New England Cable & Telecommunications Association, Inc.
New England Cable & Telecommunications Association, Inc.
Ten Forbes Road • Suite 440W • Braintree, MA 02184
TEL: 781.843.3418 • FAX: 781.849.6267

page where personal information is collected, which in light of the law's excessively broad definition of personal information will require excessive notices to consumers that would become redundant, inconvenient, and likely would be ignored by customers. If the law is not revised, it will cause thousands of California businesses to incur substantial costs and operational burdens to comply with the onerous and expansive obligations regarding consumer access, portability, and deletion of data that in some respects exceeds even the European Union (EU) General Data Protection Directive (GDPR). In other respects, the law even weakens consumer privacy protections. For example, it requires that businesses deliver consumers' personal information to them in a portable format, creating unnecessary risks to both the security of the consumer's information and the business' ability to protect such information. The CCPA goes beyond the FTC's established privacy framework in that it applies its protections to households rather than requiring information to be linked or reasonable linkable to an *individual.* The CCPA opt-out scheme limits consumer choice and restricts businesses' ability to communicate with their consumers and let them know about items that may be of interest to them.

The GDPR, which came into effect on May 25, 2018, requires companies that process the data of EU data subjects to adopt extensive technical and organizational measures, as well as to adhere to specified data security systems. Compliance with the GDPR requires companies to adopt substantial recordkeeping procedures and costly systems to track compliance measures. Further, companies must invest resources in responding to the GDPR's numerous data subject requests, notably the "right to be forgotten" which requires deletion of customer data in certain circumstances, as well as rights to access and rectification. Additionally, data controllers must undergo an extensive contracting process to ensure all third parties that process personal data on their behalf conform to the GDPR's strict obligations. GDPR compliance is not limited to European companies, but applies to U.S.-based companies that process the data of individuals located in the E.U when offering goods or services targeted at customers in the EU. The cost of compliance for companies has already been substantial. As of May 2018, Fortune 500 companies in the U.S. had already spent an estimated $7.8 billion on GDPR compliance. Oliver Smith, *The GDPR Racket: Who's Making Money From This $9bn Business Shakedown*, Forbes.com, May 2, 2018, https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#6e52c5134a22. And according to a recent survey by Dimensional Research, 31% of U.S. companies intend to spend $1 million on compliance between June and December 2018. TrustArc Press Release, July 12, 2018, https://www.trustarc.com/press/20-of-companies-report-being-gdpr-compliant-post-may-25-deadline/. Because the CCPA contains many provisions that are inconsistent with those imposed by the GDPR, the costs of new infrastructure necessary to comply with the CCPA will only add to this financial burden, and these costs undoubtedly will be passed to consumers.