



March 15, 2020

Via: Electronic Mail

**RE: Vote “NO” on Cloture for H.R. 6172, the USA FREEDOM Reauthorization Act of 2020**

Dear Senator,

The Electronic Frontier Foundation (EFF) writes to oppose invoking cloture on H.R. 6172, the USA FREEDOM Reauthorization Act of 2020. This will allow the Senate to vote on the amendments. Refusing to invoke cloture is also the fastest way to move the bill off the Senate’s calendar so the Senate can consider other business, especially measures to deal with the novel coronavirus.

EFF is a member-supported, non-profit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 30,000 members. EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law to technology.

Congress has had over four years to consider provisions of the Patriot Act set to expire on March 15, 2020. Despite this, H.R. 6172 is being jammed through without any opportunity for amendments, without any committee markup, and with limited debate.

Over the last several years, it has become abundantly clear that many of our surveillance laws are broken. Since 2006, EFF has been in litigation to stop the government’s mass surveillance programs, including the bulk collection of billions of Americans’ domestic telephone call detail records (CDRs), showing who called whom and when).<sup>1</sup> In 2013, thanks to the Snowden revelations, Congress and the public were shocked to learn that the executive branch had relied on Section 215 to conduct this mass surveillance program.<sup>2</sup> After a federal appeals court ruled that the government’s interpretation of Section 215 was “unprecedented and unwarranted,” Congress passed the 2015 USA FREEDOM Act to amend Section 215 to stop mass surveillance of Americans’ telephone records. The law limited the government’s collection records of calls within “two hops” of a “specific selection term.”<sup>3</sup> It also included an expiration date on the authorities to force Congress to revisit these programs in 2019.

However, in 2018, the NSA announced that it received large numbers of CDRs it should not have had access to under USA FREEDOM, and that these “technical irregularities” began

---

<sup>1</sup> NSA Spying, EFF, <https://www.eff.org/nsa-spying>.

<sup>2</sup> Rainey Reitman, 3 Years Later, the Snowden Leaks Have Changed How the World Sees NSA Surveillance, EFF, <https://www.eff.org/deeplinks/2016/06/3-years-later-snowden-leaks-have-changed-how-world-sees-nsa-surveillance>.

<sup>3</sup> Julian Sanchez, USA Freedom: The Rubber Meets the Road, Just Security, <https://www.justsecurity.org/28830/usa-freedom-rubber-meets-road/>.

in 2015.<sup>45</sup> Despite this, the NSA encountered yet another “overcollection” incident just months later.<sup>6</sup> As a remedy, the NSA deleted every record it had collected since the technical irregularities began and announced that it had voluntarily stopped the CDR program entirely.

In the fall of 2019, both in response to these revelations and because the authority for the programs was expiring, both the House Committee on the Judiciary and the Senate Committee on the Judiciary called witnesses from the NSA, the FBI, and the DOJ to discuss Section 215.<sup>78</sup> The witnesses told both Committees they were requesting the renewal of the legal authorization for the CDR program - that they had voluntarily shut down - because it *might* be useful one day. Additionally, the witnesses confirmed that the 215 “business records” provision may allow the government to collect sensitive information, like medical records, location data, or even possibly footage from a Ring camera.<sup>9</sup> Both Committees appeared rightfully skeptical.

Even outside of the hearings, the DOJ, FBI and NSA have also been slow to respond to requests for information from concerned Representatives and Senators. Senator Wyden sent a letter to the Office of the Director of National Intelligence in July 2019 asking about the collection of sensitive geolocation information using Section 215 and only received a reply in November.<sup>1011</sup> Similarly, Senators Leahy and Lee sent a letter to the Office of the Director of National Intelligence and the Attorney General in July seeking more information about overcollection of CDRs and have yet to receive a response.<sup>12</sup> It’s clear that relying on the NSA to remedy its failures to stay within the law as passed by Congress is insufficient and that additional oversight and transparency measures are

---

<sup>4</sup> Spencer Ackerman, NSA Admits It Improperly Collected a Huge Amount of Americans’ Call Records, Daily Beast, <https://www.thedailybeast.com/nsa-admits-it-improperly-collected-a-huge-amount-of-americans-call-records>.

<sup>5</sup> NSA Reports Data Deletion, NSA, <https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/>.

<sup>6</sup> Ellen Nakashima, Repeated mistakes in phone record collection led NSA to shutter controversial program, The Washington Post, [https://www.washingtonpost.com/world/national-security/repeated-mistakes-in-phone-record-collection-led-nsa-to-shutter-controversial-program/2019/06/25/f256ba6c-93ca-11e9-b570-6416efdc0803\\_story.html](https://www.washingtonpost.com/world/national-security/repeated-mistakes-in-phone-record-collection-led-nsa-to-shutter-controversial-program/2019/06/25/f256ba6c-93ca-11e9-b570-6416efdc0803_story.html).

<sup>7</sup> India McKinney, The FISA Oversight Hearing Confirmed That Things Need to Change, EFF, <https://www.eff.org/deeplinks/2019/09/fisa-oversight-hearing-confirmed-things-need-change>.

<sup>8</sup> Reauthorizing the USA FREEDOM Act of 2015, United States Senate Committee of the Judiciary, <https://www.judiciary.senate.gov/meetings/reauthorizing-the-usa-freedom-act-of-2015>.

<sup>9</sup> Matthew Guariglia, Amazon’s Ring is a Perfect Storm of Privacy Threats, EFF, <https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats>.

