THE CHRISTIAN SCIENCE MONITOR

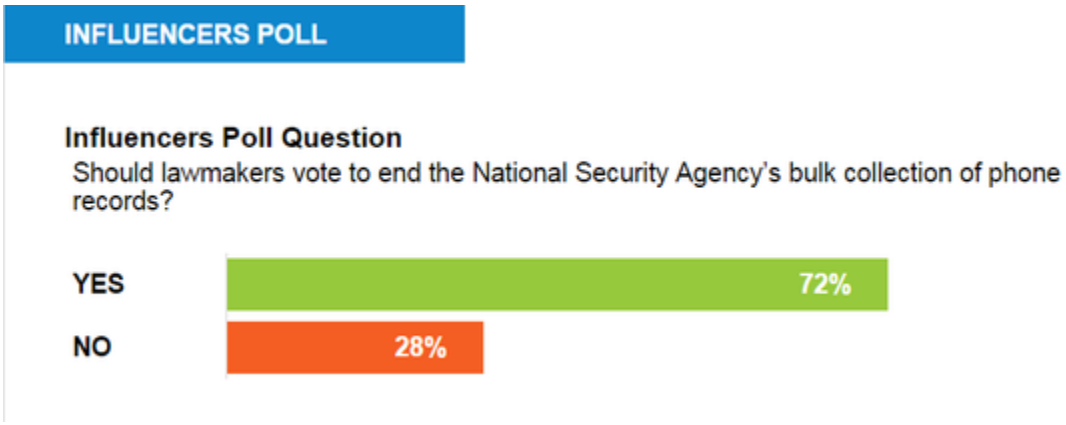
# Influencers: Congress should end NSA bulk data collection

**In a Passcode survey, a group of more than 90 experts from across government, the private sector and privacy advocacy community call for surveillance reforms.**

By Sara Sorcher

May 6, 2015

Lawmakers should vote to end the National Security Agency's sweeping surveillance program that scooped up the call records of tens of millions of Americans, a strong majority of Passcode's Influencers said.




Nearly two years after former NSA contractor Edward Snowden exposed the controversial program, the House of Representatives is scheduled to vote next week on the USA Freedom Act, a bill that would effectively end bulk collection. Yet Senate Majority Leader Mitch McConnell, backed by defense hawks, is pushing instead for a five-year extension of a key Patriot Act provision set to expire on June 1. Intelligence agencies have used that provision, Section 215, to justify the bulk collection.

With three weeks left on the clock, 72 percent of Passcode's Influencers – a group of more than 90 security and privacy experts from across government, the private sector, academia, and the privacy community – are calling for Congress to break the standoff and make reforms.

However, they differed on the reasons why. "Two years ago, people learned that intelligence agencies have been indiscriminately collecting the private records of innocent people around the world. This is a violation of basic human rights and it must end," said Amie Stepanovich, senior policy counsel at Access, a human rights organization.

Heather West, from Internet performance and security company CloudFlare, said ending bulk collection of both phone and online records "is an important step in ensuring that the US government – and by proxy, US companies – are trusted globally."

The current bulk collection program is of dubious national security value, said Chris Finan, chief executive officer of security company Manifold Security. "It is no different in principle to the British writs of assistance that inspired the Fourth Amendment," Mr. Finan said. "If lawmakers think such warrantless collection is necessary for the nation's security they should put forward a Constitutional amendment. Metadata can be used to create a rich mosaic of a person's life, allowing a spy agency to do so without a warrant is simply not consistent with what the Framers intended."

From an intelligence perspective, collecting data from call records is "invaluable" to find a "needle in a haystack" during investigations and missions, acknowledged Rick Howard, chief security officer for Palo Alto Networks, who also served in the Army for 23 years. "By drawing phone and e-mail nodal analysis diagrams of suspects (link analysis), intelligence analysts can very quickly find key leaders of terrorist groups," Mr. Howard said.

But Howard also agreed lawmakers should vote to end the program because it runs up against the Fourth Amendment, meant to ensure people's rights to be secure against unreasonable searches and seizures unless there's probable cause for a specific warrant. "This debate fundamentally comes down to our to country's decision on this one issue: do we care more about liberty or security? The Snowden revelations clearly demonstrate what the country is willing to do to preserve our security. I worry about what we give up as a nation when we do that and how far do we go down that rabbit hole if we commit to it," Howard said.

"In the entire world history of governments using spy agencies to collect information on enemies and frenemies, without fail, when the state turns its intelligence apparatus on its own citizens, things get ugly quickly ... We tell ourselves, 'It is just metadata, what's the harm?' But over time, as we keep chipping parts of the Fourth Amendment away, pretty soon we might find ourselves in an Orwellian novel and wondering how we got here. What's on the table is a chance to reform Section 215 into something we can all be more comfortable with."

A minority of 28 percent of Passcode Influencers said lawmakers should not vote to end bulk collection.

