Testimony of Nancy Libin

On Behalf of NECTA — New England Cable & Telecommunications Association

Before the Committee on General Law

on

Connecticut SB 893, An Act Concerning Consumer Privacy

February 25, 2021

Senate Chairman Maroney, House Chairman D'Agostino, Senate Vice Chairman Fonfara, House Vice Chairman Gibson, Senate Ranking Member Witkos, and House Ranking Member Rutigliano, thank you for the opportunity to submit this testimony regarding Senate Bill (SB) 893 relating to the privacy of personal information. My name is Nancy Libin, and I am a partner at the law firm of Davis Wright Tremaine LLP, where I co-chair the Technology, Communications, Privacy & Security practice. Prior to private practice, I served from 2009 to 2012 as the Chief Privacy Officer of the U.S. Department of Justice (DOJ), where I was the DOJ representative to the Obama White House's interagency task force that developed the Obama Administration's approach to consumer data privacy. Prior to that, I was counsel to then-Senator Joseph Biden on the Senate Judiciary Committee, where I advised Senator Biden on privacy and cybersecurity issues.

I am here today on behalf of the New England Cable & Telecommunications Association (NECTA), the regional trade association that represents private cable and telecommunications companies in Connecticut and several other states in New England. We commend the committee for addressing this very important issue.

NECTA's members work hard to protect their customers' privacy and maintain their customers' trust. In doing so, they operate under a regime of federal and state privacy laws and regulations, including the privacy framework of the Federal Trade Commission (FTC), the Communications Act, the Cable Act, the Children's Online Privacy Protection Act (COPPA), the Video Privacy Protection Act, the Electronic Communications Privacy Act, and Connecticut state law. Some members also are subject to the European Union's General Data Protection Regulation (GDPR). In addition, none of the Connecticut NECTA members share their customers' sensitive personal information (such as financial, children's, and health information)

without their affirmative, express consent. All of our members' privacy practices, as outlined in their publicly available privacy notices, are clear, transparent, and conspicuous for all NECTA members' customers, and enforceable under Connecticut's unfair and deceptive trade practices act.

As a general matter, online privacy is fundamentally an interstate – and therefore federal – issue, best addressed by Congress. For this reason, our members have long supported strong *federal* consumer privacy legislation that would ensure uniform privacy protections and requirements and that would apply the same way across the country no matter where consumers are at any given time or where companies in the United States are doing business. We are hopeful that the Biden Administration, supported by a Congress under Democratic control, will enact comprehensive and robust federal privacy legislation that would apply uniformly to all entities throughout the United States. Indeed, there is reason to be optimistic, given the strong bipartisan support for such legislation and increasing calls for its enactment.

Businesses that operate in the Internet ecosystem face the prospect of conflicting privacy rules as states seek to follow California in enacting consumer privacy legislation. This amalgam of potential obligations threatens to create insurmountable challenges. State laws that apply different standards and rules depending on where a consumer resides or happens to be at any given moment when interacting with a company will set impossible compliance goals for businesses and, more important, a confusing and frustrating experience for consumers. Indeed, this is unfortunately what is increasingly happening now at the state level, where California, Maine, Virginia, and a few other states have passed their own versions of a privacy law (and many others are in the legislative pipeline) that are all very different, leading to confusion for consumers and uncertainty and mounting burdens and costs for thousands of businesses.

Consumers should not have to worry about receiving different types of protection when they travel around the country, and businesses should not have to incur significant costs for complying with this inconsistent regime when resources instead could have been invested in new products, services, and innovations that benefit their customers.

That said, should Connecticut decide to enact a state consumer privacy law, SB 893 is the right approach. While far from perfect, it provides consumers with meaningful protections and rights, while allowing businesses to use data to engage in legitimate business activities, innovate, and adapt to ever-changing technology. It attempts to achieve this important balance by focusing on potential privacy harms to consumers, such as by subjecting sensitive data to heightened protection, while allowing greater flexibility to share and use non-sensitive data.

