SB

13

<TARGET><BILL>SB 13</BILL><SUBJECT>SB
13</SUBJECT><COMM>SCRA29</COMM></TARGET>

ALASKA STATE LEGISLATURE

Session

State Capitol, Rm. 419
Juneau, AK 99801
(907) 465-2435
Fax: (907) 465-6615

Interim

716 W. 4th Ave, Ste. 409
Anchorage, AK 99501
(907) 269-0120
Fax: (907) 269-0122

Senator.Bill.Wielechowski@akleg.gov

Resources Committee

State Affairs Committee

Joint Armed Services Committee

Judiciary Committee

SENATOR BILL WIELECHOWSKI

MEMORANDUM

3 February 2015

TO: Senator Click Bishop, Chair
Senate Community and Regional Affairs Committee

From: Senator Bill Wielechowski

SUBJ: Hearing Request for SB 13- Warrantless Search of Electronic Data

I am writing to request a hearing on Senate Bill 13: Warrantless Search of Electronic Data.

This bill would protect Alaskans' civil liberties by barring state and municipal agencies from cooperating with federal authorities seeking electronic records on an Alaskan resident, unless the federal government first obtains a warrant.

Included in the bill packet:

- SB 13- Sponsor Statement
- SB 13- Version A
- SB 13- Supporting Documents
  - Support letter from Tenth Amendment Center
  - Relevant News Articles

If you have any questions please feel free to contact me or my staff Sarah Evans at 465-2435. Thank you for your consideration.

ALASKA STATE LEGISLATURE

Session

State Capitol, Rm. 419
Juneau, AK 99801
(907) 465-2435
Fax: (907) 465-6615

Interim

716 W. 4th Ave, Ste. 409
Anchorage, AK 99501
(907) 269-0120
Fax: (907) 269-0122

Senator.Bill.Wielechowski@akleg.gov

Resources Committee

State Affairs Committee

Joint Armed Services Committee

Judiciary Committee

SENATOR BILL WIELECHOWSKI

Sponsor Statement

Senate Bill 13- Warrantless Search of Electronic Data

This bipartisan bill would protect Alaskans' civil liberties by barring state and municipal agencies from cooperating with federal authorities seeking electronic records on an Alaskan resident, unless the federal government first obtains a warrant.

The bill seeks to limit unconstitutional overreach by the National Security Agency (NSA). Many legal scholars believe the mass surveillance activities secretly conducted by the NSA violate the Fourth Amendment to the Constitution's ban on unreasonable searches and seizures. At least one federal judge has ruled that the broad and untargeted surveillance is unconstitutional, calling it "almost Orwellian."

The spy agency has been compiling phone, text, email and Internet data on American citizens within the United States. In many cases, the agency obtains the data without a warrant and with the help of cooperating entities. This bill would ban such cooperation by state agencies and local governments in Alaska.

Legislation must defend the constitutional rights of Alaskans and Americans. Widespread, indiscriminant eavesdropping on the private communications of innocent Americans violates one of our most cherished constitutional rights, and no Alaskan should stand for it.

I hope you will join me in protecting Alaskans' most basic and essential rights.

SENATE BILL NO. 13

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-NINTH LEGISLATURE - FIRST SESSION

BY SENATOR WIELECHOWSKI

Introduced: 1/21/15
Referred: Community and Regional Affairs, Judiciary

A BILL

FOR AN ACT ENTITLED

"An Act prohibiting the state and municipalities from using assets to assist a federal agency in collecting certain telephone records or electronic data without a warrant; prohibiting the state from cooperating with a federal agency in collecting certain telephone records or electronic data without a warrant; and providing for an effective date."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

*** Section 1.** AS 29.10.200 is amended by adding a new paragraph to read:

(65) AS 29.35.081 (collection or use of telephone records or electronic data obtained without a warrant).

*** Sec. 2.** AS 29.35 is amended by adding a new section to read:

Sec. 29.35.081. Prohibition against cooperation with federal agencies engaged in collection of telephone records or electronic data. (a) A municipality or an agent of a municipality may not

(1) assist, cooperate with, or participate with a federal agency in the collection of

(A) electronic data under a federal statute, regulation, rule, or order when the collection of electronic data is undertaken without a search warrant that particularly describes the person, place, and thing to be searched or seized; or

(B) telephone records under a federal statute, regulation, rule, or order when the collection of the telephone records is undertaken without a search warrant that particularly describes the person, place, and thing to be searched or seized, or in another manner that is inconsistent with state law; or

(2) use, in a criminal investigation or prosecution, records or data that are provided by a federal agency or an officer or employee of a federal agency that were collected by the federal agency without a search warrant or in another manner inconsistent with state law as described in (1) of this subsection.

