companies, under section 215, in a targeted fashion. These kinds of records are routinely obtained by prosecutors in criminal investigations, though the use of grand jury subpoenas. It makes no sense for the government to be able to collect these records to investigate bank fraud, insider trading and public corruption, but not to help keep the country safe from terrorists.

While we must reauthorize these authorities, however, it is equally important that we reform them. But we don't yet have a reform bill that I am satisfied with.

The American people have made clear that they want the government to stop indiscriminately collecting their telephone metadata in bulk under section 215. They also want more transparency from the government and from the private sector about how section 215 and other national security authorities are being used. They want real reform.

I want to be clear that I emphatically agree with these goals. They can be achieved responsibly, and doing so will restore an important measure of trust in our intelligence community.

I agree with these reforms because the civil liberties implications of the collection of this type of bulk telephone metadata are concerning. This is especially so, given the scope and nature of the metadata collected through this program.

Now, there haven't been any cases of this metadata being intentionally abused for political or other ends. That is good. I recognize that the overwhelming majority of those who work in the intelligence community are law-abiding American heroes to whom we owe a great debt for helping to keep us safe.

But other national security authorities have been abused. Unfortunately, to paraphrase James Madison, all men aren't angels. I've been critical, for example, of the Department of Justice's handling of the so-called LOVEINT cases uncovered by the NSA's Inspector General.

Given human nature, then, the mere potential for abuse makes the status quo concerning the bulk collection of telephone metadata under section 215 unsustainable, especially when measured against the real yet modest intelligence value the program has provided.

The USA FREEDOM Act would in some ways reauthorize and reform section 215 along these lines. It would end the bulk collection of telephone metadata in 6 months, and transition the program to a system where the phone companies hold the data for targeted searching by the government.

But the bill's serious flaws cause me to believe that we can do better. Let me discuss just a few.

First, while the system to which the bill would transition the program sounds promising, it does not exist at present, and may well not exist in 6 months. Intelligence community leaders don't know for sure how long it will take to build. They don't know for sure how fast it will be able to return search results to the government. They don't know for sure whether the phone companies will voluntarily keep the metadata for later searching by the government.

On this score, then, this bill feels like a leap into the dark when we can least afford it. While we need certainty that the bulk collection of telephone metadata under section 215 will end, we also need more certainty that the new system proposed will work and be effective.

Second, the bill contains reforms to the FISA Court that are unneeded and risky. I am strongly in favor of reforming the court to make clear that it can appoint a traditional amicus, or a friend of the court, to help it get the law right. This is a well understood legal concept.

But this bill goes further—potentially dangerously so. Under certain circumstances, the bill directs the FISA Court to name a panel of outside experts who would, in the words of the New York Times, ''challenge the government's pleadings'' before the court.

Especially when the bill already ends the kind of dragnet intelligence collection under section 215 that affects so many innocent Americans, this is wholly unnecessary. And for this reason, the Administrative Office of the U.S. Courts sent a letter alerting Congress to its concerns that this outside advocate could ''impede the court's work'' by delaying the process and chilling the government's candor.

In addition, this proposed advocate is contrary to our legal traditions, in which judges routinely make similar decisions on an ex parte basis, hearing only from the government. Mobsters don't get a public defender when the government seeks to wiretap their phones. Crooked bankers don't get a public defender when the government seeks a search warrant for their offices. There is no need to give ISIS a public defender when the government seeks to spy on its terrorists to keep the country safe.

Third, the bill also contains language that amends the federal criminal code to implement a series of important and widely-supported treaties aimed at preventing nuclear terrorism and proliferation. However, the bill doesn't authorize the death penalty for nuclear terrorists. Nor does it permit the government to request authorization from a judge to wiretap the telephones of these terrorists or allow those who provide them material support to be prosecuted. These common-sense provisions were requested by both the Bush and Obama Administrations, but for unknown reasons they were omitted from the bill.

In fact, Senator WHITEHOUSE and I have introduced separate legislation, the Nuclear Terrorism Conventions Implementation and Safety of Maritime Navigation Act of 2015, which would implement these treaties with these provisions included.

