February 25, 2020

The Honorable Jerrold Nadler
Chairman
Committee on the Judiciary
U.S. House of Representatives
2138 Rayburn House Office Building
Washington, DC 20515

The Honorable Doug Collins
Ranking Member
Committee on the Judiciary
U.S. House of Representatives
2142 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Nadler and Ranking Member Collins:

We write this letter in relation to the markup of H.R. ___, the "*USA FREEDOM Reauthorization Act of 2020.*" **While H.R. ___ has positive elements, it is far from sufficient to fully address the FISA abuses that have come to light over the past two years. Thus, we urge the committee to adopt amendments to strengthen the bill.**

H.R. ___ has several positive provisions: it ends Section 215's call detail record authority; expands the role of the Foreign Intelligence Surveillance Court amici; makes clear that the USA Freedom Act required the government to declassify novel and significant opinions issued prior to 2015; and strengthens FBI reporting requirements. However, the bill also has several glaring omissions. H.R. ___ does not heighten the standard to collect information under 215 in order to end "bulky" collection; sufficiently limit the types of records that can be obtained under Section 215; require the destruction of information that does not constitute foreign intelligence; ensure that individuals subject to FISA surveillance are provided appropriate notice or disclosure; protect against First Amendment violations; or clearly prohibit discrimination.

To address these concerns, we urge the committee to adopt the following changes to the bill:

1. **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, the FISA Court ruled that the NSA could rely on it to collect Americans' telephone records in bulk. Although Congress sought to prohibit bulk collection when it passed the *USA Freedom Act* in 2015, it did so by requiring requests for collection to be tied to a "specific selection term" or "SST," and it left the definition of SST open-ended. This raised concerns that "SST" could be interpreted broadly enough to allow collection on entire companies, organizations, IP addresses, etc., resulting in "bulky" collection—i.e., collection of large amounts of information about presumptively innocent Americans.

These concerns have been borne out by official statistics indicating that the number of people whose information is collected under Section 215 is orders of magnitude greater than the number of actual targets. For example, in 2018, with just 60 targets for Section 215 orders, the government collected information relating to 214,860 unique accounts. The only way to end this "bulky" collection is to identify more specifically who is a legitimate target of collection under the law.

Thus, the bill should be amended to include the language contained in Section 105 of H.R. 5675, the *Safeguarding Americans' Private Records Act of 2020*, limiting the permissible targets of Section 215 collection to foreign powers, agents of foreign powers (defined to include suspected terrorists), and people in contact with or known to foreign powers or agents of foreign powers.

2. Clearly limit the types of records that can be obtained under Section 215.

Under Section 215, the government is permitted to obtain literally "any tangible thing."[1] 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 health information, gun records, book sales and library records, and a host of other sensitive information.[2]

Section 102 attempts to limit the types of records that can be obtained under Section 215 by stating that authority cannot be used to obtain information "if the compelled production of such thing would require a warrant for law enforcement purposes." While a step forward from existing law, this language is insufficient for two reasons.

One, the government has not fully disclosed how it is interpreting the Supreme Court's decision in *Carpenter v. United States*,[3] which held that the government had to obtain a warrant to collect cell site location information from providers. Following *Carpenter*, the NSA has stated that it does not obtain GPS and cell site location information under Section 215, but has not disclosed whether it believes it can collect similarly detailed location information from other sources (for example, from wifi hotspots) or whether it believes *Carpenter* forecloses other types of collection that implicate similarly sensitive personal data.

Two, it is not clear how the FISA court will interpret this language in cases where lower courts have ruled that a warrant is required for certain types of information, but there is no binding Supreme Court precedent. For example, following the Sixth Circuit's *Warshak*[4] decision in 2010, most major providers began requiring a warrant for content information, like emails. Despite this, it is unclear whether the government tool the official legal position that a warrant was required for all content information, given that the opinion had not yet been affirmed by the

[1] *See* 50 U.S.C. § 1861.
[2] *See* 50 U.S.C. § 1861(a).
[3] *Carpenter v. United States*., 138 S. Ct. 2206, 2218 (2018).
[4] *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

Supreme Court. Given that the FISC is not bound by other circuits, there is a risk that it will diverge from instructive Court of Appeals decisions.

