

## **House Intelligence Committee Calls for End to NSA Bulk Telephone Metadata Program While Preserving Counterterrorism Capabilities**

On the morning of September 11, 2001, Khalid al-Mihdhar stepped on to American Airlines Flight 77, the flight he would later hijack and crash into the Pentagon. Al-Mihdhar might have been in prison, instead of on that flight, if the government knew he had called an al-Qaeda safehouse in Yemen from inside the U.S. seven times before the attacks. The failure to spot phone calls by al-Mihdhar and others led the Intelligence Community to begin collecting large volumes of call data records—specifically the number dialed and the date and duration of the call—to determine whether suspected terrorists had contacts inside the United States.

Since last summer, a great deal has been written about the program's scope, capabilities, and legality—much of it wrong. The fact is that the program is legal. It was authorized by Congress, overseen by all three branches of government, and found constitutional many times over. No review of the program revealed an intentional misuse of its authority.

We recognize that the Intelligence Community must have the confidence of the American people to do its life-saving work. Over the past nine months, we have studied ways to reform the program while maintaining its effectiveness. We have identified an approach that will end the government's collection of bulk telephone metadata, maintains significant capabilities to identify potential threats to the United States, and imposes no new burdens on private industry.

Our bipartisan proposal authorizes the government to obtain only the metadata it uses to guard against terrorists and other foreign bad actors. We would allow the government to obtain records of individual numbers for which there is a reasonable and articulable suspicion of an association with international terrorism or clandestine intelligence activity, plus the records of numbers connected with those suspect numbers.

Our bill affirmatively prohibits the government from using this new procedure to obtain any communications content or any personally identifiable information. Just as under the current program, the government would not be able to use this new authority to listen to phone calls or read e-mails.

Our bill also mandates judicial scrutiny every step of the way. Before the government can direct a company to provide targeted metadata, the government must first create—and the Foreign Intelligence Surveillance Court (FISC) must approve—selection procedures to ensure that the government obtains only the metadata that is associated with terrorists or foreign intelligence targets, as well as detailed procedures to maximize civil liberties and privacy protections.

Once the FISC approves these procedures, the government can direct providers to search and provide metadata connected with a suspect number. If a provider believes a directive is unlawful, it can challenge the directive in court. And that directive must be supported by a “reasonable, articulable suspicion” that the number is connected to terrorism or espionage, which the government must submit to the FISC for judicial review. If the court finds that the government’s facts don’t add up, the court can order the Government to purge any metadata it received. Our bill will ensure the NSA continues to operate within the boundaries of the law.

To be clear, under this proposal, the government would no longer be able to collect bulk call records and phone companies would not be required to retain their records any longer than they already do.

Ending bulk collection isn’t the only way our bill seeks to restore the American people’s confidence in NSA programs. For the first time, the government would either have to release all significant FISC decisions or issue an unclassified summary of the opinion’s key points. FISC judges would gain the statutory power to appoint a lawyer from a precleared pool of advocates to argue against the government’s position, guaranteeing that the judges can always hear argument from both sides of a case. And the bill would require the government to regularly review its electronic surveillance policies to make sure they continue to safeguard privacy and civil liberties as technology changes.

We know there are other bills in Congress that would also end bulk collection, but many would prevent us from uncovering terrorist plots against our country and our allies. National security must not be a game of Jenga where we remove post-9/11 counterterrorism tools one at a time, until we find out which move causes the entire structure to collapse. Without NSA counterterrorism tools, Najibullah Zazi might have set off bombs during rush hour in the New York City subway in September 2009. Some people may say that’s “not enough” when compared to the amount of information the NSA obtains, but we would be shocked if anyone on September 12, 2001, wouldn’t have done everything possible to find hijackers like al-Mihdhar and prevent just one terrorist attack.

We look forward to working with our colleagues in the House and Senate to enact a bipartisan proposal that will ensure the highest levels of privacy and civil liberties while still maintaining the tools our government needs to keep us, and our allies, safe.

*Chairman Mike Rogers (R-MI) and Ranking Member Ruppertsberger serve as leaders of the U.S. House Permanent Select Committee on Intelligence. For more information, please visit <http://intelligence.house.gov/>*