Testimony of Nancy Libin

On Behalf of Comcast

on

Senate Bill 6, An Act Concerning Personal Data Privacy and Online Monitoring

March 3, 2022

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) 6 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 Joe Biden on the Senate Judiciary Committee, where I advised Senator Biden on privacy and cybersecurity issues.

I am here today on behalf of Comcast. We commend the Committee – and in particular Senator Maroney and Representative Arconti – for their hard work and thoughtful approach in addressing this very important issue.

Comcast is committed to protecting its customers' privacy and earning and maintaining its customers' trust. In doing so, it operates under a regime of federal and state privacy laws and regulations, including the Federal Trade Commission Act's privacy framework, 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. Comcast is also subject to the European Union's General Data Protection Regulation (GDPR). It is important to note that Comcast does not sell its customers' web browsing histories to third parties, nor does it sell customers' sensitive personal information (such as financial, children's, and health information). Comcast's privacy practices and commitments, as outlined

in its publicly available privacy notices, are clear, transparent, and conspicuous for customers, and enforceable under Connecticut's unfair and deceptive trade practices act (*hereafter* CUTPA).

Businesses that operate in the Internet ecosystem face the prospect of conflicting privacy rules as states seek to follow California – and now Virginia and Colorado – in enacting comprehensive privacy legislation. This amalgam of potential obligations threatens to create insurmountable challenges that will confuse, not benefit, consumers. 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 create an impossible compliance burden for businesses and, more important, a confusing and frustrating experience for consumers. Unfortunately, this is increasingly happening now at the state level, where California, Virginia, and Colorado have passed their own versions of a privacy law (and many others are in the state pipeline) all of which are different, leading to confusion for consumers and uncertainty and mounting burdens and costs for hundreds of thousands of businesses in all sectors. Consumers should not have to worry about receiving different types of protection when they travel from one state to another and around the country, and businesses should not have to divert resources to cover the significant costs of complying with this varying regime instead of investing in new products, services, and innovations that benefit and protect their customers.

That said, should Connecticut decide to enact a state consumer privacy law, we believe that some modest changes would have a significant impact by aligning this bill more closely with existing laws. If those changes were incorporated in SB 6, we are hopeful Connecticut's privacy law would come closer to striking the right balance between providing consumers with

meaningful rights and protections while enabling businesses to use data responsibly to engage in legitimate business activities and innovate.

I. SB 6 Should Be Interoperable with Other State Laws

Alignment with existing state law is critical. This is the only way to avoid potential legislative conflicts and enable businesses to adopt a single set of internal business processes – or build on existing privacy compliance programs – to comply with the various laws. Indeed, each new state law that differs from others – even in seemingly modest ways – can require businesses to make a host of internal changes and renegotiate contracts with every service provider and third party with whom they do business. This is already happening with the state laws currently on the books and we respectfully urge the committee to address the interoperability concerns raised today by Comcast and other interested parties. Moreover, alignment, consistency, and interoperability benefits consumers because they ensure that consumers will receive consistent protections across different jurisdictions and they lower barriers to market entry, fostering competition – which means greater choice and lower costs – for goods and services in the marketplace.

While we continue to have concerns about certain elements of the Colorado Privacy Act, it is a good model because it gives strong privacy protections to consumers while providing relatively clear definitions and straightforward requirements for businesses that help reduce the substantial burdens and costs of complying with an ever-fluctuating state patchwork. Instead of imposing a series of prescriptive requirements, the Colorado approach focuses on actual and potential privacy harms by, for instance, requiring assessments of data processing activities that pose privacy risks.

We commend the Committee for largely following the Colorado model, and we urge the Committee to make the following changes to align the bill more closely with that law to ensure that businesses to do not face conflicting obligations:

- *Definition of Biometric Data*: The definition of "biometric data" should be amended to expressly exclude from the definition "a physical or digital photograph, or a video or audio recording or data generated therefrom." Both the Virginia law – and with respect to photographs, even the Illinois Biometric Information Privacy Act – make clear on their face that they do not capture such information.[1] Companies in the online ecosystem increasingly use photographs and audio and video recordings to provide products and services and should not have to obtain opt-in consent before processing such widely available data. Indeed, ambiguity around whether photos and voice and video recordings are covered can undermine the seamless delivery of online services designed to be accessible for people with disabilities. Such services often leverage the use of video and audio technology, and expressly carving out such information from the definition would ensure that businesses could continue to provide such services and innovate in this area to improve accessibility.
- *Global Privacy Control*: We are concerned about the provision requiring businesses to recognize global opt-out signals, because while the idea of a global opt-out provision sounds appealing, there is no consensus regarding what the term means or how businesses should interpret a signal, particularly if the signal contradicts other signals coming from a consumer's browser (if, for instance, the browser's cookies are set to *allow* sharing of information). More time is needed to allow for the development of a

[1] The Colorado Privacy Act does not define "biometric data."

universally recognized standard, as provided in the Colorado law, and to understand how such a signal would work. For this reason, we urge the Committee to amend the bill so that the requirement to recognize such signals would not become effective until January 1, 2025.

- *Definition of Publicly Available Information*: Like other state privacy laws, SB 6 excludes "publicly available information" from the definition of "personal data." Unfortunately SB 6, as drafted, narrows the scope of the exemption, making the bill more restrictive than laws in other states, including Virginia and California, which exclude information that is made available by a person to whom the consumer has disclosed the information, provided that the consumer did not restrict the information to a specific audience. We encourage the Committee to amend the definition to ensure alignment and interoperability with other state laws and to be consistent with public policy trends elsewhere.

We would like to see additional changes to the bill, but these changes would go a long way toward making the bill more consistent and interoperable with existing privacy laws.

II. If Amended, SB 6 Would Provide Strong Privacy Protections and Preserve Flexibility for Connecticut Businesses

With these and other minor changes, SB 6 would give Connecticut consumers comprehensive baseline privacy protections while providing businesses more flexibility to continue to provide their services and innovate. 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 6 requires businesses to conduct them for more processing activities).

The bill provides these protections to consumers while allowing businesses some flexibility to continue to compete, innovate, and engage in routine business operations. For instance, it excludes from coverage any data that is not reasonably linkable to an individual and it ensures small businesses can grow by exempting them from coverage. It also 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 charging different prices—or providing inferior goods or services—to consumers who exercise their rights. And – importantly – it allows businesses to share data with their affiliates for common commercial activities, while giving consumers control over businesses' disclosures to unrelated entities for 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.

Finally, the bill effectively balances the twin objectives of encouraging compliance and punishing violations by allowing businesses 60 days within which to come into compliance after being informed by the Connecticut Attorney General that they are in violation of the Act, provided that the Attorney General determine that a cure is possible. If a business fails or refuses to cure the violation within that time period, the Attorney General can bring an enforcement action with stiff fines. 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 the cure period.[2] While it is prudent that the bill includes a cure provision, we would prefer that the provision be made permanent.

III. Conclusion

In closing, we commend the Committee for its hard work on this very difficult and evolving technical issue. As explained above, 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 reconfigure databases, renegotiate contracts, and revise internal policies and procedures. Therefore, if Connecticut is inclined to pass privacy legislation, we encourage the Committee to amend SB 6 to make it more compatible with the Colorado law which has been proven to provide consumers with strong privacy protections while giving businesses the flexibility to design privacy programs that enable compliance with the growing patchwork of state laws. While we would like to see additional changes, the modifications that we have proposed here would help achieve that goal.

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

[2] 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.