Most important from a business perspective, SB 893 mirrors the Virginia privacy bill, which passed the Virginia General Assembly last week and borrows responsibly from the GDPR, which is often called the most rigorous privacy framework in the world, while incorporating elements of the new California privacy law to ensure basic compatibility with that regime. While NECTA members reiterate their very strong endorsement of robust federal privacy legislation and opposition to the piecemeal approach developing in the states, we also recognize that as it is currently written, SB 893 at least attempt to strike a reasonable balance between ensuring strong privacy protections for consumers while providing clear definitions and straightforward requirements for businesses that may help reduce the substantial burdens and costs for complying with such an ever-fluctuating state patchwork.

I. SB 893 Provides Strong Baseline Protections for Consumers

SB 893 gives Connecticut consumers comprehensive baseline privacy protections that currently do not exist under Connecticut law. Specifically, the bill gives consumers the right to

know what information businesses collect about them, as well as the right to access, correct, delete, and obtain a copy of their data to port to another business. The bill also requires businesses to let consumers opt out of the sale of their personal data and the use of their data for targeted advertising or profiling, when such profiling is used to make decisions that have legal or similarly significant effects on consumers. And it goes even further than California law with respect to requirements related to data protection assessments (SB 893 requires businesses to conduct them for more processing activities and unlike California, gives the AG authority to obtain them), and in protecting "sensitive data" by requiring businesses to obtain consent from consumers before processing such data, rather than just giving consumers the right to limit the *use* of such data in limited circumstances.

The bill also imposes strong data minimization and purpose limitation obligations on businesses, requiring them to obtain consumers' consent before processing personal data for any purpose not reasonably necessary for, or compatible with, the purposes for which they originally collected the data. This minimization requirement protects consumers while allowing businesses to develop new services and improve existing ones. Some have called for a prohibition by default of *all* data sharing for commercial purposes. However, no other privacy law, including the CCPA, takes such an extreme position. SB 893 borrows the definition of consent from the GDPR, requiring a "clear affirmative act" that is "freely given, specific, informed, and unambiguous." By requiring that consent be "freely given" and "informed," this definition forecloses the use of "dark patterns" or other deceptive user interfaces that could nudge a consumer to consent to certain practices related to their sensitive data or to processing for new purposes that may not be fully apparent or that they might not fully comprehend. Finally, the bill requires businesses to provide consumers with notice of their rights and explain how consumers

can request to exercise them, and they must then respond to authenticated requests within 45 days of receiving them. Requiring consumers to make the requests, and allowing businesses to authenticate them, provides important protection for consumers because it permits businesses to establish controls to keep bad actors from wrongfully obtaining consumers' information or otherwise interfering with a consumer's relationship with the business. If consumers are not satisfied with a business's response to a request, they may appeal through an internal appeals process that businesses must develop, implement, and make conspicuously available to consumers. Ultimately, consumers may file a complaint with the Connecticut Attorney General using the contact information or other online mechanism that businesses are required to provide to consumers.

II. SB 893 Focuses on Actual Harms to Consumers and Preserves Flexibility for Connecticut Businesses

SB 893 appropriately regulates conduct that poses an actual risk of harm to consumers while allowing businesses to continue to compete, innovate, and engage in routine business operations. For instance, it makes a regulatory distinction between sensitive and non-sensitive data, and it excludes from coverage any data that is not reasonably linkable to an individual. In this respect, the bill takes an approach similar to the widely respected privacy framework that the FTC established during the Obama-Biden Administration. The FTC developed its framework after several years of fact-gathering and analysis during which it heard from multiple stakeholders, including consumers, privacy advocates, academics, and industry. Due to its thoughtful balancing of important imperatives, that framework was lauded by consumer groups and industry alike.

