1. Ensure that the government cannot access Americans' most sensitive private information without a warrant and express statutory authority

1.1 Close the Section 702 backdoor search loophole.
1.2 Close the EO 12333 backdoor search loophole.
1.3 Prohibit the government from purchasing data to evade warrant requirements and statutory privacy protections.
1.4 Bring the law in line with technology.
1.5 Strengthen Section 702's prohibition on reverse targeting.
1.6 Expressly prohibit the acquisition of purely domestic communications under Section 702 and EO 12333.
1.7 Prohibit warrantless scanning of content.

2. Rein in overbroad scope of surveillance

2.1 Prohibit bulk collection of sensitive information.
2.2 Narrow the permissible pool of foreign targets.
2.3 Prohibit "abouts" collection.
2.4 Strengthen minimization requirements.
2.5 Narrow collection under authorities that only require "relevance."
2.6 Limit use of FISA Section 702 for domestic law enforcement.

3. Ensure that judicial review is available and effective when Americans are subject to surveillance

3.1 Enact measures that will enhance the FISA Court's ability to serve as a check on surveillance.
3.2 Ensure that criminal defendants receive notice of foreign intelligence surveillance.
3.3 Fix standing problem.
3.4 Gag order fix.
3.5 Restore judicial review in civil litigation.
3.6 Establish judicial oversight over certain EO 12333 activities.
3.7 Bolster the FISA Court's role in reviewing targeting decisions.

4. Increase transparency and accountability for surveillance activities

4.1 Reforms to the classification system.
4.2 OLC opinion disclosures.
4.3. Timely and effective disclosure of FISA Court opinions.
4.4 Require ODNI publish an estimate of US person information acquired pursuant to Section 702 and EO 12333.
4.5 Prohibit the government from requiring or incentivizing encryption backdoors.
4.6 Strengthen transparency reporting, Congressional and public oversight, and accountability measures.

1. Ensure that the government cannot access Americans' most sensitive private information without a warrant and express statutory authority

1.1 Close the Section 702 backdoor search loophole. Communications are collected without a warrant under Section 702 based on the government's certification that it is targeting *only* foreigners overseas. Yet the FBI routinely conducts searches of Section 702-acquired data to find information about *Americans*, including their communications (which are "incidentally" acquired in massive amounts). Agencies should be required to obtain a warrant or FISA Title I order before conducting such searches to stop the use of Section 702 as an end-run around the Fourth Amendment.

1.2 Close the EO 12333 backdoor search loophole. Collection under Executive Order 12333 (which includes overseas collection activities, as well as certain domestic collection of non-contents information) frequently results in the "incidental" acquisition of Americans' communications and other Fourth Amendment-protected data, like geolocation information. Agencies perform backdoor searches of such data, thus evading the Fourth Amendment's warrant requirement. As with Section 702, the government should have to obtain a warrant or FISA Title I order before performing such searches.

1.3 Prohibit the government from purchasing data to evade warrant requirements and statutory privacy protections. The government has argued that even in cases where a warrant would be required to compel the production of information, it can avoid that requirement by simply purchasing the data. Congress should put an end to this circumvention of the Constitution by prohibiting law enforcement and intelligence agencies from purchasing data they would otherwise need a warrant, court order, or subpoena to obtain. (The Fourth Amendment Is Not For Sale Act would go a long way toward that end.)

1.4 Bring the law in line with technology. Due to changes in how data is produced, stored, and analyzed, certain data that can be "crunched" to reveal extremely sensitive details of our personal lives — such as geolocation data, communications metadata, Internet search and web browsing records, biometric information, and health data — are routinely held by third parties and therefore lack Fourth Amendment protection. With its 2018 decision in *Carpenter v. United States* (ruling that police need a warrant to obtain geolocation data held by a cell phone company), the Supreme Court began the long, slow process of updating the law. Congress should step in and accelerate the process by requiring the government to get a warrant in order to obtain these highly sensitive types of records.

1.5 Strengthen Section 702's prohibition on reverse targeting. Currently, Section 702 requires the government to certify that "the" purpose of collection is not to target particular, known Americans. This weak prohibition still allows the government to conduct warrantless surveillance even where spying on Americans is the government's *primary* purpose. Collection under Section 702 should be prohibited if "a" purpose is to target Americans.

1.6 Expressly prohibit the acquisition of purely domestic communications under Section 702 and EO 12333. Section 702 and EO 12333 are warrantless surveillance authorities, and as such, they

should never be used to collect communications between or among Americans. Congress should clearly specify that such collection is prohibited.

