

<http://www.nytimes.com/2013/09/07/us/politics/legislation-seeks-to-bar-nsa-tactic-in-encryption.html>

Legislation Seeks to Bar N.S.A. Tactic in Encryption



Ryan Collard for The New York Times

Legislation proposed by Representative Rush D. Holt Jr., Democrat of New Jersey, would eliminate much of the escalation in the government's spying powers undertaken since 2001.

By [SCOTT SHANE](#) and [NICOLE PERLROTH](#)

Published: September 6, 2013

After disclosures about the [National Security Agency's stealth campaign](#) to counter Internet privacy protections, a congressman has proposed legislation that would prohibit the agency from installing “back doors” into encryption, the electronic scrambling that protects e-mail, online transactions and other communications.

Representative Rush D. Holt, a New Jersey Democrat who is also a physicist, said Friday that he believed the N.S.A. was overreaching and could hurt American interests, including the reputations of American companies whose products the agency may have altered or influenced.

“We pay them to spy,” Mr. Holt said. “But if in the process they degrade the security of the encryption we all use, it's a net national disservice.”

Mr. Holt, whose Surveillance State Repeal Act would eliminate much of the escalation in the government's spying powers undertaken after the 2001 terrorist attacks, was responding to news reports about N.S.A. documents showing that the agency has spent billions of dollars over the last decade in an effort to defeat or bypass encryption. The reports, by The New York Times, [ProPublica](#) and [The Guardian](#), were posted online on Thursday.

The agency has encouraged or coerced companies to install back doors in encryption software and hardware, worked to weaken international standards for encryption and employed custom-built supercomputers to break codes or find mathematical vulnerabilities to exploit, according to the documents, disclosed by Edward J. Snowden, the former N.S.A. contractor.

The documents show that N.S.A. cryptographers have made major progress in breaking the encryption in common use for everyday transactions on the Web, like Secure Sockets Layer, or SSL, as well as the virtual private networks, or VPNs, that many businesses use for confidential communications among employees.

Intelligence officials say that many of their most important targets, including terrorist groups, use the same Webmail and other Internet services that many Americans use, so it is crucial to be able to penetrate the encryption that protects them. In an intense competition with other sophisticated cyberespionage services, including those of China and Russia, the N.S.A. cannot rule large parts of the Internet off limits, the officials argue.

A statement from the director of national intelligence, James R. Clapper Jr., criticized the reports, saying that it was "not news" that the N.S.A. works to break encryption, and that the articles would damage American intelligence collection.

The reports, the statement said, “reveal specific and classified details about how we conduct this critical intelligence activity.”

“Anything that yesterday’s disclosures add to the ongoing public debate,” it continued, “is outweighed by the road map they give to our adversaries about the specific techniques we are using to try to intercept their communications in our attempts to keep America and our allies safe and to provide our leaders with the information they need to make difficult and critical national security decisions.” But if intelligence officials felt a sense of betrayal by the disclosures, Internet security experts felt a similar letdown — at the N.S.A. actions.

“There’s widespread disappointment,” said Dan Kaminsky, a prominent security researcher. “This has been the stuff of wild-eyed accusations for years. A lot of people are heartbroken to find out it’s not just wild-eyed accusations.”

Sascha Meinrath, the director of the Open Technology Institute, a research group in Washington, said the reports were “a startling indication that the U.S. has been a remarkably irresponsible steward of the Internet,” which he said the N.S.A. was trying to turn into “a massive platform for detailed, intrusive and unrestrained surveillance.”

Companies like Google and Facebook have been moving to new systems that, in principle, would make government eavesdropping more difficult. Google is in the process of encrypting all data that travels via fiber-optic lines between its data centers. The company speeded up the process in June after the initial N.S.A. disclosures, according to two people who were briefed on Google’s plans but were not authorized to speak publicly about them. The acceleration of the process was first reported Friday by The Washington Post.

For services like Gmail, once data reaches a user's computer it has been encrypted. But as messages and other data like search queries travel internally among Google's data centers they are not encrypted, largely because it is technically complicated and expensive to do.

Facebook announced last month that it would also transition to a novel encryption method, called perfect forward secrecy, that makes eavesdropping far more difficult.

Marc Rotenberg, the executive director of the Electronic Privacy Information Center, a civil liberties group in Washington, said the quandary posed by the N.S.A.'s efforts against encryption began with its dual role: eavesdropping on foreign communications while protecting American communications.

"Invariably the two missions collide," he said. "We don't dispute that their ability to capture foreign intelligence is quite important. The question is whether their pursuit of that mission threatens to undermine the security and privacy of Internet communications."