"Although it may make sense to make some changes to Section 215, I think NSA should continue to collect metadata on domestic phone calls for counterterrorism purposes," said Ely Kahn, cofounder of Sqrrl, a big data and cybersecurity firm. "Privacy and security is a trade-off (at least in this case), and everyone's personal privacy versus security equation will have some differences. I don't see a viable alternative to this program, and losing it would degrade our abilities to stop the next terrorist attack. For me, the loss of some modicum of personal privacy is worth the greater good of reducing the risk of terrorism."

Even some Influencers who said lawmakers should leave the program alone acknowledged the relative unpopularity of the program since it was exposed publicly may be too strong to keep it. Lawmakers should "optimally" keep the program running, one Influencer, who chose to remain anonymous, said. "But if ending it gives Congress the political fortitude and the intelligence community the necessary top cover to continue vastly more important collection programs, then the sacrifice is well worth it."

To preserve the candor of their responses, Influencers have the choice to keep their comments anonymous, or voice their opinions on the record.

"It's unconstitutional. It's as simple as that. Imagine a world where the British tracked every single letter sent by American colonists – and the Founders were okay with that. You can't, can you? The Fourth Amendment was written precisely to limit dragnet searches for the details of our lives." – **Alvaro Bedoya, Georgetown Law Center**

"A vote is literally not necessary since the current authorities expire on June 1. However, the fact that three other authorities (individualized investigations under 215, 'lone wolf,' and roving wiretaps) will also expire on that same date make the absence of any vote extremely unlikely. It is also not clear that Congress ever specifically authorized this collection program since the original author if the USA PATRIOT Act, Congressman Sensenbrenner, says bulk collection of telephone metadata was never contemplated by him. In any event, based on the conclusions reached by both the Privacy and Civil Liberties Oversight Board and The President's Review Group on Intelligence and Communications Technologies, it seems clear that the telephone metadata program is of very limited value in preventing terrorism attacks and that whatever value there may be is outweighed by the costs in terms of privacy, civil liberties, and information security." **– Influencer**

"Ending bulk metadata collection is a first step to reestablishing trust in the intelligence community's respect for basic American ideals." **– Influencer**

"The foreign intelligence mission is important to a wide array of U.S. government functions. However, when it comes to domestic collection of intelligence, there are serious questions of both equities and authorities that clearly appear not to have been addressed in any systematic or democratic manner. While it is not reasonable that sources and methods be discussed or disclosed in public, it seems the barest minimum of responsible policy development that the rules under which such things are conducted would be debated clearly, very publicly, and with the active participation of a variety of stakeholders. Several branches of the U.S. government have failed in their duty to do the latter. When even elected lawmakers have to torturously parse

language and meticulously craft statements to even begin to discuss whether a domestic surveillance program is fundamentally legal, citizens should take the hint that our country is proceeding down a perilous slope, in secret and in darkness. The Church Committee proceedings in the 1970s were a response to overreach on the part of the U.S. Intelligence agencies. We may do well to revisit this sort of earnest review again in the present moment." **– Influencer**

"The best path lies between completely re-authorizing Section 215 of the PATRIOT Act and the proposed FREEDOM Act - but much closer to the FREEDOM Act language." **– John Pescatore, SANS Institute**

"Several pieces of current legislation, for example, the 'USA FREEDOM Act,' purport to end bulk data collection, but that's only a hollow, definitional win – these same bills legalize mass surveillance (something politicians are doing their best to obfuscate). If you really want to end mass surveillance, there is only one bill that actually does that, the Surveillance State Reform Act: Everything else is political theater and double-speak 'wins.'" **– Sascha Meinrath, X-Lab**

"Bulk collection turns upside down our constitutional right to be secure in our papers and effects, as well as our right to associate freely without being subject to governmental tracking. It turns us all into potential suspects instead of free people. Moreover, as the reports by the various Inspectors General confirm (released by the government after a FOIA by The New York Times), bulk telephone records collection simply isn't worth the huge amount of resources we've spent on it for the past decade and a half." **– Cindy Cohn, Electronic Frontier Foundation**

"While ending this program would be a start, a more useful question would be: what additional US person data is being collected under the same authority?" **– Matthew Green, Johns Hopkins University**

"But only if they also vote to 'end' or at least meaningfully constrain the collection and collation of *much* more sensitive personal data by private firms. Seriously. Is the NSA really a greater risk to your freedom, well-being, and autonomy than are data-enabled advertisers, insurers, and service providers? Time for Americans to start asking themselves that question in a serious and honest way." **– Influencer**

"The legal threshold for collecting needs to be more exacting and precise, and the court oversight and protections for individuals need to be more robust. Mass collection has replaced good investigation in too many cases. As a result, they have missed the opportunity to detect and disrupt dangerous people." **– Jenny Durkan, Quinn Emanuel Urquhart & Sullivan**

"Congress doesn't need to vote to end the Section 215 telephony metadata program. By not renewing the 215 authority, the program ends. This program should be shut down though, either through Congressional inaction or specific legislation. Through legislation, Congress can and should reform the FISA court and NSA's even more problematic surveillance programs that operate under Executive Order 12333." **– Chris Soghoian, ACLU**

"At this point, two independent review panels have agreed that the indiscriminate collection of innocent American's sensitive phone records is not necessary—nor even an effective intelligence

tool. The president and the intelligence community have both accepted that it should end. Resistance to reform from legislators at this point is not about protecting American security, but simply stubborn posturing." **– Julian Sanchez, Cato Institute**

