WASHINGTON
LEGISLATIVE OFFICE

March 27, 2017

RE: Vote NO on S.J. Res. 34, Providing for Congressional Disapproval of the Federal Communication Commission's Rule, "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services"

Dear Member,

On behalf of the American Civil Liberties Union (ACLU) please find the below vote recommendation urging you to vote "NO" on S.J. Res. 34, providing for Congressional disapproval of the Federal Communication Commission's (FCC) rule, "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services." We expect a vote on S.J. Res. 34, which passed the Senate by a thin margin of 50-48 last week, could occur as soon as tomorrow (Note: This resolution is identical to H.J. Res. 86, introduced in the House by Rep. Marsha Blackburn). The resolution, pursuant to the Congressional Review Act (CRA), would eliminate the FCC's broadband privacy rule in its entirety and prevent the FCC from making a rule that is "substantially the same" in the future.

The ACLU opposes efforts to roll back the FCC's rule[1], which requires broadband internet service providers to get customers' consent before sharing their sensitive data with third parties. Furthermore, we oppose using the CRA in this context, as it would eliminate privacy protections for consumers and could foreclose future efforts from the FCC to protect consumers' privacy.

We urge members of the House to vote "NO" on S.J. Res. 34, should it come up for a vote.

If you have any questions please contact Legislative Counsel, Neema Guliani, at nguliani@aclu.org or 202-675-2322.

Sincerely,

Faiz Shakir
Director

Neema Singh Guliani
Legislative Counsel

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

FAIZ SHAKIR
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

[1] *See* American Civil Liberties Union, Comment Letter on Proposed Rule on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (May 27, 2016), https://www.aclu.org/other/aclu-comments-federal-communications-commissions-rulemaking-protecting-privacy-customers; *see also* Access Humbolt et. al., Opposition to Petitions for Reconsideration, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (Mar. 6, 2017) https://www.aclu.org/sites/default/files/field_document/2017-03-07_coalition_opposition_fcc_pettitions_reconsideration_broadband_privacy_rule.pdf.

ACLU Vote Recommendation: Vote NO on S.J. Res. 34, Providing for Congressional Disapproval of the FCC's Rule, "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services"

The Federal Communication Commission (FCC) adopted a rule on October 27, 2016 to protect consumer privacy by requiring broadband internet access service (BIAS) providers (i.e. companies that provide broadband internet, such as Verizon, AT&T, and Comcast) to, among other things, (1) obtain opt-in consent before using or sharing sensitive information, such as web browsing history; and (2) adopt reasonable data security measures. The ACLU, along with other privacy, civil rights and consumer groups, support the rule and believe it is necessary to ensure that consumers' retain control over how their data is used by BIAS providers.[2]

S.J. Res 34 would not only undo this important rule, it would also prohibit substantially similar rules from being promulgated, undermining the ability of the government to address future privacy abuses or changing business practices. **We urge you to vote NO on S.J. Res. 34, should it come up for a vote.**

The FCC privacy rule rightly recognizes that consumers should have the choice to limit how their personal information is shared.

- The FCC rule requires BIAS providers to obtain opt-in consent from a customer before using, sharing or selling his or her sensitive information with most third parties.[3] Sensitive information includes browsing history, log-in and log-out times, IP address (which can indicate location), and app usage.
- The opt-in approach proposed in the rule is necessary to ensure that consumers' are appropriately informed and are able to control how their personal information is shared.
- This rule is particularly important given that BIAS providers have unique access to the private information of their customers, which can reveal information about their religion, political preferences, medical conditions, personal lives, or even finances.

The FCC rule prevents customers from having to choose between accessing the Internet and giving up their privacy.