Mr. Rotenberg is a veteran of what were known as the "crypto wars" of the 1990s, when the N.S.A. proposed the Clipper Chip, a government back door that would be built into every encryption program.

That proposal was defeated by a diverse coalition of technology businesses and privacy advocates, including Mr. Rotenberg's organization. But the documents make clear that the N.S.A. never gave up on the goal of being able to read everything and has made what memos call "breakthroughs" in recent years in its efforts.

A complicating factor is the role of the major American Internet companies, which have been the target of counterencryption efforts by both the N.S.A. and its closely allied British counterpart, GCHQ. One document describes “new access opportunities” in Google systems; the company said on Thursday that it had not given the agencies access and was aware of no breach of its security.

But the perception of an N.S.A. intrusion into the networks of major Internet companies, whether surreptitious or with the companies’ cooperation, could hurt business, especially in international markets.

“What buyer is going to purchase a product that has been deliberately made less secure?” asked Mr. Holt, the congressman. “Even if N.S.A. does it with the purest motive, it can ruin the reputations of billion-dollar companies.”

In addition, news that the N.S.A. is inserting vulnerabilities into widely used technologies could put American lawmakers and technology companies in a bind with regard to China.

Over the last two years, American lawmakers have accused two of China’s largest telecommunications companies, Huawei Technologies and ZTE, of doing something parallel to what the N.S.A. has done: planting back doors into their equipment to allow for eavesdropping by the Chinese government and military. Both companies have denied collaborating with the Chinese government, but the allegations have eliminated the companies’ hopes for significant business growth in the United States. After an investigation last year, the House Intelligence Committee concluded that [government agencies should be barred](#) from doing business with Huawei and ZTE, and that American companies should avoid buying their equipment.

Some foreign governments and companies have also said that they would not rely on the Chinese companies' equipment out of security concerns. Last year, Australia barred Huawei from bidding on contracts in Australia's \$38 billion national broadband network. And this year, as part of its effort to acquire Sprint Nextel, SoftBank of Japan pledged that it would not use Huawei equipment in Sprint's cellphone network.

Claire Cain Miller contributed reporting.

A version of this article appears in print on September 7, 2013, on page A14 of the New York edition with the headline: Legislation Seeks to Bar N.S.A. Tactic In Encryption.

(Washington, D.C.) – U.S. Rep. Rush Holt (NJ-12) today released the following statement in response to reports in [The New York Times](#) and [The Guardian](#) that the National Security Agency has weakened or broken the online encryption relied upon by hundreds of millions of Americans to protect their private data.

According to news reports, the NSA has covertly weakened the computer security protocols that American citizens and businesses rely on. The NSA has surreptitiously obtained the encryption keys used by major corporations to protect online data. And the NSA has demanded that manufacturers insert “back doors” into computer hardware to enable secret government eavesdropping.

Holt has introduced legislation, the [Surveillance State Repeal Act](#) , that would outlaw many of the activities described in these reports.

“These reports, if true, show that the NSA, in its zeal to spy, may be leaving Americans less secure.

“It’s as though the NSA had secretly copied the keys to your home. Worse, it’s as though the NSA had prohibited manufacturers from even making secure locks – all while assuring the public that of course their belongings were safe.

“The NSA has long taken part in setting standards for communications security. Its role in this activity has been respected. But it now appears that the NSA may have abused this role to make Americans’ communications more vulnerable.

“Although the NSA’s goal may have been to allow the U.S. government to spy on communications, by introducing vulnerabilities into widely used computer hardware and software, the NSA would be rendering all communications vulnerable to criminals and foreign intelligence agencies. Anyone can walk through an open door if they can find it.

“Further, these revelations raise questions for American technology companies. What foreign business would buy products that have been deliberately rendered insecure?

“Earlier this year I introduced legislation, the Surveillance State Repeal Act, that would make it illegal for the NSA to insert ‘back doors’ into computer hardware or software. These revelations give that proposal new urgency.

“Our constitution protects Americans against unreasonable searches and seizures. I believe that includes a right for innocent citizens to encrypt their data securely.”

(Washington, DC) Today Rep. Rush Holt introduced legislation to repeal federal surveillance laws that the government abused by collecting personal information on millions of Americans in violation of the Constitution, as revealed by a federal whistleblower and multiple media outlets last month.

"As we now know, the National Security Agency and the Federal Bureau of Investigation have been collecting the personal communications of literally millions of innocent Americans for no legitimate reason," said Holt. "Instead of using these powers to zero in on the tiny number of real terrorist threats we face, the executive branch turned these surveillance powers against the American people as a whole. My legislation would put a stop to that right now."