<sup>10</sup> Senator Ron Wyden, Letter to Office of the Director of National Intelligence, United State Senate, <https://www.wyden.senate.gov/imo/media/doc/070319%20Wyden%20Letter%20to%20ODNI%20RE%20Phone%20Location%20Tracking.pdf>.

<sup>11</sup> Letter in response to Senator Ron Wyden’s Letter, Office of the Director of National Intelligence, <https://www.wyden.senate.gov/imo/media/doc/111419%20ODNI%20Reponse%20to%20Wyden%20RE%20Phone%20Location%20Tracking.pdf>.

<sup>12</sup> Senators Patrick Leahy and Mike Lee, Letter to Director of National Intelligence and United States Attorney General, United States Senate, [https://www.leahy.senate.gov/imo/media/doc/Leahy\\_and\\_Lee-Letter\\_re\\_NSA\\_implementation\\_of\\_the\\_USA\\_FREEDOM\\_Act.pdf](https://www.leahy.senate.gov/imo/media/doc/Leahy_and_Lee-Letter_re_NSA_implementation_of_the_USA_FREEDOM_Act.pdf).

desperately needed. EFF and other civil liberties advocates were hopeful Congress would take this well-timed opportunity to enact real reform and necessary transparency.<sup>13</sup>

Despite this record, disappointingly, the reforms contained in H.R. 6172 are minimal – in many cases merely representing a codification of the status quo. In addition, the bill contains provisions that would be a step back from the current our flawed statute, such as adding a new criminal penalty.

The current bill contains several concerning provisions and omits key reforms. For example:

- **The bill fails to require that individuals receive appropriate notice and access to information when FISA information is used against them.** The government asserts that it has no obligation to provide notice to individuals whose records are collected under Section 215, even if those records are then introduced into evidence against those individuals in court. While the bill contains a provision requiring notice when information “obtained or derived” from Section 215 is used against targets of collection, this provision is utterly inadequate. The bill wrongly allows the government to continue to evade its notice obligations merely by unilaterally asserting that notice would harm national security. This is a step backward from current law that sets a dangerous precedent. Nor does the bill define “derived,” despite concerns that the government has narrowly interpreted this term in the past to avoid providing notice. It limits the notice provision to only cover a small subset of individuals, if any. And it fails to ensure that individuals or their counsel are able to access FISA applications and orders so that they may fully and fairly defend themselves.
- **The bill fails to fully address deficiencies with the FISA court that have led to illegal surveillance.** Pursuant to the USA FREEDOM Act, the FISA court has the discretion to appoint an amicus in “novel and significant” cases. H.R. 6172 expands this provision to also permit appointment in cases where there are “exceptional” First Amendment concerns. However, the bill fails to create a presumption that an amicus be appointed in other cases involving the targeting of US persons or raising constitutional concerns; does not guarantee amici have access to sufficient information to allow them to intervene in cases where there are concerns; and fails to ensure that amici are not denied access to necessary materials. We are particularly disappointed that the sponsors rejected meaningful amicus improvements proposed by prominent members on both sides of the aisle.
- **The bill fails to appropriately limit the types of information that can be collected under Section 215 of the Patriot Act.** Under Section 215, the government is permitted to obtain literally “any tangible thing.”<sup>14</sup> Though the government has not disclosed a complete list of the types of items it obtains under Section 215, this collection can include phone records, tax returns, medical and other

---

<sup>13</sup> Letter to United States House of Representatives Committee on the Judiciary, ACLU, [https://www.aclu.org/sites/default/files/field\\_document/2019-03-18\\_section\\_215\\_coalition\\_transparency\\_letter.pdf](https://www.aclu.org/sites/default/files/field_document/2019-03-18_section_215_coalition_transparency_letter.pdf).

<sup>14</sup> See 50 USC § 1861.

health information, gun records, book sales and library records, and a host of other sensitive information.<sup>15</sup> This bill prohibits the FBI from using Section 215 for the collection of cell site and GPS information – which the government has already said is current practice following the Supreme Court’s *Carpenter* decision.<sup>16</sup> However, the bill fails to clearly prohibit the government from collecting other types of sensitive records, including web browsing and search history, despite thoughtful proposals from members of both parties to exclude these and other types of sensitive information.

- **The bill fails to appropriately raise the standard for collecting information under Section 215.** Section 215 of the Patriot Act lowered the standard for collecting business records to mere “relevance.” This standard is so opaque and broad, the FISA court ruled that the NSA could rely on it to collect Americans’ telephone records in bulk. The bill fails to include provisions that would heighten this standard and limit large-scale collection under this authority.
- **The bill fails to appropriately limit the retention of information collected under Section 215.** Based on the public minimization procedures for other FISA authorities—including Section 702 and CDR collection activities—it is safe to assume that the government retains Section 215 data for a *minimum* of 5 years, regardless of whether anyone has determined that the data includes foreign intelligence information. H.R. 6172 puts in place a 5-year retention limit – however this limitation is riddled with loopholes and exceptions.

Thus, we urge members to vote against invoking cloture. The Senate should be allowed to consider amendments and to include real reforms to this bill. Absent real reforms, Section 215 and the other provisions should be allowed to expire.

Sincerely,

**Lee Tien**  
Senior Staff Attorney  
[lee@eff.org](mailto:lee@eff.org)  
Electronic Frontier Foundation

**India McKinney**  
Director of Federal Affairs  
[india@eff.org](mailto:india@eff.org)  
Electronic Frontier Foundation

---

<sup>15</sup> See 50 USC § 1861(a).

<sup>16</sup> Chief Justice Roberts, *Carpenter v. United States*, Supreme Court of the United States, [https://www.supremecourt.gov/opinions/17pdf/16-402\\_h315.pdf](https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf).