

Casey	Heller	Paul
Cassidy	Hirono	Perdue
Coats	Hoeven	Peters
Cochran	Inhofe	Portman
Collins	Isakson	Reed
Coons	Johnson	Reid
Corker	Kaine	Risch
Cornyn	King	Roberts
Cotton	Klobuchar	Rounds
Crapo	Lankford	Sasse
Daines	Leahy	Schatz
Donnelly	Lee	Schumer
Durbin	Manchin	Scott
Enzi	Markey	Sessions
Ernst	McCain	Shaheen
Feinstein	McCaskill	Shelby
Fischer	McConnell	Stabenow
Flake	Menendez	Tester
Franken	Merkley	Tillis
Gardner	Mikulski	Toomey
Gillibrand	Moran	Udall
Grassley	Murkowski	Warner
Hatch	Murphy	Warren
Heinrich	Murray	Whitehouse
Heitkamp	Nelson	Wicker

## NOT VOTING—10

Booker	Rubio	Vitter
Cruz	Sanders	Wyden
Graham	Sullivan	
Kirk	Thune	

The concurrent resolution (S. Con. Res. 16) was agreed to, as follows:

## S. CON. RES. 16

*Resolved by the Senate (the House of Representatives concurring),*

## SECTION 1. STATEMENT OF POLICY ON RELEASE OF UNITED STATES CITIZENS IN IRAN.

(a) FINDINGS.—Congress makes the following findings:

(1) Saeed Abedini of Idaho is a Christian pastor unjustly detained in Iran since 2012 and sentenced to eight years in prison on charges related to his religious beliefs.

(2) Amir Hekmati of Michigan is a former United States Marine unjustly detained in 2011 while visiting his Iranian relatives and sentenced to 10 years in prison for espionage.

(3) Jason Rezaian of California is a Washington Post journalist credentialed by the Government of Iran. He was unjustly detained in 2014 and has been held without a trial.

(4) Robert Levinson of Florida is a former Federal Bureau of Investigations (FBI) official who disappeared in 2007 in Iran. He is the longest held United States citizen in United States history.

(b) STATEMENT OF POLICY.—It is the policy of the United States that—

(1) the Government of the Islamic Republic of Iran should immediately release Saeed Abedini, Amir Hekmati, and Jason Rezaian, and cooperate with the United States Government to locate and return Robert Levinson; and

(2) the United States Government should undertake every effort using every diplomatic tool at its disposal to secure their immediate release.

## MORNING BUSINESS

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the Senate be in a period of morning business, with Senators permitted to speak therein for up to 10 minutes each.

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

## USA FREEDOM ACT

Mr. LEAHY. Mr. President, section 215 of the USA PATRIOT Act expires in a matter of weeks. Senator LEE and I have a bipartisan bill, the USA FREE-

DOM Act, that would end the use of section 215 to authorize the bulk collection of Americans' phone records and replace it with a more targeted program. It also would enact other important reforms to bring more accountability and transparency to government surveillance. The Speaker of the House of Representatives is bringing that same bill for a vote in the House on Wednesday.

Last week, some opponents came to the floor to voice their opposition. They claimed that ending this bulk collection program would somehow put our national security at risk and that a bulk collection program like this could somehow have prevented the September 11 attacks. But the facts are not on their side. According to the headline of a recent National Journal story, these opponents of reform have made "dubious claims in defense of NSA surveillance."

I agree these claims are dubious, and I want to set the record straight. I ask unanimous consent that the National Journal story dated May 8, 2015, and an analysis by the Center for Democracy and Technology of similar claims be printed in the RECORD.

One Senator stated on the Senate floor last week, "If this program had existed before 9/11, it is quite possible we would have known that 9/11 hijacker Khalid Al Mihdhar was living in San Diego and was making phone calls to an Al Qaeda safe house in Yemen."

Another seemed to suggest that the bulk collection program would "have prevented 9/11."