"The NSA's bulk collection of American's call records under Section 215 should end immediately. The legal grounds for the bulk collection program are faulty, the privacy intrusion is severe, and multiple experts with access to classified intelligence have concluded that the program offers no real benefit to national security. However, this debate isn't really about one bulk collection program - rather, this debate is about the government's claim of legal authority to collect Americans' records in bulk. It's not enough to shutter the existing program - Congress needs to change the law to prevent other bulk collection programs in the future. The USA FREEDOM Act of 2015 would end domestic bulk collection under the PATRIOT Act, and we urge Congress to pass it swiftly without weakening the bill." **– Harley Geiger, Center for Democracy and Technology**

"While I have doubts that such action will stop the U.S. government or others from spying on the public, the vote to end it 'officially' will send a signal that such covert activities should be exercised with prudence. Knowledge engines and big data analytics are making every individual a target of powerful corporations, not just governments, and the attention on the NSA is an unfortunate diversion from more dangerous future threats to individuals. Algorithmic oppression and biometric surveillance is expanding to the point at which people are in danger of being spied upon and manipulated by anyone who's willing to pay for the service. See, for instance, Facebook's emotion experiment: and the growing field of affective computing and the 'emotion economy': The near future will likely involve advertisers and others surveilling you in your home through the telecommunications, TV and gaming equipment YOU buy and pay a monthly fee to own. In 2013, Rep. Mike Capuano of Massachusetts drafted the We Are Watching You Act, to require businesses to indicate when sensing begins, and to give consumers the right to disable sensors and he could not convince colleagues to sign on because, 'The most difficult part is getting people to realize that this is real.'" **– Influencer**

"Although the bill does not contain all of the reforms that the Open Technology Institute believes are necessary, passage of the USA FREEDOM Act of 2015 would represent an important first step in the long process of reining in the NSA's overreaching surveillance programs. OTI therefore urges the Judiciary and Intelligence Committees to favorably report the bill to the House floor as soon as possible, and for the House to approve the legislation without delay and without weakening any of its important reforms. A strong vote in the House will help ensure that the bill can pass through the Senate ahead of the June 1st deadline for the renewal of PATRIOT Section 215, that deadline being the primary leverage for obtaining reform during this Congress. In addition to being necessary to protect Americans' privacy, reform is also necessary to restore international trust in the US technology industry, which as detailed in OTI's report "Surveillance Costs" has been seriously damaged by news of the NSA's mass surveillance programs..... Passing USA FREEDOM now, using the upcoming expiration of Section 215 as leverage, is our last, best chance for meaningful surveillance reform in the foreseeable future. Anyone in Congress who cares about ending bulk surveillance by the NSA should support this bill, because the most likely alternatives if this bill fails are either a sham reform bill that's much weaker, or a straight reauthorization of Section 215 with no reform at all. At this point, a vote against USA

FREEDOM is a vote against surveillance reform, period, even if it's motivated by a desire for stronger reforms. We want more reforms too—but the best way to get them is to succeed in passing USA FREEDOM now and then build on that success, rather than let this opportunity slip by." **– Kevin Bankston, Open Technology Institute**

"Why would they do that? What abuses do they claim they are stopping?" **– Influencer**

"Intelligence analysts need tools to protect our nation. However, there may be ways to modify the existing program to better protect civil liberties and privacy, while still retaining the operational benefits of the program." **– Influencer**

"'Just stop collecting' is as capricious, is no more responsible and is as ineffective as saying, 'Let's collect and access everything.' The present system is clearly flawed, and through leaked materials it's clear that access to bulk collections was abused by the government. But rather than speaking in methods - "Shut it down!" - let's think in outcomes: the desire shared by those on both sides of this debate is, while defending the civil and human rights of citizens, to protect our nation against terror, violent crime and acts (like human trafficking and money laundering) that support those things. If that's the desired outcome, no extreme will ever be the right answer. True transparency and oversight - dismantling the kangaroo FISA court, removal of extra-Constitutional secret hearings, and putting a stop to the over-classification of everything by an increasingly Orwellian national security regime - are far more pressing than policy on any given datatype." **– Nick Selby, StreetCred software**

"What Congress could usefully do is to rescind the location triangulation regime that tracks position (Location Services) as not doing tracking yet retaining mobility is 100% feasible whereas making the claim that by some legislative doodad we can make the Internet immune to traffic analysis is flatly mendacious. In other words, mandate something that is, in fact, possible and don't mandate something that is, in fact, impossible. The worst laws are the ones that cannot be enforced and 'don't watch packets in routed networks' is of that unenforceable sort. Precisely." **– Dan Geer, In-Q-Tel**

"Oversight by Congress is appropriate but it needs to be balanced not to impede on the national security mission. Tracing potential terrorism threats and connecting the networks via bulk phone records is a useful tool. Privacy of individuals who are not a threat needs to be a priority and protocols can be established. However, we must be careful not to throw the baby out with the bathwater." **– Chuck Brooks, Xerox**