1.7 Prohibit warrantless scanning of content. When the government conducts surveillance of communications in transit over the Internet backbone, it temporarily seizes and scans the content of all communications flowing past the point of interception in order to locate the communications of targets. This is similar to a general warrant in which police search all the homes in a city to see which of them contain incriminating evidence. Although the scanning is done without manual review, a police search of every home in a city would not be acceptable simply because the search was performed by robots. Congress should specify that any scanning must be limited to the communications metadata in order to minimize the unnecessary intrusion on Fourth Amendment rights.

2. Rein in overbroad scope of surveillance

2.1 Prohibit bulk collection of sensitive information. Under various surveillance authorities (including even administrative subpoena authorities), the government has engaged in "bulk collection" — the indiscriminate collection of data without any specific targets. As a general matter, most of the people whose data is obtained through "bulk collection" are entirely innocent and unrelated to any investigation. Moreover, under EO 12333, bulk collection can result in the acquisition of purely domestic communications, and does result in the collection of unquantified but massive amounts of information about Americans. Congress should prohibit the bulk collection of communications or other sensitive data under any authority, with at most an exception for areas experiencing active hostilities during wartime.

2.2 Narrow the permissible pool of foreign targets. Under Section 702 and EO 12333, the government can conduct surveillance of almost any foreigner abroad, subject only to (1) an exceptionally broad definition of "foreign intelligence" in FISA, and (2) a list of legitimate objectives set forth in EO 14086, which the next president could revoke and which the current president may amend in secret (as expressly provided in the order). Allowing surveillance of foreigners who pose no threat to the U.S. jeopardizes the privacy of the Americans with whom they communicate. It also threatens U.S. business interests: Overbroad U.S. surveillance authorities have led European courts to strike down data-transfer agreements between EU and U.S. companies. This reform will require some combination of the following approaches:

1. Require intelligence analysts to have reasonable suspicion to believe that the target of surveillance is a foreign power or agent of a foreign power, as broadly defined in FISA (but excluding civil society NGOs)
2. Remove the overbroad catch-all provisions from FISA's definition of "foreign intelligence" (i.e., remove 50 U.S.C. 1801(e)(2))
3. Codify legitimate purposes similar to those set forth in EO 14086, and require the government to have a reasonable belief, based on specific and articulable facts, that surveillance of each target is likely to provide information that is directly relevant to one or more of the objectives

2.3 Prohibit "abouts" collection. Under Section 702, the government for years collected not only communications *to* and *from* the targets of surveillance, but also communications *about* those

targets. This practice swept in many conversations among innocent people who did not meet the criteria for targeting, as well as purely domestic communications. After pushback from the FISA Court, the government stopped this practice under Section 702's Upstream program (which directly taps into and scans internet backbone traffic) in 2017, but under current law the government is free to restart it as long as it gives Congress 30 days' notice. Meanwhile, some experts are concerned that a similar practice may be occurring "downstream," where most Section 702 surveillance occurs. Downstream "abouts" collection would be alarming because it would mean the government is still warrantlessly acquiring communications that merely mention a target, rather than only communications to or from a target. "Abouts" collection is unnecessary and intrusive, and Congress should prohibit it.

2.4 Strengthen minimization requirements. Under both Section 702 and EO 12333, the government is currently allowed to retain "incidentally" collected U.S. person information for up to 5 years, and there are several exceptions that allow much longer retention periods. These long and flexible periods cannot be squared with the statutory and constitutional mandate to "minimize" the retention of Americans' information. Congress should shorten the time period to three years and eliminate the multiple exceptions. Retention beyond this limit should be permitted only for information that has actually been reviewed by an individual who makes a written determination that the information constitutes foreign intelligence or evidence of a crime. In addition, Congress should mandate protections for information subject to attorney-client privilege.

2.5 Narrow collection under authorities that only require "relevance." The USA Freedom Act sought to prohibit bulk collection under a range of FISA authorities that are available on a low "relevant to" an investigation standard, including Section 215, pen register/trap-and-trace orders, and national security letters. Prior to the USA Freedom Act, the government and the FISA Court had interpreted this "relevance" standard to permit the NSA's bulk collection of Americans' phone records under Section 215. The USA Freedom Act attempted to address this problem by requiring collection to be based on "specific selection terms" (SSTs) defined separately for each authority. The government's statistical reports, however, suggest that large numbers of people other than the actual targets are continuing to be swept up under these provisions, raising the specter of "bulky" collection. Congress should tighten the definitions for SSTs, removing potentially broad terms like "entity," which could encompass at least hundreds or thousands of people. Alternatively, it should replace the "relevance" standard, and permit collection only where the government has reasonable grounds to believe that the subject of the information to be collected is a foreign power or agent of a foreign power. This would also reinforce reform 2.1.