When I was chairman in the last Congress, the Senate Judiciary Committee held six hearings to examine revelations about government surveillance activities. At one of those hearings, I asked former counterterrorism official Richard Clarke, who was working in the Bush administration on September 11, whether the NSA bulk collection program would have prevented those attacks. He testified that the government had the information it needed to prevent the attacks but failed to properly share that information among Federal agencies.

Senator Bob Graham, who investigated the September 11th attacks as head of the Senate Intelligence Committee, likewise has said that "there were plenty of opportunities without having to rely on this metadata system for the FBI and intelligence agencies to have located Mihdhar."

The other claim that has been made repeatedly over the past few days is that, as one Senator put it, the bulk collection of Americans' phone records is "very effective at keeping America safe." Another stated that the USA FREEDOM Act would "eliminate the essential intelligence this program collects."

But numerous national security experts also have concluded that the NSA's bulk collection program is not essential to national security. The President's Review Group on Intel-

ligence and Communications Technology, which included two former national security officials, stated:

The information contributed to terrorist investigations by the use of section 215 telephony metadata was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders.

Former Acting CIA Director Michael Morell testified to the Senate Judiciary Committee that the review group's recommendation to end the government's collection of that data and instead allow the government to search phone records held by the telecommunications providers would not add a substantial burden to the government. That is precisely the approach of our bipartisan USA FREEDOM Act.

Last year, the Director of National Intelligence and the Attorney General supported a prior version of the USA FREEDOM Act, which also ended bulk collection under section 215 and replaced it with a more targeted phone records program. The Attorney General and the Director of National Intelligence said that our bill "preserve[d] essential Intelligence Community capabilities."

These individuals are not newcomers to the issue of national security. They understand the threats to our Nation. They do not have a political motive. They have the best interests of our Nation and its values in mind when they tell us that we can end the dragnet collection of innocent Americans' phone records and keep our country safe.

The USA FREEDOM Act does not just end NSA's bulk collection program under section 215. It also fills other gaps in our intelligence capabilities. It ensures that the government can quickly obtain business records—including phone records—in emergency situations. It ensures that if a foreign terrorist who poses a serious threat comes into the United States, the government does not have to stop its surveillance while it seeks emergency wiretap authorization from the Attorney General. It ensures that the government need not terminate FISA surveillance on a foreigner who temporarily travels outside the United States. And it ensures that the FBI has the tools it needs to investigate individuals who are facilitating the international proliferation of weapons of mass destruction on behalf of a foreign government or terrorist organization. These provisions were requested by the FBI and by the House Permanent Select Committee on Intelligence. They were not part of the bill that was filibustered in the Senate in November.

As a final matter, it is notable that there has been not a single Senate committee hearing on surveillance reform or the expiring provisions in the 5 months of this new Congress under Republican leadership. There has been zero committee consideration on the bill that Senator MCCONNELL has now brought directly to the Senate calendar that would simply extend these

expiring provisions. I recall the promises that under new leadership the committees would work through regular order, but that has not occurred even though it was apparent to all last year that we would need to grapple with long-overdue reforms. This lack of leadership or any committee process is also despite the fact that the leader and chairmen of the relevant committees would not even let us debate the USA FREEDOM Act last year, in part because it had not gone through committee. As the process moves forward this year, we should not be hearing complaints about lack of process from those who did not provide it.

There is no question that the USA FREEDOM Act contains far-reaching surveillance reforms. But the most high-ranking intelligence officials in the country have endorsed its approach because it is a responsible bill. It protects Americans' privacy and keeps them safe. The Senate should take up the bill once the House passes it this week.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

[From National Journal, May 8, 2015]  
 REPUBLICANS MAKE DUBIOUS CLAIMS IN  
 DEFENSE OF NSA SURVEILLANCE

MITCH MCCONNELL AND HIS COHORT OF SECURITY HAWKS ARE STOPPING AT NOTHING TO RENEW THE SPY AGENCY'S PHONE DRAGNET. BUT HOW FAIR IS THEIR DEFENSE?

(By Dustin Volz)

One by one, several powerful Republican senators took to the floor Thursday morning to offer one of the most full-throated defenses of the National Security Agency's bulk collection of billions of U.S. phone records since Edward Snowden exposed the program nearly two years ago.

The crux of their argument is unmistakable: The NSA's expansive surveillance powers need to remain intact and unchanged to keep Americans safe from potential terrorist threats—and if these powers existed before Sept. 11, 2001, they may have assisted in preventing the attacks on the World Trade Center and the Pentagon.

But some of the talking points used by Senate Majority Leader Mitch McConnell and his allies appear to rely heavily on assertions that are either dubious in their veracity or elide important contextual details.

Here is a review of some of their declarations:

Claim: "Not only have these tools kept us safe, there has not been a single incident, not one, of intentional abuse of them."—McConnell

McConnell may have been referring specifically to the phone records program here, but the NSA does not, as he implies, have a spotless record.

According to a 2013 inspector general report, NSA analysts intentionally misused foreign surveillance authorities at least a dozen times in the past decade, sometimes for the purpose of spying on their romantic interests. So-called "loveint"—short for "love intelligence"—was revealed by the inspector general in response to a letter sent from Republican Sen. Chuck Grassley, who this year renewed a call for the Justice Department to provide an update on how it was handling its investigation into the alleged willful abuses and to "appropriate accountability for those few who violate the trust placed in them."

Additionally, a 2012 internal audit obtained by The Washington Post found that the NSA has violated privacy restrictions set in place for its surveillance programs thousands of times each year since 2008. The audit found that most—though not all—infractions were unintended.

Claim: "The compromise legislation rolls us back to the same thing we were doing pre-9/11."—Senate Intelligence Chairman Richard Burr

The USA Freedom Act referenced by Burr would reauthorize three key surveillance provisions under the post-9/11 Patriot Act. It would usher in several reforms related to transparency and oversight, but it would keep those authorities intact. Section 215 of the law would no longer allow for the bulk collection of U.S. phone metadata by the NSA, but the authority—created after 9/11—would still exist.

Claim: "The alternatives to the current program would not come close to offering the capabilities that now enable us to protect Americans."—Sen. Tom Cotton

Cotton's claim does not align with the stance of Director of National Intelligence James Clapper and then-Attorney General Eric Holder, who sent a letter to lawmakers last year expressing their support for an earlier iteration of the Freedom Act. "The intelligence community believes that your bill preserves essential intelligence-community capabilities; and the Department of Justice and the Office of the Director of National Intelligence support your bill and believe that it is a reasonable compromise that enhances privacy and civil liberties and increases transparency," the letter read. That version of the Freedom Act is widely considered more limiting of surveillance powers than the one being debated in Congress this year.

Claim: "One alternative offered by opponents of this program is to have phone companies retain control of all call data and provide the NSA only the data responsive to searches phone companies would run on the NSA's behalf. This is not technologically feasible."—Cotton

The reliance on phone companies to retain call data already occurs, as they are the ones who turn the records over to the government in bulk. Cotton, who voted for a pared down iteration of the Freedom Act last year when he served in the House, cites an 85-page study from the National Research Council to support this assertion. But the Arkansas freshman appears to be conflating its findings, which dealt with whether software could fully replace bulk collection, with what backers of the Freedom Act are attempting to do. "Although no software can fully replace bulk with targeted information collection, software can be developed to more effectively target collection and to control the usage of collected data," the report concluded. Cotton's reservations—that the new system may take longer than the old—have more to do with process than technological capabilities.

Claim: "Here's the truth. If this program had existed before 9/11, it is quite possible that we would have known that the 9/11 hijacker Khalid al-Mihdhar was living in San Diego and making phone calls to an al-Qaida safehouse in Yemen. There's no guarantee we would have known. There's no way we can go back in time and prove it, but there is a probability that we would have known and there's a probability that American lives could have been saved."—Sen. Marco Rubio.