(b) In this section, "electronic data" includes electronic mail and text messages.

* **Sec. 3.** AS 44.99.040(a) is amended to read:

(a) A state or municipal agency may not use or authorize the use of an asset to implement or aid in

(1) the implementation of a requirement of

(A) [(1)] an order of the President of the United States, a federal regulation, or a law enacted by the United States Congress that is applied to

(i) [(A)] infringe on a person's right, under the Second Amendment to the Constitution of the United States, to keep and bear arms;

(ii) [(B)] deny a person a right to due process, or a protection of due process, that would otherwise be available to the person under the Constitution of the State of Alaska or the Constitution of the United States; or

(B) [(2)] P.L. 109-13, Division B (REAL ID Act of 2005)**;**

(2) the collection by a federal agency of electronic data without a search warrant; in this paragraph, "electronic data" includes electronic mail and text messages; or

(3) the collection by a federal agency of telephone records without a search warrant, unless the records are collected in a manner consistent with state law.

* **Sec. 4.** AS 44.99 is amended by adding a new section to article 1 to read:

Sec. 44.99.050. Prohibition against cooperation with federal agencies engaged in collection of telephone records or electronic data. (a) The state or an agent of the state may not

(1) assist, cooperate with, or participate with a federal agency in the collection of

(A) electronic data under a federal statute, regulation, rule, or order when the collection of electronic data is undertaken without a search warrant that particularly describes the person, place, and thing to be searched or seized; or

(B) telephone records under a federal statute, regulation, rule, or order when the collection of the telephone records is undertaken without a search warrant that particularly describes the person, place, and thing to be searched or seized, or in another manner that is inconsistent with state law; or

(2) use, in a criminal investigation or prosecution, records or data that are provided by a federal agency or an officer or employee of a federal agency that were collected by the federal agency without a search warrant or in another manner inconsistent with state law as described in (1) of this subsection.

(b) In this section, "electronic data" includes electronic mail and text messages.

* **Sec. 5.** This Act takes effect immediately under AS 01.10.070(c).

29-LS0006\W
Strasbaugh
3/19/15

CS FOR SENATE BILL NO. 13( )

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-NINTH LEGISLATURE - FIRST SESSION

BY

Offered:
Referred:

Sponsor(s): SENATORS WIELECHOWSKI, Gardner, Dunleavy

A BILL

FOR AN ACT ENTITLED

"An Act prohibiting the state and municipalities from using assets to assist a federal data collection and surveillance agency in collecting certain telephone records or electronic data without a warrant; prohibiting the state from cooperating with a federal data collection and surveillance agency in collecting certain telephone records or electronic data without a warrant; and providing for an effective date."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

* **Section 1.** AS 29.10.200 is amended by adding a new paragraph to read:

(65) AS 29.35.081 (collection or use of telephone records or electronic data obtained without a warrant).

* **Sec. 2.** AS 29.35 is amended by adding a new section to read:

Sec. 29.35.081. Prohibition against cooperation with federal data collection and surveillance agencies engaged in collection of telephone records or electronic data. (a) A municipality or an agent of a municipality may not

(1) assist, cooperate with, or participate with a federal data collection and surveillance agency in the collection of

(A) electronic data under a federal statute, regulation, rule, or order when the collection of electronic data is undertaken without a search warrant that particularly describes the person, place, and thing to be searched or seized; or

(B) telephone records under a federal statute, regulation, rule, or order when the collection of the telephone records is undertaken without a search warrant that particularly describes the person, place, and thing to be searched or seized, or in another manner that is inconsistent with state law; or

(2) use, in a criminal investigation or prosecution, records or data that are provided by a federal data collection and surveillance agency or an officer or employee of a federal data collection and surveillance agency that were collected by the federal data collection and surveillance agency without a search warrant or in another manner inconsistent with state law as described in (1) of this subsection.

(b) In this section,

(1) "electronic data" includes electronic mail and text messages;

(2) "federal data collection and surveillance agency" has the meaning given in AS 44.99.040(b).

* **Sec. 3.** AS 44.99.040(a) is amended to read:

(a) A state or municipal agency may not use or authorize the use of an asset to implement or aid in

(1) the implementation of a requirement of

(A) [(1)] an order of the President of the United States, a federal regulation, or a law enacted by the United States Congress that is applied to

(i) [(A)] infringe on a person's right, under the Second Amendment to the Constitution of the United States, to keep and bear arms;

(ii) [(B)] deny a person a right to due process, or a protection of due process, that would otherwise be available to the

person under the Constitution of the State of Alaska or the Constitution of the United States; or

(B) [(2)] P.L. 109-13, Division B (REAL ID Act of 2005)**;**

(2) the collection by a federal data collection and surveillance agency of electronic data without a search warrant; or

(3) the collection by a federal data collection and surveillance agency of telephone records without a search warrant, unless the records are collected in a manner consistent with state law.

* **Sec. 4.** AS 44.99.040(b) is amended by adding new paragraphs to read:

(3) "electronic data" includes electronic mail and text messages;

(4) "federal data collection and surveillance agency" means a federal agency that is involved in the routine surveillance or involuntary bulk collection and storage of telephone records or electronic data concerning United States citizens and that claims the legal authority to collect and store telephone records and electronic data concerning United States citizens in bulk.

* **Sec. 5.** AS 44.99 is amended by adding a new section to article 1 to read:

Sec. 44.99.050. Prohibition against cooperation with federal data collection and surveillance agencies engaged in collection of telephone records or electronic data. (a) The state or an agent of the state may not

(1) assist, cooperate with, or participate with a federal data collection and surveillance agency in the collection of

(A) electronic data under a federal statute, regulation, rule, or order when the collection of electronic data is undertaken without a search warrant that particularly describes the person, place, and thing to be searched or seized; or

(B) telephone records under a federal statute, regulation, rule, or order when the collection of the telephone records is undertaken without a search warrant that particularly describes the person, place, and thing to be searched or seized, or in another manner that is inconsistent with state law; or

(2) use, in a criminal investigation or prosecution, records or data that are provided by a federal data collection and surveillance agency or an officer or

employee of a federal data collection and surveillance agency that were collected by the federal data collection and surveillance agency without a search warrant or in another manner inconsistent with state law as described in (1) of this subsection.

(b) In this section, "electronic data" and "federal data collection and surveillance agency" have the meanings given in AS 44.99.040(b).

* **Sec. 6.** This Act takes effect immediately under AS 01.10.070(c).

Fiscal Note

State of Alaska
2015 Legislative Session

Bill Version: SB 13
Fiscal Note Number:
() Publish Date:

Identifier: SB013-DOA-ETS-03-13-15
Title: WARRANTLESS SEARCH OF ELECTRONIC DATA
Sponsor: WIELECHOWSKI
Requester: Senate Community and Regional Affairs

Department: Department of Administration
Appropriation: Enterprise Technology Services
Allocation: Enterprise Technology Services
OMB Component Number: 2082

Expenditures/Revenues

Note: Amounts do not include inflation unless otherwise noted below. (Thousands of Dollars)

	FY2016 Appropriation Requested	Included in Governor's FY2016 Request	Out-Year Cost Estimates				
OPERATING EXPENDITURES	**FY 2016**	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**
Personal Services							
Travel							
Services							
Commodities							
Capital Outlay							
Grants & Benefits							
Miscellaneous							
Total Operating	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Fund Source (Operating Only)

None							
Total	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Positions

Full-time							
Part-time							
Temporary							

Change in Revenues							

Estimated SUPPLEMENTAL (FY2015) cost: 0.0 *(separate supplemental appropriation required)*
(discuss reasons and fund source(s) in analysis section)

Estimated CAPITAL (FY2016) cost: 0.0 *(separate capital appropriation required)*
(discuss reasons and fund source(s) in analysis section)

ASSOCIATED REGULATIONS

Does the bill direct, or will the bill result in, regulation changes adopted by your agency? No
If yes, by what date are the regulations to be adopted, amended or repealed?

Why this fiscal note differs from previous version:

Not applicable, initial version of bill.

Prepared By: Jim Bates, Director — Phone: (907)465-2220
Division: Enterprise Technology Services — Date: 03/13/2015 08:00 AM
Approved By: Sheldon Fisher, Commissioner — Date: 03/13/15
Agency: Department of Administration

STATE OF ALASKA
2015 LEGISLATIVE SESSION

BILL NO. SB 13

Analysis

Enterprise Technology Services (ETS) is the primary provider of email, telephone and other communication services for executive branch state agencies. ETS currently conducts appropriate searches of electronic data within its operating budget. So long as the necessary legal requirements are met -- specifically that if a warrant is necessary, a warrant has been acquired -- this division will conduct the searches.

As this bill reinforces a current practice for ETS there would be no change to service delivery, should this bill be enacted into law, and therefore ETS submits a zero fiscal note.

APOA
ALASKA PEACE OFFICERS ASSOCIATION

Making a Difference in the Last Frontier

February 2, 2015

The Honorable Bill Wielechowski
Alaska State Senate
State Capitol Rm 419
120 4th Street, Mail Stop: 3100
Juneau AK, 99801-1185

Dear Senator Wielechowski:

On behalf of the Alaska Peace Officers Association (APOA), I am writing with concerns regarding SB13, "An Act prohibiting the state and municipalities from using assets to assist a federal agency in collecting certain telephone records or electronic data without a warrant; prohibiting the state from cooperating with a federal agency in collecting certain telephone records or electronic data without a warrant; and providing for an effective date."

The APOA Board of Directors recently reviewed this proposed legislation and unanimously opposes this bill. While we are sensitive to our state citizens' rights, we believe passage of this bill would reduce cooperation between law enforcement agencies and negatively impact the work of law enforcement throughout the state. It is common practice for local/state officers to share legally seized information with federal partners as often federal charges become more appropriate due to the scope and impact of the crime. This bill would be especially detrimental in this current age of reduced law enforcement budgets and staffing. During this fiscally challenging era, it is crucial all levels of law enforcement be provided the ability to share resources and cooperate effectively to protect the citizens and resources of the state of Alaska.

Please contact the APOA office in Anchorage at 277-0515, if there is anything our organization can do to assist you in your work for our state.

Sincerely,

Brad Johnson
State President

) Box 240106
Anchorage, AK 99524
(907)277-0515
(907)272-5355 fax
email: apoa@gci.net
www.apoaonline.org

ANCHORAGE POLICE DEPARTMENT

4501 Elmore Road • Anchorage, Alaska 99507-1599
Telephone (907) 786-8500

Dan Sullivan, Mayor

Service since 1921

March 24, 2015

The Honorable Bill Wielechowski
State Capitol Room 419
Juneau, AK 99801

Dear Senator Wielechowski:

The Anchorage Police Department appreciates your commitment to preserving the constitutional rights of Alaska citizens, as reflected in Senate Bill 13. While we, too, are committed to the rights of Alaskan and the residents of Anchorage, we are, unfortunately, unable to support this bill.

We would never intentionally acquire information in unauthorized ways, nor would we assist another agency in doing so. But the language in this bill could potentially prevent us from cooperating in investigative activities that are not unauthorized. Information is shared between many enforcement and/or security entities; not all of it pertains to domestic or international terrorism. Sometimes these agencies stumble upon important information concerning common (but serious) crime. Of particular concern to us is the bill's impact on our ability to work cyber, child pornography, and drug cases, which often involve close cooperation with federal agencies.

We believe there are potential unintended consequences to SB13, but we do appreciate your interest in law enforcement and your dedication to the protection of our citizens.

Thank you.

Sincerely,

Mark T. Mew
Chief of Police

Alaska Association of Chiefs of Police

March 6, 2015

The Honorable Bill Wielechowski
State Capitol Room 419
Juneau AK, 99801
Senator.Bill.Wielechowski@akleg.gov

Dear Senator Wielechowski,

In my capacity as President of the Alaska Association of Chiefs of Police, I am writing to express our opposition of Senate Bill 13 "*An Act prohibiting the state and municipalities from using assets to assist a federal agency in collecting certain telephone records or electronic data without a warrant; prohibiting the state from cooperating with a federal agency in collecting certain telephone records or electronic data without a warrant; and providing for an effective date.*" Our Association is comprised of more than 100 law enforcement executives from all across Alaska, and while we understand that this bill was well intentioned, we are unable to lend our support to it. Cooperation between law enforcement agencies is the foundation of our profession, and often our lives and those of the public may depend on the support we get from officers of other agencies. While we will always follow the law and strive to protect the rights of the public, we cannot support legislation which serves to sever or limit our relationships with fellow officers who are adhering to federal law. It is crucial that state, local and federal agencies maintain the ability to share resources cooperate effectively to protect the citizens of Alaska.

We want to thank you for your dedication to the people of Alaska and your continued interest in law enforcement issues. We encourage you to reach out to us by contacting our executive director, Kalie Klaysmat at kalie.klaysmat@aacop.org should you wish to further discuss this or any other matter.

Sincerely,

Deputy Chief Brad Johnson, President

327 E FIREWEED LANE, SUITE 101, ANCHORAGE, AK 99503-2110

How the NSA's Domestic Spying Program Works

The NSA's domestic spying program, known in official government documents as the "President's Surveillance Program," ("The Program") was implemented by President George W. Bush shortly after the attacks on September 11, 2001. The US Government still considers the Program officially classified, but a tremendous amount of information has been exposed by various whistleblowers, admitted to by government officials during Congressional hearings and with public statements, and reported on in investigations by major newspaper across the country.

Our NSA Domestic Spying Timeline has a full list of important dates, events, and reports, but we also want to explain—to the extent we understand it—the full scope of the Program and how the government has implemented it.

In the weeks after 9/11, President Bush authorized the National Security Agency (NSA) to conduct a range of surveillance activities inside the United States, which had been barred by law and agency policy for decades. When the NSA's spying program was first exposed by the *New York Times* in 2005, President Bush admitted to a small aspect of the program—what the administration labeled the "Terrorist Surveillance Program"—in which the NSA monitored, without warrants, the communications of between 500-1000 people inside the US with suspected connections to Al Qaeda.

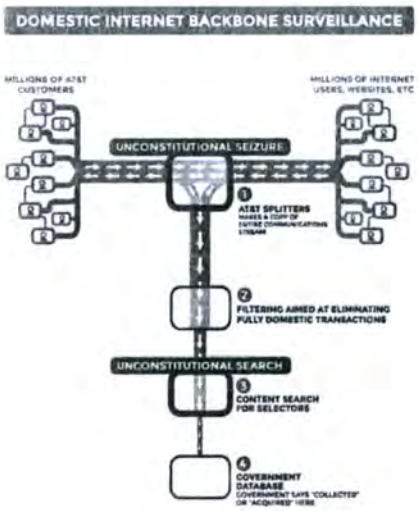
But other aspects of the Program were aimed not just at targeted individuals, but perhaps millions of innocent Americans never suspected of a crime.

Details of Every American's Call History

First, the government convinced the major telecommunications companies in the US, including AT&T, MCI, and Sprint, to hand over the "call-detail records" of their customers. According to an investigation by *USA Today*, this included

"customers' names, street addresses, and other personal information." In addition, the government received "detailed records of calls they made—across town or across the country—to family members, co-workers, business contacts and others."

A person familiar with the matter told *USA Today* that the agency's goal was "to create a database of every call ever made" within the nation's borders. All of this was done without a warrant or any judicial oversight.



Real Time Access to Phone and Internet Traffic

Second, the same telecommunications companies also allowed the NSA to install sophisticated communications surveillance equipment in secret rooms at key telecommunications facilities around the country. This equipment gave the NSA unfettered access to large streams of domestic and international communications in real time—what amounted to at least 1.7 billion emails a day, according to the Washington Post. The NSA could then data mine and analyze this traffic for suspicious key words, patterns and connections. Again, all of this was done without a warrant in violation of federal law and the Constitution.

The Technology That Made It Possible

But how did the government accomplish this task and how do we know? In addition to investigative reports by the *New York Times* and others, AT&T technician turned whistleblower Mark Klein provided EFF with eyewitness

testimony and documents describing one such secret room located at AT&T's Folsom Street facility in San Francisco, California.

It works like this: when you send an email or otherwise use the internet, the data travels from your computer, through telecommunication companies' wires and fiber optics networks, to your intended recipient. To intercept these communications, the government installed devices known as "fiber-optic splitters" in many of the main telecommunication junction points in the United States (like the AT&T facility in San Francisco). These splitters make exact copies of the data passing through them: then, one stream is directed to the government, while the other stream is directed to the intended recipients.

The Klein documents reveal the specific equipment installed at the AT&T facility and the processing power of the equipment within the secret rooms. One type of machine installed is a Narus Semantic Traffic Analyzer, a powerful tool for deep packet inspection. Narus has continually refined their capabilities and—as of the mid-2000s—each Narus machine was capable of analyzing 10 gigabits of IP packets, and 2.5 gigabits of web traffic or email, per second. It is likely even more powerful today. The Narus machine can then reconstruct the information transmitted through the network and forward the communications to a central location for storage and analysis.

