ACLU Connecticut

Legislative Testimony
765 Asylum Avenue, First Floor
Hartford, CT 06105
860-523-9146
www.acluct.org

Written Testimony Supporting Sections 1, 2, and 6 of Senate Bill 4, An Act Concerning Data Privacy, Net Neutrality, Cyber Security and Fairness in Data Usage in the New Age of a Digital Workforce, with Concerns on Sections 10-13

Senator Needleman, Representative Arconti, Ranking Member Formica, Ranking Member Ferraro, and distinguished members of the Energy and Technology Committee:

My name is Kelly McConney Moore, and I am the interim senior policy counsel for the American Civil Liberties Union of Connecticut (ACLU-CT). I am submitting this testimony in support of Sections 1, 2, and 6 of Senate Bill 4, An Act Concerning Data Privacy, Net Neutrality, Cyber Security and Fairness in Data Usage in the New Age of a Digital Workforce, because it would establish net neutrality principles and set data privacy standards for internet service providers. Sections 10-13 of this bill, though, raise concerns. We recommend that these sections be removed from this bill and addressed separately, since they address real problems but also raise concerns about criminalizing protected speech. We take no position on Sections 3-5, 7, 8, 9, and 14 of this bill. We address some of the key provisions of this bill in turn below.

Net Neutrality (Section 1)

The ACLU-CT believes in defending free speech and protecting First Amendment rights. The free flow of information and the ability to communicate freely are key to America's democracy. The internet is central to how Connecticut residents and Americans everywhere express their opinions, share their knowledge, and learn from one another. It is also how many people learn about and debate important policies,

organize themselves around issues, and evaluate candidates for office. Equal access to information is imperative for everyone to participate in our democracy.

Network neutrality, very simply, is the idea that broadband internet service providers (ISPs), which provide internet access to 92% of Americans,[1] cannot (1) prioritize which websites or apps users access, (2) slow down – or "throttle" – traffic to websites or apps, or (3) entirely restrict access to websites or apps. Without net neutrality, broadband ISPs can determine which content we can see, how quickly we can access it, and if we have to pay extra for certain content.

Unfortunately, although net neutrality was formerly required of broadband ISPs,[2] the Federal Communications Commission (FCC) under the Trump administration repealed net neutrality.[3] In the absence of net neutrality protections, broadband ISPs have repeatedly throttled and prohibited access to content in periods when there were no net neutrality protections. For example, an ISP throttled the Santa Clara County Fire Department's service during recent California wildfires. The fire department's full speed was restored only after it purchased a new, more expensive plan.[4] In November 2018, Sprint was caught throttling Skype by pushing those video calls into the slow lane of the Internet.[5] Broadband ISPs have repeatedly prioritized certain content based on their financial interests, like when AT&T, Sprint, and Verizon all blocked access to Google Wallet because it competed with their proprietary wallet product.[6] Even more troublingly, broadband ISPs also have a history of blocking access to information based on message. For example, Verizon blocked text messages

---

[1] Federal Communications Commission, 2018 Broadband Deployment Report (Feb. 2, 2018), *available at* https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2018-broadband-deployment-report.
[2] *See* Klint Finley, "The WIRED Guide to Net Neutrality." Wired (May 9, 2018), *available at* https://www.wired.com/story/guide-net-neutrality/.
[3] *Id.*
[4] Colin Dwyer, "Verizon Throttle Firefighters' Data as Mendocino Wildfire Raged, Fire Chief Says." NPR (Aug. 22, 2018), *available at* https://www.npr.org/2018/08/22/640815074/verizon-throttled-firefighters-data-as-mendocino-wildfire-raged-fire-chief-says.
[5] Olga Kharif, "Sprint Is Throttling Microsoft's Skype Service, Study Finds." Bloomberg (Nov. 8, 2018), *available at* https://www.bloomberg.com/news/articles/2018-11-08/sprint-is-throttling-microsoft-s-skype-service-study-finds.
[6] Adi Robertson, "Here's how companies have flouted net neutrality before and what made them stop." The Verge (Jun. 11, 2018), *available at* https://www.theverge.com/2018/6/11/17438638/net-neutrality-violation-history-restoring-internet-freedom-order.