Recently, I have been heartened that there is a bipartisan group of members of the Judiciary and Intelligence Committees who share these and other concerns. We have been discussing an alternative reform bill that would also end the bulk collection of telephone metadata under section 215. But it would also do a better job of ensuring that our national security is still protected.

So I support a short, temporary reauthorization with the hope that an alternative reform bill can be crafted that addresses the core reform goals of the American people and that appropriately balances national security with the privacy and civil liberties of all Americans. There is work ahead, but it is important that we get this reform right.

USA FREEDOM ACT

Mrs. FEINSTEIN. Mr. President, I rise today to discuss the votes the Senate will soon take relating to three expiring provisions in the Foreign Intelligence Surveillance Act.

I will vote to support the USA FREEDOM Act, the bill passed by the House last week by a vote of 338 to 88, and strongly urge my colleagues to do the same. In my view, this is the only action that we can take right now that will prevent important intelligence authorities from expiring at the end of next week.

Let me describe the situation in a little more detail.

On Monday morning at 12:01 a.m. on June 1, three separate sections of the Foreign Intelligence Surveillance Act, or FISA, will expire. Two of those provisions were first added to FISA in 2001 in the USA PATRIOT Act, shortly after the terrorist attacks of September 11. They are the business records section, also known as section 215, and the roving wiretap provision.

The business records provision was originally intended to allow the government to go to the FISA Court to get an order to be able to obtain a variety of records relevant to an investigation. The authority was, and remains, very important for the FBI.

Since 2006, the business records authority in FISA has also been used by the NSA to get telephone metadata records from telephone companies—the records of the telephone numbers and the time and duration of a call. Metadata does not include the content or the location or names of the individuals on the phone.

The roving wiretap provision allows the government to use surveillance authorities under FISA, pursuant to a court order, against an individual who seeks to evade surveillance by switching communication devices. If a terrorist gets a new cell phone or changes an email address, the government can continue surveillance on that individual under the same probable cause

warrant from the FISA court rather than having to go back to the Court for authority to collect information from each new phone number or email address.

The third provision, the so-called ''lone wolf'' provision, was added in 2004 over concern that the intelligence community may not be able to gather information on a known terrorist if it could not demonstrate his membership in a specific terrorist group. Given the threat we face today from individuals inspired by ISIL, for example, that threat is even more real today than it was a decade ago.

These provisions have been reviewed by the Intelligence and the Judiciary Committees for many years and have been subject to enormous public scrutiny.

For more than a year, there has been a strong desire by the American public, supported by the President and by the House of Representatives, to make a basic change in the use of the business records authority. That change is to end the bulk collection of phone records by the NSA and to replace it with a system for the government to get a FISA Court order to be able to obtain a much more specific set of records from the telecommunications providers when there is a ''reasonable, articulable suspicion'' that a phone number is associated with a foreign terrorist group.

The Director of National Intelligence and the Attorney General have written to the Senate to indicate their support for this change, which they state ''preserves essential operational capabilities of the telephone metadata program and enhances other intelligence capabilities needed to protect our nation and its partners.''

I would also note that the USA FREEDOM Act will allow private companies that receive requests and orders from the government to produce information, at their own discretion, that allows them to be more transparent about those requests and orders from the government. I support this additional transparency and thank the sponsors of the USA FREEDOM legislation for including it.

I have spoken to a number of technology companies, including several founded and based in California, that believe that transparency is not only good policy but that it will help them show publicly that their products and services are secure and independent from government control.

So the choice before the Senate today is a clear one: whether to vote for the only sure way to continue the use of important intelligence authorities in a way that has the support of the American people, the President, the intelligence community, and the Department of Justice or to hope that the authorities will be renewed for 2 months despite clear communications from the House that it will not support such an extension.

FBI Director Comey said earlier this week that the expiration of the business records and roving wiretap authorities would be a ''huge problem,'' and I believe him.

Given the wide range of threats facing Americans, both at home and abroad—particularly from ISIL and Al Qaeda—we should not allow these valuable authorities to expire.