- As a common-sense protection, the rule prohibits the practice of conditioning service, or certain kinds of service, on the waiver of privacy rights.[4]

---

[2] *See* Access Humbolt et. al, *supra* note 1; Letter from Consumer and Privacy Groups to Marlene Dortch Secretary, Fed. Comm. Commission, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (May 27, 2016) http://consumerfed.org/wp-content/uploads/2016/05/5-26-16-Broadband-Privacy_Letter.pdf; Ctr. for Dem. & Tech., Comment Letter on Proposed Rule on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (May 27, 2016), https://cdt.org/files/2016/05/Broadband-Privacy-Comment-FINAL-word.pdf; Electronic Priv. Info. Ctr., Comment Letter on Proposed Rule on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (May 27, 2016), https://epic.org/apa/comments/EPIC-FCC-Privacy-NPRM-2016.pdf.

[3] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274, 87,275 (Dec. 2, 2016) [Hereinafter, "Final Rule"]

[4] *Id.* at 87,316.

- With most consumers having few options for BIAS providers,[5] as a practical matter, they may be unable to simply choose a BIAS provider that better protects their privacy. This is especially true for those without financial means to find alternative service or those living in rural areas.

Using the CRA to eliminate the FCC rule would leave consumers without proactive privacy protections under the FCC or FTC.

- In 2016, the Ninth Circuit ruled that the FTC does not have authority to take actions against "common carriers" for "unfair or deceptive acts" pursuant to Section 5 of the FTC Act.[6] Under this ruling, the FTC would not have the jurisdiction over certain BIAS providers, including AT&T.
- Even if the FTC did have jurisdiction over BIAS providers, it is unable to promulgate rules to proactively prevent privacy abuses, and thus lacks the appropriate tools to protect consumers' privacy in this arena.
- Congress explicitly directed the FCC to protect consumer privacy under Section 222 of the Communications Act. Given that broadband internet providers are considered "common carriers," the FCC rightly exercised its authority under Section 222 to promulgate the privacy rule.

The CRA could foreclose future attempts to enact rules that are necessary to protect consumers' privacy and security online, raising unintended consequences in the future.

- If passed, the resolution would prevent the FCC from promulgating rules that are "substantially the same" absent additional legislation.[7]
- It is unclear how FCC Chairman Ajit Pai and how future Chairs of the FCC will interpret the CRA's prohibition on substantially similar rules; however, we are concerned that the FCC might claim that it is prevented from issuing rules in the future that remedy abuses, address new technologies, or respond to changing business practices. For example, the resolution could impact future attempts to create rules requiring data security protections given that the current rule contains provisions on this issue.[8]

The privacy framework created by the rule is similar to FTC's own privacy approach and reflects recent FTC rulings.

- The rule adopted by the FCC adopts the FTC's framework of designating sensitive information. However, the FCC's rule additionally explicitly recognizes the sensitive nature of browsing history, log-in and log-out times, IP address, and app usage.
- The FTC has recently recognized that additional types of information should be considered sensitive data. For example, in February, the FTC fined VIZIO for collecting

[5] Steve Lohr, *The Push for Net Neutrality Arose From Lack of Choice*, N.Y.TIMES Feb. 25, 2015, http://www.nytimes.com/2015/02/26/technology/limited-high-speed-internet-choices-underlie-net-neutrality-rules.html?_r=0.

[6] FTC v. AT&T Mobility LLC, 835 F.3d 993 (9th Cir. 2016) *available at* https://cdn.ca9.uscourts.gov/datastore/opinions/2016/08/29/15-16585.pdf.

[7] 5 U.S.C. § 801(b)(2).

[8] The portion of the rule requiring "reasonable" data security measures was stayed from going into effect on March 2, 2017 by Chairman Pai. F.C.C. Order Granting Stay in Part, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (Mar. 1, 2017), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0301/FCC-17-19A1.pdf.

viewing data—which is a close analogue to web browsing history—from their smart TVs without customer consent.[9] The court order in the case requires VIZIO to get opt-in consent before collecting the data in the future.

Using the CRA to overturn the FCC's privacy rules removes common-sense protections for consumers online and opens the door to potential unintended consequences in the future. **We urge you to vote "NO" on S.J. Res. 34, should it come up for a vote.** If you have any questions please contact Legislative Counsel, Neema Guliani, at nguliani@aclu.org or 202-675-2322.

[9] Press Release, F.T.C., VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it?utm_source=govdelivery.