May 12, 2020

RE: Vote Recommendation on Amendments to H.R. 6172

Dear Senator,

As soon as this week, the Senate is expected to consider at least five amendments to H.R. 6172, the USA FREEDOM Reauthorization Act of 2020. This is the first time Congress has had the opportunity to consider any amendments to H.R. 6172. There has been no markup of this legislation in either chamber, nor did the House permit members to introduce amendments prior to passage. The prior cloture motion for this bill was withdrawn on March 16, 2020, following opposition from members of both parties who pressed for the opportunity to improve the bill. **Absent improvements, the ACLU urges you to vote "NO" on H.R. 6172.**

The ACLU urges you to vote "YES" on the following amendments:

- **An amendment led by Senators Lee (R-UT) and Leahy (D-VT)**, which would enhance the role of the Foreign Intelligence Surveillance Court amici;
- **An amendment led by Senators Wyden (D-OR) and Daines (R-MT)**, which would ensure that internet search and browsing history is not collected under Section 215 of the Patriot Act; and
- **An amendment led by Senator Paul (R-KY)**, which prohibits the use of FISA, as well as surveillance conducted under claimed Article II power, against people in the United States or in proceedings against them.

It is anticipated that Senator McConnell will introduce side-by-side amendments to the Wyden/Daines and Lee/Leahy led amendments. The proposed side-by-side amendments would gut the original amendments and may be worse than the status quo in places. Thus, we urge you to reject these side-by-side amendments as alternatives to the Lee/Leahy and Wyden/Daines amendments.

The ACLU will be scoring these votes.

<u>The ACLU opposes H.R. 6172 in its current form because it fails to address the litany of surveillance abuses that have come to light.</u>

Over the last several years, it has become abundantly clear that many of our surveillance laws are broken. Despite reforms in 2015, the NSA and FBI continue to rely on the Patriot Act to engage in large-scale collection of Americans' information. For example, in 2018, the

AMERICAN CIVIL LIBERTIES UNION

National Political Advocacy Department
915 15th St. NW, 6th FL
Washington, D.C. 20005
aclu.org

Susan Herman
President

Anthony Romero
Executive Director

Ronald Newman
National Political Director

government used Section 215 of the Patriot Act's traditional business authority to surveil 60 targets, yet swept in the communications information of over 214,000 individuals.[1] Disturbingly, the government has refused to reveal the full range of information it believes it can collect under Section 215.

Recent disclosures also demonstrate that the Foreign Intelligence Surveillance Court (FISC) is not equipped to protect Americans' rights. For example, an Inspector General report released last year revealed that there were a litany of errors and omissions in the government's applications to surveil Trump campaign advisor Carter Page. Despite these problems, the court approved both an initial surveillance application and three subsequent renewals.[2] During a House hearing, FBI Director Christopher Wray agreed that at least a portion of the surveillance of Carter Page was illegal. And, the FISC itself accepted the Justice Department's position that at least two of the surveillance applications for spying on Page were invalid, and the court took extraordinary steps to order the government to try to remedy its wrongdoing and avoid a repeat. Despite the secrecy around FISA proceedings, the Page episode offers a window into the abuses that predictably follow from giving the government extraordinary powers with minimal checks and no meaningful due process.

Unfortunately, a subsequent audit released by the Department of Justice Inspector General, following the House passage of H.R. 6172, demonstrates that the Page incident was not an isolated incident. An audit released on March 31, 2020 examined 25 FISA applications and found "apparent errors or inadequately supported facts" in *every single case file examined.* The same report identified 4 additional cases where the associated Woods files, which are intended to help ensure the accuracy of FISA applications, could not be found at all.[3]

Despite this, H.R. 6172 lacks key reforms to prevent similar abuses. Specifically, the bill fails to require that individuals receive appropriate notice and access to information when FISA information is used against them; appropriately limit the types of information that can be collected under Section 215 of the Patriot Act; raise the standard for collecting information under Section 215; or limit the retention of information collected under Section 215. Our attached vote recommendation on the cloture motion filed in early March details these deficiencies in more detail.

The ACLU urges you to Vote "Yes" on the Lee/Leahy amendment to strengthen oversight of the FISA courts.

---

[1] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES, at 26 (April 2019), https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf.

[2] OFFICE OF THE INSPECTOR GENERAL, U.S.DEP'T OF JUSTICE, REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (December 2019), https://www.justice.gov/storage/120919-examination.pdf.

[3] OFFICE OF THE INSPECTOR GENERAL, U.S.DEP'T OF JUSTICE, MANAGEMENT ADVISORY MEMORANDUM FOR THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION REGARDING THE EXECUTION OF WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS, at 3 (March 2020), https://oig.justice.gov/reports/2020/a20047.pdf.