2.6 Limit use of FISA Section 702 for domestic law enforcement. Current law permits Section 702 — ostensibly a foreign intelligence authority — to broadly be used for routine domestic law enforcement. The law permits use of Section 702-acquired information in assessments and investigations concerning *any* crime. Although current law imposes some limitations on the use of this information in criminal court proceedings, those limitations are vague, elastic, and give the Attorney General broad authority to set parameters for how the rules apply. Information acquired under Section 702 should only be used in assessments, investigations, and criminal proceedings involving a narrow set of serious offenses that are specifically enumerated, and this

limit should apply to *all* stages of investigation and prosecution, not just use in criminal court proceedings.

3. Ensure that judicial review is available and effective when Americans are subject to surveillance

3.1 Enact measures that will enhance the FISA Court's ability to serve as a check on surveillance. In 2020, the Senate approved an amendment offered by Senators Leahy and Lee by a vote of 77-19. The amendment included several provisions that would bolster the role of FISA Court amici, giving them better access to information and expanding the categories of cases in which they should presumptively be involved — namely cases involving sensitive targets like domestic media, religious groups, and political groups. It also included provisions to ensure that the materials the government presents to the FISA Court are accurate and include any exculpatory information. This amendment should be enacted into law as part of FISA without being watered down, given its overwhelming bipartisan support.

- flowchart available

3.2 Ensure that criminal defendants receive notice of foreign intelligence surveillance. Congress required the government to provide notice to criminal defendants when using notice "obtained or derived from" FISA surveillance. The government has frequently avoided this obligation by engaging in "parallel construction," i.e., reconstructing an evidentiary trail using information it wouldn't have obtained but for FISA in an effort to avoid disclosing more controversial surveillance practices. Not only does this practice deprive defendants of their right to challenge the surveillance used against them, but it also deprives the public at large of the government accountability that results from courts considering the legality of novel or controversial surveillance. Congress should close off this loophole by clarifying that evidence "derived from" FISA includes evidence that would not have been obtained "but for" the FISA collection.

3.3 Fix standing problem. The Supreme Court has made it nearly impossible for plaintiffs to challenge unlawful surveillance if they lack proof that they have been surveilled — something few plaintiffs would ever have. Congress should provide that individuals and organizations have a right to sue if they regularly communicate foreign intelligence information with foreigners abroad and have taken objectively reasonable measures to avoid surveillance, or if they have demonstrated a concrete injury arising from a good-faith belief that their rights have been, are being, or imminently will be violated through surveillance.

3.4 Gag order fix. One reason challenges to surveillance are rare is because the law makes it far too easy for the government to silence service providers who have been required to turn over their customers' communications or other records to the government. Bills like Sen. Wyden's Government Surveillance Transparency Act or Rep. Nadler's NDO Fairness Act would strike a much better balance between providing notice to people who have been surveilled and safeguarding the integrity of investigations. Congress should include such legislation as part of reauthorization.

3.5 Restore judicial review in civil litigation. Even if plaintiffs can show standing, the Supreme Court recently held that FISA's provisions for handling national security

information in surveillance cases — provisions that require the court to issue a ruling on the lawfulness of the surveillance — are not meant to displace the "state secrets privilege," which the government routinely uses to shut down lawsuits entirely. If this decision is allowed to stand, civil challenges to unlawful foreign intelligence surveillance will be effectively taken off the table. Congress should clarify that FISA's provisions for handling national security information are the exclusive means for addressing national security information in electronic surveillance cases.

3.6 Establish judicial oversight over certain EO 12333 activities. No program that involves the collection of Americans' communications and other constitutionally protected information should occur without any judicial oversight. At a minimum, the government should be required to provide notice to criminal defendants when using evidence obtained or derived from EO 12333 surveillance so the defendant may bring a challenge.

3.7 Bolster the FISA Court's role in reviewing targeting decisions. Currently, the FISA Court reviews and approves targeting procedures and the broad purposes for which a person or entity may be targeted, but it does not review targeting decisions — which means the government could be violating the procedures and the Court wouldn't know it unless the government chose to self-report. Congress should require the FISA Court to audit a random sample of targeting decisions to determine whether the government is adhering to the targeting procedures and the frequency of any non-compliance.

4. Increase transparency and accountability for surveillance activities

4.1 Reforms to the classification system. It is increasingly clear that legislative reforms will not be effective if the surveillance system remains in a black box, inaccessible to lawmakers and judges as well as the public. Moreover, the presence of classified documents in the homes of former President Trump, President Biden, and former Vice President Pence have led to calls for classification reform, and there is broad bipartisan support in Congress for such an undertaking.