Rubio hedges his language several times with this claim, but the statement still omits important context. As reported by a 2013 ProPublica investigation, "U.S. intelligence agencies knew the identity of the hijacker in question, Saudi national Khalid al-Mihdhar, long before 9/11 and had the ability

find him, but they failed to do so." Such missed opportunities to disrupt Midhar's activities, which were being monitored by at least as early as 1999, reflect a failure of information sharing among intelligence agencies, ProPublica notes, and are described in detail in the 9/11 Commission report.

#### SENATORS' QUESTIONABLE CLAIMS ABOUT NSA BULK COLLECTION

CENTER FOR DEMOCRACY & TECHNOLOGY

On May 7th, 2015, the Second Circuit issued a ruling that declared the NSA's bulk collection of Americans' phone records was clearly unlawful under the Section 215 of the PATRIOT Act. The ruling provided another boost to supporters of surveillance reform and the backers of the USA FREEDOM Act. Hours after the ruling came down, several U.S. Senators—Mitch McConnell, Richard Burr, Tom Cotton, Jeff Sessions, and Marco Rubio—took to the Senate Floor to forcefully defend the NSA's bulk collection program. The Senators made some statements that merit a second look, and serious skepticism.

Claim 1: The NSA's bulk collection of Americans' phone records is essential to national security. "Under consideration in the House and proposed in the Senate is the so-called USA FREEDOM Act, which will eliminate the essential intelligence this program collects."—Senator Tom Cotton

The weight of public evidence contradicts this claim, based on statements from experts with access to classified intelligence:

The Attorney General and the Director of National Intelligence stated that the USA FREEDOM Act of 2014—which is in all ways identical to or less restrictive of surveillance than the 2014 bill—"preserves essential Intelligence Community capabilities" though the bill "bans bulk collection under a variety of authorities."

The President's Review Group noted in 2014 that the bulk collection program yielded information that was "not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders."

The Privacy and Civil Liberties Oversight Board stated in 2014: "Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack."

Senators Wyden, Heinrich, and Udall said in 2013 "[We] have reviewed this surveillance extensively and have seen no evidence that the bulk collection of Americans' phone records has provided any intelligence of value that could not have been gathered through less intrusive means."

It's important not to conflate the value of Sec. 215 overall with the effectiveness of the use of Section 215 for bulk collection. Sec. 215 can be used for targeted—not just bulk—data collection. The USA FREEDOM Act ends nationwide bulk collection under Sec. 215, but preserves the government's ability to use Sec. 215 for more targeted collection. What is at stake with USA FREEDOM is not Sec. 215 itself, but its continued use for bulk domestic surveillance.

Claim 2: The bulk collection program could have stopped 9/11. "Here is the truth. If this program had existed before 9/11, it is quite possible we would have known that 9/11 hijacker Khalid Al Mihdhar was living in San Diego and was making phone calls to an Al

Qaeda safe house in Yemen.”—Senator Marco Rubio

A bulk collection program was not necessary to find Al Mihdhar prior to 9/11. As the PCLOB report details, the NSA had already begun intercepting calls to and from the safe house in Yemen in the late 1990s. Since the government knew the number of the safe house, and Al Mihdhar was calling that number, it would only be necessary to collect the phone records of the safe house to discover Al Mihdhar in San Diego. This is, in fact, an example of how targeted surveillance would have been more effective than bulk collection. The 9/11 Commission Report and other sources note that the CIA was aware of Mihdhar well before the attack and missed multiple opportunities to deny him entry to the U.S. or intensify their surveillance of him.

Claim 3: Bulk collection of phone records is the same as a subpoena. “This is the way the system works and has worked for the last 50 years—40 years at least. A crime occurs. A prosecutor or the DEA agent investigates. They issue a subpoena to the local phone company that has these telephone toll records—the same thing you get in the mail—and they send them in response to the subpoena.”—Senator Jeff Sessions

The Second Circuit opinion, which held that the bulk collection program is unlawful, included a lengthy comparison of subpoenas and the bulk collection program. The bulk collection program encompasses a vastly larger quantity of records than could be obtained with a subpoena. The Second Circuit notes that subpoenas typically seek records of particular individuals or entities during particular time periods, but the government claims Sec. 215 provides authority to collect records connected to everyone—on an “ongoing daily basis”—for an indefinite period extending into the future.