Holt's bill, the "Surveillance State Repeal Act", would repeal the PATRIOT Act and the FISA Amendments Act, each of which contains provisions that allowed the dragnet surveillance. The bill would reinstate a uniform probable cause-based warrant standard for surveillance requests, and prohibit the federal government from forcing technology companies from building in hardware or software "back doors" to make it easier for the government to spy on the public. Additional features of the bill include the true legal protections for national security whistleblowers, as well as changes to the Foreign Intelligence Surveillance Court to give it greater expertise in reviewing and challenging executive branch applications for surveillance operations.

"The executive branch's groundless mass surveillance of Americans has turned our conception of liberty on its head. My legislation would restore the proper constitutional balance and ensure our people are treated as citizens first, not suspects."

For a more detailed summary of the provisions, click [here](#) .

For the text of the legislation, click [here](#) .

Summary of the Surveillance State Repeal Act

The Surveillance State Repeal Act would:

1. Repeal the PATRIOT Act (which contains the telephone metadata harvesting provision).
2. Repeal the FISA Amendments Act (which contains the email harvesting provision).
3. Ensure that any FISA collection against a US Person takes place only pursuant to a valid warrant based on probable cause (which was the original FISA standard from 1978 to 2001).
4. Retain the ability for government surveillance capabilities to be targeted against a specific natural person, regardless of the type of communications method(s) or device(s) being used by the subject of the surveillance.
5. Retains provisions in current law dealing with the acquisition of intelligence information involving weapons of mass destruction from entities not composed primarily of U.S. Persons.
6. Prohibit the government from mandating that electronic device or software manufacturers build in so-called “back doors” to allow the government to bypass encryption or other privacy technology built into said hardware and/or software.
7. Increase the terms of judges on the Foreign Intelligence Surveillance Court (FISC) from seven to ten years and allow their reappointment.
8. Mandate that the FISC utilize technologically competent Special Masters (technical and legal experts) to help determine the veracity of government claims about privacy, minimization and collection capabilities employed by the US government in FISA applications.
9. Mandate that the Government Accountability Office (GAO) regularly monitor such domestic surveillance programs for compliance with the law, including responding to Member requests for investigations and whistleblower complaints of wrongdoing.

.....
(Original Signature of Member)

113TH CONGRESS
1ST SESSION

H. R.

To repeal the USA PATRIOT Act and the FISA Amendments Act of 2008,
and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. HOLT introduced the following bill; which was referred to the Committee
on _____

A BILL

To repeal the USA PATRIOT Act and the FISA
Amendments Act of 2008, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Surveillance State Re-
5 peal Act”.

6 **SEC. 2. REPEAL OF USA PATRIOT ACT.**

7 The USA PATRIOT Act (Public Law 107–56) is re-
8 pealed, and the provisions of law amended or repealed by

1 such Act are restored or revived as if such Act had not
2 been enacted.

3 **SEC. 3. REPEAL OF THE FISA AMENDMENTS ACT OF 2008.**

4 (a) REPEAL.—The FISA Amendments Act of 2008
5 (Public Law 110–261; 122 Stat. 2477) is repealed, and
6 the provisions of law amended or repealed by such Act
7 are restored or revived as if such Act had not been en-
8 acted.

9 (b) EXCEPTION.—Subsection (a) of this Act shall not
10 apply to sections 103 and 110 of the FISA Amendments
11 Act of 2008 (Public Law 110–261; 122 Stat. 2477).

12 **SEC. 4. TERMS OF JUDGES ON FOREIGN INTELLIGENCE**
13 **SURVEILLANCE COURT; REAPPOINTMENT;**
14 **SPECIAL MASTERS.**

15 (a) TERMS; REAPPOINTMENT.—Section 103(d) of the
16 Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.
17 1803(d)) is amended—

18 (1) by striking “maximum of seven” and insert-
19 ing “maximum of ten”; and

20 (2) by striking “and shall not be eligible for re-
21 designation”.

22 (b) SPECIAL MASTERS.—Section 103(f) of such Act,
23 as amended by section 3 of this Act, is further amended
24 by adding at the end the following new paragraph:

25 “(4) SPECIAL MASTERS.—

1 **SEC. 6. ADDITIONAL PROVISIONS FOR COLLECTIONS**
2 **UNDER THE FOREIGN INTELLIGENCE SUR-**
3 **VEILLANCE ACT OF 1978.**

4 (a) IN GENERAL.—Title VII of the Foreign Intel-
5 ligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.),
6 as amended by section 3 of this Act, is further amended
7 to read as follows:

8 **“TITLE VII—ADDITIONAL**
9 **PROVISIONS**

10 **“SEC. 701. WARRANT REQUIREMENT.**

11 “Notwithstanding any other provision of this Act, no
12 information relating to a United States person may be ac-
13 quired pursuant to this Act without a valid warrant based
14 on probable cause.”.