The Page incident and subsequent IG audits highlight existing deficiencies within FISA. The secretive, one-sided nature of FISA proceedings before the FISC allowed the errors within the Page application to accumulate and continue largely unchallenged. Pursuant to the *USA FREEDOM Act of 2015*, the FISC has the discretion to appoint an amicus in cases involving "novel and significant" interpretations of the law – which was not triggered in the Page case. A provision in H.R. 6172 expands the 2015 provision to also permit appointment in cases where there are "exceptional" First Amendment concerns. But that reform, standing alone, would fall far short and is likely to cover only a small fraction of circumstances that raise civil liberties concerns.

The Lee/Leahy amendment would strengthen H.R. 6172 in key ways. One, it encourages the appointment of amici — with expertise in privacy and civil liberties expertise — in a large number of cases, including those raising significant First Amendment concerns; involving the targeting of sensitive individuals, including domestic news media, religious organizations, and political candidates; relating to new surveillance programs or uses of technology; or other cases involving novel or significant civil liberties or privacy issues. Two, the amendment makes clear that the government must turn over exculpatory information— information that may suggest the proposed surveillance is not justified—to the FISC. Three, the amendment helps to ensure that the amici are granted access to information critical in to provide meaningful expertise to the court. Four, the amendment requires the FISC to approve accuracy procedures designed to ensure FISA court applications are complete and truthful, and requires Inspector General reporting on omissions, errors, and unsubstantiated facts identified in FISA applications.

At the same time, the amendment does not interfere with the efficiency and independence of the FISC. Ultimately, the court can decline to appoint an amicus at its discretion with a written finding. In addition, the amendment does not prevent the government from using existing emergency authorities that bypass preapproval by the FISC in certain cases. Moreover, the expanded amicus provision is unlikely to overburden the court. For example, according to the most recent ODNI report, there were only 232[4] Title I FISA applications targeting US persons, representing 12.2% of total Title I cases. The amendment's additional categories for when there is a presumption of an amicus appointment would largely only apply to a subset of these cases; and, any other additional appointment of amici is restricted to a minimal number of cases involving new programs, technologies, or novel or significant civil liberties issues.

The McConnell side-by-side amendment effectively guts the Leahy/Lee amendment and should be rejected as an alternative. The anticipated side-by-side amendment would expand the amicus provision in the base bill to only applications that target political campaigns and where the underlying criminal predicate in a FISA cases is a violation of the Foreign Agents Registration Act (FARA). Thus, it provides greater protection to political candidates, while rejecting these very same protections for religious groups, domestic news media, individuals facing significant or novel civil liberties deprivations, or cases involving

[4] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES, at 9 (April 2019), https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf.

new surveillance programs or uses of technology. The amendment also bars use of any information in a FISA application that comes from a political campaign – even if the source of such information is disclosed, there is additional corroborating evidence, or it is exculpatory – preventing the FISC from considering information that could be helpful in making its determination. Finally, the bill would have public reporting on errors in omissions in applications from the Attorney General, instead of the independent Inspector General.

The ACLU urges you to Vote "Yes" on the Wyden/Daines amendment to prevent warrantless collection of internet search history and browsing history under Section 215 of the Patriot Act.

The Wyden/Daines amendment would prohibit Section 215 of the Patriot Act, one of the authorities extended by H.R. 6172, from being used to collect internet search and browsing history. The amendment would not prevent the government from gathering this information; rather, it would simply require the government to rely on other FISA authorities that require a probable cause showing. This amendment is sorely needed for several reasons.

One, internet search and browsing history is extremely revealing in nature and the Fourth Amendment requires a warrant to obtain this information. As the Supreme Court in *Riley* noted, "An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns — perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD."[5] Thus, similar to cell site location information which the Supreme Court ruled in *Carpenter* requires a warrant under the Fourth Amendment, this information provides an "intimate window" into an individual's life. For example, the fact that someone visited christianmingle.com, teapartypatriots.org, or ashleymadison.com may reveal information about their religion, political views, relationship status, or behavior. Consistent with this analysis, courts have ruled that some types of search history require a warrant and many providers generally require a warrant for this information.[6]

Two, the government's history of abusing Section 215 and the secrecy surrounding the authority underscore the need for clear, bright-line rules about what can and cannot be collected. The government has stated that Section 215 generally does not allow collection of the types of information that would require a warrant in the criminal context[7] — yet it has refused to reveal what information it collects under Section 215 or how it is applying relevant Supreme court precedent. Thus, the government has provided no clarity regarding whether it believes it can collect internet search and browsing history under Section 215. This is particularly concerning given the government's history of adopting incorrect legal interpretations of Section 215. For example, under Section 215, the government can collect information under a standard far more permissive than a probable cause warrant – it must merely show that information is relevant to an international counterterrorism or

[5] *Riley v. California*, 573 U.S. 373, 395-96 (2014)
[6] In re Google, 806 F.3d 125 (3rd Cir. 2015)
[7] *Reauthorizing the USA FREEDOM Act of 2015 Before the S. Comm. on the Judiciary*, 116th Cong. (2019).

counterintelligence investigation.[8] In the past, this has been wrongly interpreted by the government to collect the call records of virtually every American on an ongoing basis.