Claim 4: The government is only analyzing a few phone records. “The next time that any politician—Senator, Congressman—talking head, whoever it may be, stands up and says “The U.S. Government is [ . . . ] going through your phone records,” they are lying. It is not true, except for some very isolated instances—in the hundreds—of individuals for whom there is reasonable suspicion that they could have links to terrorism.”—Senator Marco Rubio

The NSA’s telephony bulk collection program collects the phone records of millions of Americans with no connection to a crime or terrorism. These records are stored with the NSA and they are analyzed scores of times each year when the NSA queries the numbers’ connection to the phone numbers of suspects. Moreover, until 2014, when the NSA suspected a phone number was connected to terrorism, the NSA analyzed the phone records “three hops” out—querying those who called those who called those who called the original suspect number. As a result, the PCLOB estimated, a single query could subject the full calling records of over 420,000 phone numbers to deeper scrutiny. In 2014, the President limited the query to “two hops”—though this can still encompass the full call records of thousands of phone numbers. The USA FREEDOM Act (Sec. 101) would authorize the government to obtain “two hops” worth of call records from telecom companies.

Claim 5: The USA FREEDOM Act threatens privacy by leaving phone records with telecom companies. “[T]he opponents of America’s counterterrorism programs would rather trust telecommunication companies to hold this data and search it on behalf of our government. [ . . . ] In addition to making us less safe, the USA FREEDOM Act would make our privacy less secure.”—Senator Mitch McConnell

The telecom companies already have the phone records since the records are created in the normal course of their business. The USA FREEDOM Act does not shift control of data from NSA to telecoms; the bill limits the volume of what the government can collect from companies with a single 215 order. Keeping the records with the phone companies, as the USA FREEDOM Act would require, does not create a new privacy intrusion, or, according to the public record, pose new security risks. In contrast, it is highly intrusive for the government to demand companies provide a copy of the communication records of millions of Americans on a daily basis to a secretive military intelligence agency for data mining.

One last important point: The discussion on the Senate Floor centered exclusively on the bulk collection of phone records. However, the debate and the legislation before Congress are not just about one telephony metadata program. The debate is over whether the government should have the authority to collect a variety of records in bulk under the PATRIOT Act. The government has claimed that its bulk collection authority extends to any type of record that can reveal hidden relationships among individuals—which could include phone call, email, cell phone location, and financial transaction records. Framing the issue in terms of phone records makes the problem seem much smaller than it is, especially as our society moves into a technology-enabled future where each individual will create much more metadata and digital records than the present. The stakes are high.

#### VOTE EXPLANATION

Mrs. BOXER. Mr. President. Due to a commitment in my state, I was unable to be here for the votes on the Iran Nuclear Agreement Review Act. Had I been present, I would have voted in support of this bill.

#### HONORING THOSE WHO HAVE GIVEN THE ULTIMATE SACRIFICE SERVING IN U.S. CUSTOMS AND BORDER PROTECTION

Mr. CARPER. Mr. President, the mission of U.S. Customs and Border Protection, CBP, is broad and diverse. The more than 60,000 men and women of CBP protect our borders at and between our ports of entry. They protect Americans against terrorists and the instruments of terror. They enforce our laws and help boost our economic security and prosperity by facilitating trade and travel. While the roles they play each day may differ, the men and women of CBP share one common goal: to keep our country a safe, secure, and resilient place where the American way of life can thrive. They provide selfless service to our country, and they do so with honor and distinction under an ever-present and evolving threat.