from NARAL, a reproductive rights advocacy organization, because the company determined the texts were "controversial."[7] Canadian Telecom company Telus blocked a union website because it was in a labor dispute with the union.[8] While it is likely that the FCC under President Biden will make different moves, the existing standards remain now. Moreover, the back-and-forth on net neutrality demonstrates that Connecticut should pass its own standards that are insulated from D.C. partisan politics.

State regulation of net neutrality is clearly permissible following a United States District Court for the District of Columbia decision invalidating the portion of the FCC's net neutrality repeal that prohibited state action in 2019.[9] Recent decisions by the federal executive branch dropping litigation against state net neutrality laws indicate that they agree.[10] In 2019, Maine implemented statewide net neutrality;[11] other states in New England are attempting to follow suit right now.[12] Passing net neutrality legislation in Connecticut would send a strong message that broadband ISPs in this state may not interfere with customers' free and equal access to information.

ISP Privacy Protections (Sections 2 & 6)

While ISPs claim that they have privacy policies in place to protect consumers, these same companies have a history of tracking all of our data and monetizing it. Just a few years ago, Verizon and AT&T tracked the internet activity of more than

---

[7] Adam Liptak, "Verizon Blocks Messages of Abortions Rights Group." New York Times (Sept. 27, 2007), *available at* https://www.nytimes.com/2007/09/27/us/27verizon.html.
[8] "Telus cuts subscriber access to pro-union website." CBC News (Jul. 24, 2005), *available at* https://www.cbc.ca/news/canada/telus-cuts-subscriber-access-to-pro-union-website-1.531166.
[9] *Mozilla Corp. v. Fed. Commc'ns Comm'n.*, 2019 WL 4777860 (D.C. Cir. Oct. 1, 2019), available at https://www.cadc.uscourts.gov/internet/opinions.nsf/FA43C305E2B9A35485258486004F6D0F/$file/18-1051-1808766.pdf.
[10] *See, e.g.*, Kimberly Adams, "To undo Trump's net neutrality policy, the Biden admin drops a lawsuit." Marketplace, Feb. 9, 2021, *available at* https://www.marketplace.org/2021/02/09/biden-administration-drops-trump-net-neutrality-lawsuit/.
[11] L.D. 1364, An Act Regarding Net Neutrality and Internet Policy (Maine 2019), *available at* http://legislature.maine.gov/LawMakerWeb/summary.asp?ID=280072688.
[12] *See* Heather Morton, "Net Neutrality 2019 Legislation." Nat'l Conf. of State Legislatures (Oct. 1, 2019), *available at* https://www.ncsl.org/research/telecommunications-and-information-technology/net-neutrality-2019-legislation.aspx.

100,000,000 customers with "supercookies" – small packets of data that allowed the companies to catalogue the website those people visited. Those supercookies could not be erased or evaded by using "incognito" modes for web browsers.[13] The data they collect is used to sell targeted advertising, ads that follow you after you have visited a particular website. All the while, the ISP profits. Information collected by ISPs and sold to the highest bidder can be used to swing elections, alter individual lives, manipulate public discourse, and even populate FBI databases.

People do not want to be monitored and monetized. A Pew Research Institute study found that 74% of respondents think being in control of who can get information about them online is very important, and that 90% of U.S. adults think it is important to control what information is collected about them.[14] Despite that, there are currently significant limitations to internet consumers' privacy.