To me, this is an easy choice, and I will support the USA FREEDOM Act.

Mr. BROWN. Mr. President, I ask unanimous consent to engage in a colloquy with Senator CORNYN and Senator LEAHY, ranking member of the Judiciary Committee, regarding important aspects of S. 337, the FOIA Improvement Act of 2015, that could affect the essential work of our financial regulators.

The PRESIDING OFFICER. Without objection, it is so ordered.

FOIA IMPROVEMENT ACT OF 2015

Mr. BROWN. I recognize the principles of this legislation, which seeks to increase government transparency, but as the ranking member of the Senate Banking Committee, I also recognize the need for regulatory agencies to thoroughly fulfill their oversight and supervisory responsibilities over our Nation's financial institutions and the health and welfare of our financial system. The financial regulatory agencies are responsible for ensuring the safety and soundness of the financial system, compliance with Federal consumer financial law, and promoting fair, orderly, and efficient financial markets. Effective regulation requires that financial regulators have full access to information from regulated entities, and regulated entities should be confident that regulators will be able to protect an entity's confidential information from disclosure. Congress provided for this important exchange of information in the Freedom of Information Act, FOIA, by protecting supervisory information specifically in 5 U.S.C. §552(b)(8), commonly referred to as exemption 8, and more generally in other exemptions. Accordingly, I appreciate that S. 337 does not intend to limit the scope of the protections under exemption 8, or other exemptions relevant to financial regulators; nor does the bill intend to require release of confidential information about individuals, or information that a financial institution may have, the release of which could compromise the stability of the financial institution or the financial system, or undermine regulators' consumer protection efforts. Because the release of confidential or sensitive information relating to the supervision of regulated entities could cause harm to such entities, their customers, or the financial system, a financial regulatory agency could reasonably foresee that disclosure of such information requested under FOIA may harm an interest protected by exemption 8. This is precisely why Congress continues to provide these statutory exemptions.

Mr. LEAHY. I thank Senator BROWN for his interest and support for this legislation. I agree that the safety and soundness of our financial system and financial institutions depends on our financial regulators' ability to perform effective oversight and supervision of financial institutions. I also agree that the free flow of information between regulators and financial institutions is important to this process. Exemption 8 was intended by Congress, and has been interpreted by the courts, to be very broadly construed to ensure the security of financial institutions and to safeguard the relationship between financial institutions and their supervising agencies. The proposed amendments to FOIA are not intended to undermine the broad protection in exemption 8 or to undermine the integrity of the supervisory examination process. In addition, I note that some information that the government may withhold under exemption 8 is also protected under exemption 4, which exempts from disclosure commercial and financial information that is privileged or confidential. Exemption 4 covers information prohibited from disclosure under the Trade Secrets Act and similar laws, and as such does not provide for discretionary disclosure under FOIA. As with other exemptions that are based on separate legal restrictions, it is understood that the foreseeable harm standard will not apply to most of the information falling under exemption 4. I will continue to work with the banking committee and financial regulatory agencies to clarify the scope of the bill as we move forward in the legislative process and address any remaining concerns.

Mr. CORNYN. I, too, thank Senator BROWN for his remarks and for his interest and support for this legislation. I agree with Senator LEAHY that the important goals of this bill are not intended to impede regulatory agencies' oversight and supervisory responsibilities, nor are they meant to hinder communication between financial regulators and the institutions that they regulate. I agree that it is important to ensure that our financial regulators are able to do the work required to maintain the safety and soundness of our financial system. I will also work with the chair and ranking member of the banking committee and the financial regulatory agencies to address any remaining concerns on this issue as we advance this very important piece of legislation.

Mr. BROWN. I thank Senator CORNYN and Senator LEAHY for their work on this important legislation and for working with me to clarify the scope of this bill. I hope Senator CORNYN and Senator LEAHY continue to work on these issues with the financial regulatory agencies, including if the bill is considered in any conference with the House of Representatives, to ensure that this new standard will not undermine the broad protections currently afforded to confidential supervisory information and in turn undermine the