To address this, the bill should amend Section 215 to clearly foreclose the government from obtaining sensitive information that federal courts have already ruled requires a warrant. 50 U.S.C. 1861 should be amended to add at the end the following: "The term 'tangible things' does not include content information, web browsing history, web search history, cell site location information, GPS information, location information of an individual or device, educational records, biometric information, book sales/library records, or medical records." In addition, Section 102 should be amended to read "if the compelled production of such thing would require a warrant for law enforcement purposes *in any federal court."*

3. **Require purging of information collected under Section 215 and related FISA authorities after 3 years.**

Congress has required the government to "minimize" the retention of information about U.S. persons collected under Section 215. However, there is no "minimization" requirement for other FISA authorities that can be used to collect similar types of information, including the FISA pen register/trap-and-trace (PR/TT) authority or National Security Letters (NSLs). Moreover, the government has not disclosed any of the minimization procedures it applies to traditional Section 215 collection.

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. During this lengthy period of time, highly personal information sits in massive databases where it is subject to theft, hacking, negligent mishandling, or abuse.

The bill should be amended to include the language contained in Section 107 of H.R. 5675, the *Safeguarding Americans' Private Records Act of 2020*, which requires purging of information within 3 years unless it is determined to be foreign intelligence or evidence of a crime. It should also extend this 3-year retention limit to information acquired under the FISA PR/TT authority and NSLs.

4. **Ensure that individuals receive appropriate notice and disclosure when information obtained from FISA 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. Section 103 of the bill makes clear that the government must provide notice when information "obtained or derived from" Section 215 is used against someone in a proceeding. While a positive step forward, this language is insufficient for two reasons. One, it fails to define "derived from," leaving room for the government to circumvent its notice obligation by narrowly defining this language and/or by engaging in "parallel construction" (essentially laundering the evidence by re-obtaining it through different means). The government has used these methods in the past to avoid its notice obligations under Section 702 of FISA, and

there is every reason for concern that it would do so under the new Section 215 notice requirement. Two, the bill fails to ensure that individuals or their counsel are able to access FISA applications and orders, so that they may fully defend themselves in cases where FISA information is used against them.

To address this, the bill should adopt the language in Section 203(a) of H.R. 5675, the *Safeguarding Americans' Private Records Act of 2020,* that clearly defines "derived from," and should make clear that individuals are entitled to obtain access to underlying FISA applications and orders under such protective orders as the court may impose.

5. Strengthening the First Amendment protections.

Section 215 and other Patriot Act authorities prohibit surveillance based "solely" on First Amendment-protected activities.[5] This language oddly does not restrain the government from engaging in surveillance based "in part" on First Amendment-protected activities. In addition, neither Section 215 nor other provisions of FISA prohibit the government from targeting individuals based on race, religion, ethnicity, or other protected-class status.

To address this, we urge the committee to amend 50 U.S.C. 1861(a)(1) to add "or in part" following "solely." In addition, we urge the committee to amend 50 U.S.C. 1861(a) to add: (4) An investigation of a United States person under this section shall not be based solely or in part on race, ethnicity, national origin, religion, gender, gender identity, or sexual orientation, except when there is credible factual information that links the individual person with a particular characteristic described in this paragraph to an identified international terrorism or clandestine intelligence activity"; and to amend 50 U.S.C. 1861(k)(4)(i) to add: "(III) is not based solely or in part on race, ethnicity, national origin, religion, gender, gender identity, or sexual orientation, except when there is credible factual information that links the individual person with a particular characteristic described in this paragraph to an identified international terrorism or clandestine intelligence activity."

6. Further expand the role of the FISA court amici.

Pursuant to the *USA Freedom Act*, the FISA court has the discretion to appoint an amicus in cases presenting a "novel or significant interpretation of the law." Section 202 expands this to also permit appointment in cases raising First Amendment concerns. While this is a positive change, we urge the committee to also expand amici participation in cases that involve new surveillance technologies or novel applications of existing technologies.

Accordingly, we recommend amending Section 202, amending 50 U.S.C. 1803(i)(2)(A) to add at the end, "(iii) in any case involving new technologies or novel applications of existing technologies."

[5] *See* 50 U.S.C. § 861(a).

If you have questions, feel free to contact Neema Singh Guliani, Senior Legislative Counsel at the ACLU, at nguliani@aclu.org, or Elizabeth Goitein, Co-Director of the Liberty and National Security Program at the Brennan Center for Justice, at elizabeth.goitein@nyu.edu.

Sincerely,

American Civil Liberties Union
Brennan Center for Justice at NYU School of Law

cc: Members of the U.S. House Committee on the Judiciary