15 (b) TABLE OF CONTENTS AMENDMENTS.—The table
16 of contents in the first section of the Foreign Intelligence
17 Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as
18 amended by section 3 of this Act, is further amended by
19 striking the items relating to title VII and section 701 and
20 inserting the following new items:

“TITLE VII—ADDITIONAL PROVISIONS

“701. Warrant requirement.”.

21 **SEC. 7. ENCRYPTION AND PRIVACY TECHNOLOGY OF ELEC-**
22 **TRONIC DEVICES AND SOFTWARE.**

23 Notwithstanding any other provision of law, the Fed-
24 eral Government shall not mandate that the manufacturer

1 of an electronic device or software for an electronic device
2 build into such device or software a mechanism that allows
3 the Federal Government to bypass the encryption or pri-
4 vacy technology of such device or software.

5 **SEC. 8. GAO COMPLIANCE EVALUATIONS.**

6 (a) IN GENERAL.—The Comptroller General of the
7 United States shall annually evaluate compliance by the
8 Federal Government with the provisions of the Foreign In-
9 telligence Surveillance Act of 1978 (50 U.S.C. 1801 et
10 seq.).

11 (b) REPORT.—The Comptroller General shall annu-
12 ally submit to Congress a report containing the results of
13 the evaluation conducted under subsection (a).

14 **SEC. 9. WHISTLEBLOWER COMPLAINTS.**

15 (a) AUTHORIZATION TO REPORT COMPLAINTS OR IN-
16 FORMATION.—An employee of or contractor to an element
17 of the intelligence community that has knowledge of the
18 programs and activities authorized by the Foreign Intel-
19 ligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)
20 may submit a covered complaint—

21 (1) to the Comptroller General of the United
22 States;

23 (2) to the Permanent Select Committee on In-
24 telligence of the House of Representatives;

1 (3) to the Select Committee on Intelligence of
2 the Senate; or

3 (4) in accordance with the process established
4 under section 103H(k)(5) of the National Security
5 Act of 1947 (50 U.S.C. 3033(k)(5)).

6 (b) INVESTIGATIONS AND REPORTS TO CONGRESS.—
7 The Comptroller General shall investigate a covered com-
8 plaint submitted pursuant to subsection (b)(1) and shall
9 submit to Congress a report containing the results of the
10 investigation.

11 (c) COVERED COMPLAINT DEFINED.—In this sec-
12 tion, the term “covered complaint” means a complaint or
13 information concerning programs and activities authorized
14 by the Foreign Intelligence Surveillance Act of 1978 (50
15 U.S.C. 1801 et seq.) that an employee or contractor rea-
16 sonably believes is evidence of—

17 (1) a violation of any law, rule, or regulation;
18 or

19 (2) gross mismanagement, a gross waste of
20 funds, an abuse of authority, or a substantial and
21 specific danger to public health or safety.

1 **SEC. 10. PROHIBITION ON INTERFERENCE WITH REPORT-**
2 **ING OF WASTE, FRAUD, ABUSE, OR CRIMINAL**
3 **BEHAVIOR.**

4 (a) **IN GENERAL.**—Notwithstanding any other provi-
5 sion of law, an officer or employee of an element of the
6 intelligence community shall be subject to administrative
7 sanctions, up to and including termination, for taking re-
8 taliatory action against an employee of or contractor to
9 an element of the intelligence community who seeks to dis-
10 close or discloses covered information to—

11 (1) the Comptroller General;

12 (2) the Permanent Select Committee on Intel-
13 ligence of the House of Representatives;

14 (3) the Select Committee on Intelligence of the
15 Senate; or

16 (4) the Office of the Inspector General of the
17 Intelligence Community.

18 (b) **DEFINITIONS.**—In this section:

19 (1) **COVERED INFORMATION.**—The term “cov-
20 ered information” means any information (including
21 classified or sensitive information) that an employee
22 or contractor reasonably believes is evidence of—

23 (A) a violation of any law, rule, or regula-
24 tion; or

1 (B) gross mismanagement, a gross waste
2 of funds, an abuse of authority, or a substantial
3 and specific danger to public health or safety.

4 (2) INTELLIGENCE COMMUNITY.—The term
5 “intelligence community” has the meaning given the
6 term in section 3 of the National Security Act of
7 1947 (50 U.S.C. 3003).