4.2 OLC opinion disclosures. Like overclassification, it is increasingly clear that secret legal opinions issued by the Office of Legal Counsel within the DOJ can eviscerate even explicit Congressional intent, especially in relation to surveillance authorities, like the faulty opinions used to enable the illegal mass surveillance programs known as StellarWind (one of which was the precursor to Section 702). Reliable oversight of surveillance would include a requirement that legal conclusions considered binding on the executive branch be declassified, if necessary, and published as required by the SUNLIGHT Act.

4.3. Timely and effective disclosure of FISA Court opinions. The USA FREEDOM Act required that the government publish any novel or significant FISA Court opinions, a measure designed to prevent secret law. Unfortunately, the government has delayed the publication of some important rulings by a year or more. The law should be amended to require timely disclosure of FISA Court opinions within 60 days of their being issued. The amici should also have the ability to petition for rulings to be designated as significant.

4.4 Require ODNI to publish an estimate of US person information acquired pursuant to Section 702 and EO 12333. For Congress and the public to fully understand the privacy impact of foreign intelligence surveillance, agencies must release at least an estimate of how much information about and communications of Americans they are acquiring under relevant authorities. The government previously committed to providing this estimate for Section 702.

4.5 Prohibit the government from requiring or incentivizing encryption backdoors. Historically, this prohibition was linked to the "backdoor search fix" as offered in the House as an appropriations amendment, which passed the House in 2014 and 2015. Many members are on the record supporting this fix and it may also be attractive to companies. Prohibiting requirements or incentives for backdoors would also serve to increase confidence in US technology.

4.6 Strengthen transparency reporting, Congressional and public oversight, and accountability measures. This involves strengthening existing transparency, oversight, and accountability provisions, and adding certain additional requirements. Importantly, however, reforms to ensure better oversight of surveillance should not come at the expense of reforms that would actually rein in surveillance.

- Transparency:
    - Allow private actors to provide more granular transparency around directives, national security letters, targets, and estimated USP communications and metadata ("incidentally" or otherwise) acquired
    - Expand reporting requirements
    - Codify reporting requirements concerning the number of US person queries the FBI conducts
    - Implement false-positive testing, for instance by requiring the FISA Court or other auditor to sample acquired information (under both Section 702 and EO 12333) and estimate the proportion of acquired information that is not later determined to constitute foreign intelligence information (i.e. drawing from scientific methodological best practices around disclosing error rates)
    - Require PCLOB to examine and publicly report on the degree to which FISA disproportionately targets and impacts various marginalized groups, such as racial, ethnic, and religious minorities, as well as political dissidents and immigrants, including by auditing discrete, randomized samples of intelligence agency targeting and querying decisions, and disclosing how that information is used and the false positive error rates for these practices
- Enhance Congressional and public oversight:
    - Require ODNI to publish descriptions of the subject matter for each Section 702 certification and report the number of persons targeted under each
    - Strengthen PCLOB by allowing it to review foreign intelligence and cyber activities (currently its jurisdiction is limited to "terrorism") and permitting whistleblower complaints to PCLOB
    - Allow members of Congress to hear from Intelligence Community whistleblowers
    - House-specific: TS/SCI clearances for personal offices
- Accountability:
    - Enhance penalties for wrongful targeting and wrongful use of information acquired under FISA

- Require that statutorily compelled "technical assistance" for surveillance be necessary, narrowly tailored, and not overly burdensome, and require FISA Court approval
- Require and preserve documentation of FISA Court proceedings and communications between the government and the FISA Court

ENDORSING ORGANIZATIONS:

Advocacy For Principled Action In Government
American Civil Liberties Union
Americans for Prosperity
Asian Americans Advancing Justice | AAJC
Brennan Center for Justice at NYU School of Law
Center for Democracy & Technology
Center for Security, Race and Rights
CommonDefense.us
Constitutional Alliance
Defending Rights & Dissent
Demand Progress
Due Process Institute
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Fight for the Future
Free Press Action
Freedom of the Press Foundation
FreedomWorks
Government Information Watch
Libertas Institute
Media Alliance
National Association of Criminal Defense Lawyers
Oakland Privacy
Organization for Identity & Cultural Development
PEN America
People For the American Way
Project for Privacy and Surveillance Accountability (PPSA)
Project On Government Oversight
Public Citizen
Restore The Fourth
Secure Justice
Surveillance Technology Oversight Project
Wikimedia Foundation
X-Lab