March 18, 2015

The Honorable Michael C. Burgess & Jan Schakowsky
Chairman & Ranking Member
Subcommittee on Commerce, Manufacturing & Trade
Energy & Commerce Committee, House of Representatives
Washington, DC

RE: Data Security and Breach Notification Act of 2015

Dear Chairman Burgess and Ranking Member Schakowsky:

We are twelve organizations representing the public interest in the areas of privacy and consumer policy. We write to express our strong opposition to the draft Data Security and Breach Notification Act of 2015. As currently written, the bill severely undercuts communications data breach protections upon which millions of Americans rely, by superseding key parts of the Telecommunications Act of 1996 as implemented in rules promulgated by the Federal Communications Commission.

Communications record data is among the most private information we have "because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[1] A Pew survey from just five months ago found that 67% of Americans expected that telephone calls were somewhat or very secure.[2] And a breach of that security could cause emotional or even physical harm:

- Telephone records can reveal damaging and even potentially threatening information. Domestic violence victims who contact support hotlines would be in danger of abuse; political candidates' donors could be revealed; calls to suicide hotlines or emotional support centers would be discouraged.[3]
- Laws protecting our most confidential data, such as health and financial records, depend on communications security.[4] Without strong security for communications, that sensitive information could be left out to dry.
- Communications data underlies the mass surveillance programs that many have opposed and decried. Weakening protections on that data will only open the door to further abuse of that data for surveillance purposes.

For decades, the Communications Act has protected this sensitive information about communications network usage. Sections 201 and 222 of that Act ensure that providers implement strong protections for a wide range of data, termed "customer proprietary network information" or "CPNI."[5] The FCC uses both rulemakings and enforcement actions to keep those protections in step with modern technological developments.

---

[1] *Smith v. Maryland*, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting).
[2] Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* (2014), *available at* http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.
[3] *See* Timothy B. Lee, *Here's How Phone Metadata Can Reveal Your Affairs, Abortions and Other Secrets*, Wash. Post, Aug. 27, 2013.
[4] *See* 42 U.S.C. § 17932 (health care data); 15 U.S.C. § 6801 (financial records).
[5] 47 U.S.C. § 222(h)(1).

But section 6(c) of the proposed Data Security and Breach Notification Act of 2015 would replace many of those key protections with weaker standards:

- It would require companies to notify consumers of a data breach only if financial harm—not emotional or physical—were likely to occur as a result of the breach. As explained above, breach of communications data can result in numerous kinds of emotional or physical harms, harms avoided by the CPNI statutes and regulations[6] but not by the proposed bill.
- It allows numerous communications data breaches to go unnoticed and unremedied. While the FCC requires every breach that occurs to be reported,[7] the bill only requires notification to the Federal Trade Commission of data breaches where over 10,000 records were lost.[8] Thus, many smaller data breaches may be under-reported, under-investigated, and under-deterred.
- It eliminates the rulemaking authority that has allowed for the CPNI privacy protections to keep in step with the times. The FCC can implement new rules, such as its 2007 rules responding to "pretexting."[9] But the FTC, to whom data breach oversight would be transferred, has no such ability, and thus will be shackled to preventing data breaches of the future using the law of the past.

This excoriation of communications data breach protection could not come at a worse time, right on the heels of the FCC's historic open Internet order. Millions of Americans called for the FCC to reclassify broadband Internet as a telecommunications service under Title II of the Communications Act. The FCC listened and reclassified broadband to protect the open Internet.[10]

Following reclassification, Sections 201 and 222 of the Communications Act will now apply to broadband providers, vesting the FCC with strong authority to further protect consumers' information in the broadband sphere.[11] As the order explains, "consumers concerned about the privacy of their personal information will be more reluctant to use the Internet, stifling Internet service competition and growth."[12] As the phone networks transition to Internet-based systems, that Internet privacy becomes only more important, to ensure that the privacy expectations of those 67% of Americans are maintained. And so FCC Chairman Tom Wheeler stated that, in the wake of the reclassification order, consumer privacy will be a top issue for the Commission. "Privacy is not a secondary activity here," he said; "Privacy is an important issue to us."[13]

---

[6] *See* 47 C.F.R. §§ 64.2010–.2011.
[7] *See* 47 C.F.R. § 64.2009(e).
[8] *See* Data Security and Breach Notification Act of 2015, sec. 3(a)(3).
[9] *See* Implementation of the Telecommunications Act of 1996, 67 Fed. Reg. 59205 (Sept. 20, 2002).
[10] *See* Report & Order on Remand, Declaratory Ruling, and Order, FCC GN Docket No. 14-28 (Mar. 12, 2015), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf.
[11] *Id.* ¶ 462.
[12] *Id.* ¶ 54.
[13] Adam Sneed, *Privacy is the Star at "Tech Prom,"* Politico Morning Tech, Mar. 11, 2015, *available at* http://www.politico.com/morningtech/0315/morningtech17426.html.

To eliminate those data breach protections that consumers currently enjoy under the Communications Act, to take authority from a commission with decades of experience regulating use of personal information by communications providers, to cut back on the FCC's ability to protect consumers when the FCC has prominently expressed its commitment to protecting them—these would not merely be a mistake. These would be an affront to the American people's expectations for privacy and for their communications services.

We certainly look forward to an ongoing discussion with the Subcommittee and Congress on how to strongly protect consumer privacy and data security.[14] But a bill that cuts back on the privacy guaranteed by the Communications Act with no sufficiently corresponding benefit is not acceptable to us. We cannot support this bill, and encourage you and the Subcommittee to oppose it.

Sincerely,

Public Knowledge
Center for Media Justice
Common Cause
Consumer Federation of America
Media Action Grassroots Network
Consumer Action
Consumer Watchdog
Center for Digital Democracy
U.S. PIRG
Privacy Rights Clearinghouse
Future of Music Coalition
Free Press Action Fund

Cc: Members of the Subcommittee

[14] *Cf., e.g.*, Letter to Senate Commerce Committee on the Personal Data Notification and Protection Act (Feb. 4, 2015), *available at* http://www.consumerfed.org/pdfs/150205_Senate-Commerce_Letter_data-breach-hearing.pdf.