Today I wish to pay tribute to the agents and officers who have given the ultimate sacrifice in the service of our Nation. All told, 33 courageous men and women of CBP have died in the line of duty since the agency’s inception in 2003. Today we commemorate these brave men and women, celebrate their lives, and offer their families and loved ones our continued support. They have

earned the respect and appreciation of a grateful nation. I ask unanimous consent that a list of these agents and officers be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

James P. Epling, Border Patrol Agent, U.S. Customs and Border Protection, Yuma, Arizona, End of Watch: December 16, 2003; Travis W. Attaway, Senior Patrol Agent, U.S. Customs and Border Protection, Harlingen, Texas, End of Watch: September 19, 2004; Jeremy M. Wilson, Senior Patrol Agent, U.S. Customs and Border Protection, Harlingen, Texas, End of Watch: September 19, 2004; George B. Debates, Senior Patrol Agent, U.S. Customs and Border Protection, Casa Grande, Arizona, End of Watch: December 19, 2004; Nicholas D. Greenig, Senior Patrol Agent, U.S. Customs and Border Protection, Tucson, Arizona, End of Watch: March 14, 2006; David N. Webb, Senior Patrol Agent, U.S. Customs and Border Protection, Ajo, Arizona, End of Watch: November 3, 2006.

Ramon Nevarez, Jr., Border Patrol Agent, U.S. Customs and Border Protection, Lordsburg, New Mexico, End of Watch: March 15, 2007; David J. Tourscher, Border Patrol Agent, U.S. Customs and Border Protection, Lordsburg, New Mexico, End of Watch: March 16, 2007; Clinton B. Thrasher, Air Interdiction Agent, U.S. Customs and Border Protection, McAllen, Texas, End of Watch: April 25, 2007; Richard Goldstein, Border Patrol Agent, U.S. Customs and Border Protection, Indio, California, End of Watch: May 11, 2007; Robert F. Smith, Air Interdiction Agent, U.S. Customs and Border Protection, El Paso, Texas, End of Watch: May 22, 2007; Eric N. Cabral, Border Patrol Agent, U.S. Customs and Border Protection, Boulevard, California, End of Watch: July 26, 2007.

Julio E. Baray, Air Interdiction Agent, U.S. Customs and Border Protection, El Paso, Texas, End of Watch: September 24, 2007; Luis A. Aguilar, Border Patrol Agent, U.S. Customs and Border Protection, Yuma, Arizona, End of Watch: January 19, 2008; Jarod C. Dittman, Border Patrol Agent, U.S. Customs and Border Protection, San Diego, California, End of Watch: March 30, 2008; Nathaniel A. Afolayan, Border Patrol Agent, U.S. Customs and Border Protection, Artesia, New Mexico, End of Watch: May 1, 2009; Cruz C. McGuire, Border Patrol Agent, U.S. Customs and Border Protection, Del Rio, Texas, End of Watch: May 21, 2009; Robert W. Rosas, Jr., Border Patrol Agent, U.S. Customs and Border Protection, Campo, California, End of Watch: July 23, 2009.

Mark F. Van Doren, Border Patrol Agent, U.S. Customs and Border Protection, Falfurrias, Texas, End of Watch: May 24, 2010; Charles F. Collins II, CBP Officer, U.S. Customs and Border Protection, Anchorage, Alaska, End of Watch: August 15, 2010; Michael V. Gallagher, Border Patrol Agent, U.S. Customs and Border Protection, Casa Grande, Arizona, End of Watch: September 2, 2010; John R. Zykas, CBP Officer, U.S. Customs and Border Protection, San Diego, California, End of Watch: September 8, 2010; Brian A. Terry, Border Patrol Agent, U.S. Customs and Border Protection, Naco, Cochise, Arizona, End of Watch: December 15, 2010; Hector R. Clark, Border Patrol Agent, U.S. Customs and Border Protection, Yuma, Arizona, End of Watch: May 12, 2011; Eduardo Rojas, Jr., Border Patrol Agent, U.S. Customs and Border Protection, Yuma, Arizona, End of Watch: May 12, 2011.