The bill takes this balanced approach in other ways, too. It ensures small businesses can grow by exempting them from coverage, and it excludes personal data that businesses collect in

the employment or commercial contexts, focusing instead on actual *consumers—i.e.,* residents of the State who act in a household or individual context. It prohibits the use of personal data to discriminate on the basis of race or other protected class and prohibits charging different prices—or providing inferior goods or services—to consumers who exercise their rights. It allows businesses to share data with their affiliates for common commercial activities, while giving consumers control over businesses' disclosures to unrelated entities for monetary consideration, targeted advertising, and profiling—*i.e.,* processing that predicts certain aspects of a consumer's characteristics, when such processing could have an adverse impact on consumers. With respect to profiling, the bill would allow companies to profile consumers for beneficial reasons, such as to ensure that certain consumers are not inadvertently being denied access to their products and services because of their racial or ethnic origin. With respect to advertising, it protects against the unfettered dissemination of personal data throughout the advertising ecosystem, while ensuring that businesses can continue to use first-party data for advertising and engage in contextual advertising, which does not involve the tracking of consumers across sites or apps.

Finally, the bill effectively balances the twin objectives of encouraging compliance and punishing violations by allowing businesses 30 days within which to come into compliance after being informed by the Connecticut Attorney General that they are in violation of the Act. If a business fails or refuses to cure the violation within that time period, the Attorney General can bring an enforcement action. This approach ultimately benefits consumers, because it encourages businesses to fix mistakes quickly and spend resources on compliance instead of defending against regulatory enforcement proceedings. Indeed, in testimony before the U.S. Congress, the California Attorney General characterized the similar right-to-cure provision in the

California Consumer Privacy Act as very effective in incentivizing businesses to fix compliance errors within 30 days.[1] And the threat of enforcement and possible penalties under SB 893 are even greater than under the CCPA: the bill gives the Connecticut Attorney General authority to seek penalties of up to $7,500 *per violation—triple* the CCPA's baseline civil fine amount of $2,500 for violations. The significant penalties that businesses will face for non-compliance are more than enough to deter wrongful conduct. And by relying on regulatory enforcement instead of a private right of action, the bill ensures that businesses can devote resources to privacy-by-design and other proactive compliance measures rather than diverting them toward litigation defense.

III. SB 893 Is Generally Interoperable with Other Laws

We commend the decision to adopt the framework that the Virginia legislature codified, which in turn is largely compatible with other privacy laws. By enacting a law that is generally interoperable with the state law to date, Connecticut can avoid creating potential legal conflicts and enable businesses to adopt a single set of internal business processes – or build on existing privacy compliance programs – to comply with the laws. Interoperability also benefits consumers because it ensures that they will receive consistent protections across different jurisdictions and it lowers barriers to market entry, fostering competition – which means greater choice and lower costs – for goods and services in the marketplace.

Any substantive changes to the bill would undermine the interoperability that SB 893 currently achieves, however. We therefore respectfully urge the committee not to amend the bill. Even minor changes can have unintended consequences and can – from a business operations

[1] Oral Testimony of Xavier Becerra, Attorney General, State of California, *Revisiting the Need for Federal Privacy Legislation*, U.S. Senate Committee on Commerce, Science, and Transportation, Sept. 23, 2020.

standpoint – create insurmountable conflicts with other laws. California is instructive in that regard. The California legislature had to amend the CCPA twice after its initial passage because of seemingly innocuous language that posed significant problems. We recognize the importance of this policy issue to the committee as evidenced by the very first bill on the hearing agenda for today, SB 156 *An Act Concerning Consumer Privacy*, and are very pleased that you are holding this hearing today and giving the issue careful consideration.

At the same time, I do not wish to overstate the value of interoperability; as noted above, the clear preference of NECTA members and the clear benefits for consumers would be greater if Congress were to enact a single uniform privacy law that applies the same robust protections for consumers and the same sensible requirements for all businesses across all states.

VI. Conclusion

As mentioned above, NECTA strongly prefers federal legislation that would apply uniformly to all businesses across the United States. A slew of inconsistent state laws would make compliance impossible, undermining the very consumer protection that privacy laws seek to provide. Indeed, each new state privacy law that differs from other laws – even in seemingly modest ways – requires businesses to make a host of internal changes to business operations and in some cases to renegotiate contracts with each service provider and third party with which they share data. Although we typically would advocate against new state privacy laws for the reasons outlined above, if Connecticut is inclined to pass privacy legislation, SB 893 is at least compatible approach that establishes strong protections for consumers while reducing excessive compliance costs and burdens for covered businesses.

Thank you again for the opportunity to appear before you today.