Connecticut consumers are at the mercy of their ISPs' privacy policies, since no ISP is a clear leader in consumer privacy and since most consumers lack a meaningful selection between ISPs.[15] The market has failed to provide a solution to protecting internet privacy. Current federal law is similarly inadequate. In 2017, Congress overturned then-existing FCC consumer privacy regulations in such a way that bars the FCC from ever instituting substantially similar regulations.[16]

It is up to Connecticut, then, to protect consumers' privacy the state. The key privacy elements that we support in Senate Bill 4 include: (1) appropriately expansive definitions of customer personal information; (2) a ban on the sale or transfer of customer personal information absent express consumer permission; (3) a ban on targeted advertising based on the consumer's browsing history absent express

---

[13] Craig Timberg, "Verizon, AT&T Tracking Their Users with 'Supercookies.'" Washington Post (Nov. 3, 2014), *available at* https://www.washingtonpost.com/business/technology/verizon-atandt-tracking-their-users-with-super-cookies/2014/11/03/7bbbf382-6395-11e4-bb14-4cfea1e742d5_story.html?itid=lk_inline_manual_14.
[14] Pew Research Center's Privacy Panel Survey #4, Jan. 27, 2015-Feb. 16, 2015, *available at* https://www.pewresearch.org/internet/2015/05/20/americans-views-about-data-collection-and-security/.
[15] *See, e.g.*, Sascha Segan, "Exclusive: Check Out the Terrible State of US ISP Competition." PC Mag (Dec. 15, 2017), *available at* https://www.pcmag.com/news/exclusive-check-out-the-terrible-state-of-us-isp-competition.
[16] *See* Status of Internet Privacy Legislation by State, ACLU, *available at* https://www.aclu.org/issues/privacy-technology/internet-privacy/status-internet-privacy-legislation-state.

consumer permission; (4) a prohibition on ISPs discriminating against consumers who refuse to waive privacy protections; (5) a method for complaint, investigation, and penalties when an ISP violates privacy protections.

Unregulated, your ISP will know you better than you know yourself and will be able to sell that knowledge to other companies or the government, which will be able to use your data in ways you never intended. Indeed, as artificial intelligence systems become more intelligent and complex, enabling new forms of surveillance, tracking, and data analytics, the stakes for establishing commonsense internet consumer privacy could not be higher. If state legislatures fail to protect privacy, people in America will not be able to use the internet without subjecting themselves to increasingly dangerous levels of unregulated corporate and government surveillance. The provisions in this bill, though, will curb the worst abuses and hold ISPs to a minimum standard of stewardship with our data. Connecticut should take action to limit excessive collection and sale of our data while it still can.

Cyberstalking and Doxing (Sections 10-13)

We recognize that disclosing personal information about a person online (commonly known as "doxing") can be devastating, causing fear for personal safety and security. We also understand that this is often done to target people on the basis of religious, political, or other identities. Yet laws concerning this issue must be narrowly and carefully tailored to address the harm of doxing without chilling protected speech, which includes speech that is made without the purpose of harassment, intimidation, or inciting others to such actions. This can be achieved with legislation that criminalizes only wrongful actors who engage in doxing with the intent to harass or incite others to harassment.

Sections 10-13 of this bill, though, could also criminalize third parties who re-share the doxed information. Courts have consistently held that the First Amendment protects third parties from penalties for disseminating information, as long as they obtained the information without engaging in any illegal actions themselves. This bill

might violate this principle by making it a crime for third parties to share publicly available information.

While the intent of these sections of Senate Bill 4 is good – and becoming more necessary as doxing of people for their religious or political affiliations intensifies – as written it has the potential to chill protected speech and potentially criminalize valuable speech. We suggest the Committee remove Sections 10-13 of this bill and legislate them separately to ensure that they receive the attention due to such important and sensitive policy.

Conclusion

The ACLU of Connecticut strongly supports the net neutrality and consumer privacy protections included in Sections 1, 2, and 6 of Senate Bill 4, An Act Concerning Data Privacy, Net Neutrality, Cyber Security and Fairness in Data Usage in the New Age of a Digital Workforce. The cyberstalking and doxing provisions of Sections 10-13 raise concerns and we urge this Committee to remove them from Senate Bill 4 and give them the separate attention they deserve. With that change, we urge this Committee to support Senate Bill 4.