Three, H.R. 6172's existing language fails to make fully clear that Section 215 cannot be used to collect this information. The existing language in H.R. 6172 prohibits Section 215 from being used to collect information where a warrant is required in the criminal context *if* an individual also has a reasonable expectation of privacy. The government historically has taken the position that individuals do not have a reasonable expectation of privacy in information held by third parties. Thus, it is likely the government would argue that internet search and browsing history does not fall under this prohibition.

McConnell's side-by-side amendments fails to fully prohibit warrantless collection of internet and search history and is in fact worse than the base bill. The side-by-side amendment would only prevent the collection of internet search history and browsing history to the extent such information is deemed to be content information under the Electronic Communications Privacy Act (ECPA). The amendment specifically contemplates continued collection of certain kinds of sensitive internet search and browsing history, with higher administrative approval and additional public reporting. This language will likely be used by the government to affirmatively argue that Congress has granted the authority to collect other types of sensitive internet search and browsing history without demonstrating probable cause – notwithstanding *Riley*, *Carpenter*, and other case law that supports the notion that such information should receive full Fourth Amendment protection regardless of whether it is deemed content. The fact that such determinations will be made in secret further encourages problematic interpretations that are inconsistent with the Fourth Amendment. Given this, we urge you to reject this amendment.

The ACLU urges you to Vote "Yes" on the Paul Amendment, to provide greater protection for U.S. persons.

The one-sided, secretive, and expansive nature of the FISA process is inconsistent with the Constitution. Unlike ordinary criminal wiretaps, where the government must establish probable cause that the wiretap will yield evidence of a particular crime, FISA surveillance is based on a relaxed set of standards, allowing the government to conduct surveillance with fewer restraints. Moreover, in recent years, the government has relied on FISA to deploy an array of novel and intrusive surveillance techniques—implicating the privacy rights of countless Americans who have never been suspected of any crime. In most cases, there is no entity within the FISC charged with challenging government claims, or raising potential civil liberties concerns. Targets of FISA surveillance are almost never notified, even after surveillance has been concluded, insulating the FBI from scrutiny in cases where surveillance is unwarranted or otherwise raises constitutional concerns. And, the vast majority of surveillance applications and orders are never declassified, which dramatically limits even after-the-fact scrutiny.

[8] 50 USC 1861

Even in cases in which individuals are criminally prosecuted with the aid of FISA surveillance, the government has used secrecy to thwart any meaningful scrutiny. Defense attorneys have been unable to challenge the accuracy or completeness of the government's surveillance applications because they have never been granted access to underlying FISA court applications and orders. Since FISA was enacted in 1978, the government has successfully opposed disclosure of FISA applications, orders, and related materials in every single criminal case in which a defendant has sought to challenge the surveillance used against him. As a result, important questions about the constitutionality of novel forms of FISA surveillance have not been subject to adversarial process, in violation of defendants' right to a meaningful opportunity to seek suppression. Moreover, individuals are unable to challenge potential government errors and omissions, which may be analogous to the errors and omissions in the Page applications.[9]

The Paul amendment addresses many of the fundamental deficiencies with FISA by preventing this surveillance from being used against Americans. The amendment would require the government to get a warrant in an ordinary federal court in cases where it seeks to surveil a U.S. person. In addition, the amendment prevents the government from using any information collected warrantlessly under executive branch authorities or collected under FISA from being used against U.S. persons in civil, administrative, or criminal proceedings.

We urge you to vote "Yes" on the Leahy/Lee, Wyden/Daines, and Paul amendments, and to reject the McConnell side-by-side amendments as alternatives. Absent improvements, the ACLU urges you to oppose H.R. 6172.

If you have questions, feel free to contact Senior Legislative Counsel, Neema Singh Guliani at nguliani@aclu.org.

Sincerely,

Ronald Newman
National Political Director

Neema Singh Guliani
Senior Legislative Counsel

[9] See In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F.Supp.2d 611, 620 (FISC 2002) (describing 75 FISA applications containing misstatements and omissions of material facts).