In a declaration in our lawsuit, thirty-year NSA veteran William Binney estimates that "NSA installed no few than ten and possibly in excess of twenty intercept centers within the United States." Binney also estimates NSA has collected "between 15 and 20 trillion" transactions over the past 11 years.

In April 2012, long-time national security author James Bamford reported NSA is spending $2 billion to construct a data center in a remote part of Utah to house the information it has been collecting for the past decade. "Flowing through its servers and routers and stored in near-bottomless databases," Bamford wrote, "will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital 'pocket litter.'"

The Utah data center will be fully operational in September 2013.

The New York Times

December 16, 2013

Judge Questions Legality of N.S.A. Phone Records

By CHARLIE SAVAGE

WASHINGTON — A federal district judge ruled on Monday that the National Security Agency program that is systematically keeping records of all Americans' phone calls most likely violates the Constitution, describing its technology as "almost Orwellian" and suggesting that James Madison would be "aghast" to learn that the government was encroaching on liberty in such a way.

The judge, Richard J. Leon of Federal District Court for the District of Columbia, ordered the government to stop collecting data on the personal calls of the two plaintiffs in the case and to destroy the records of their calling history. But Judge Leon, appointed to the bench in 2002 by President George W. Bush, stayed his injunction "in light of the significant national security interests at stake in this case and the novelty of the constitutional issues," allowing the government time to appeal it, which he said could take at least six months.

"I cannot imagine a more 'indiscriminate' and 'arbitrary' invasion than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval," Judge Leon wrote in a 68-page ruling. "Surely, such a program infringes on 'that degree of privacy' that the founders enshrined in the Fourth Amendment," which prohibits unreasonable searches and seizures.

Andrew Ames, a Justice Department spokesman, said government lawyers were studying the decision, but he added: "We believe the program is constitutional as previous judges have found."

The case is the first in which a federal judge who is not on the Foreign Intelligence Surveillance Court, which authorized the once-secret program, has examined the bulk data collection on behalf of someone who is not a criminal defendant. The Justice Department has said that 15 separate judges on the surveillance court have held on 35 occasions that the calling data program is legal.

It also marks the first successful legal challenge brought against the program since it was revealed in June after leaks by the former N.S.A. contractor Edward J. Snowden.

In a statement from Moscow, where he has obtained temporary asylum, Mr. Snowden praised the ruling.

"I acted on my belief that the N.S.A.'s mass surveillance programs would not withstand a constitutional challenge, and that the American public deserved a chance to see these issues determined by open courts," Mr. Snowden said in his statement. It was distributed by Glenn Greenwald, a journalist who received leaked documents from Mr. Snowden and wrote the first article about the bulk data collection. "Today, a secret program authorized by a secret court was, when exposed to the light of day, found to violate Americans' rights," the statement said. "It is the first of many."

The case was brought by several plaintiffs led by Larry Klayman, a conservative legal activist. Mr. Klayman, who represented himself and the other plaintiffs, said in an interview on Monday that he was seeking to turn the case into a class action on behalf of all Americans. "I'm extremely gratified that Judge Leon had the courage to make this ruling," he said. "He is an American hero."

Mr. Klayman argued that he had legal standing to challenge the program in part because, he contended, the government had sent inexplicable text messages to his clients on his behalf; at a hearing, he told the judge, "I think they are messing with me."

The judge portrayed that claim as "unusual" but looked past it, saying Mr. Klayman and his co-plaintiff instead had standing because it was highly likely, based on the government's own description of the program as a "comprehensive metadata database," that the N.S.A. collected data about their phone calls along with everyone else's.

Similar legal challenges to the N.S.A. program, including by the American Civil Liberties Union and the advocacy group Electronic Frontier Foundation, are at earlier stages in the courts. Last month, the Supreme Court declined to hear an unusual challenge to the program by the Electronic Privacy Information Center, which had sought to bypass lower courts.

The ruling on Monday comes as several government panels are developing recommendations on whether to keep, restructure or scrap the bulk data collection program, and as Congress debates competing bills over the program's future.

Though long and detailed, Judge Leon's ruling is not a final judgment on the program, but rather a preliminary injunction to stop the collection of data about the plaintiffs while they pursued their case.

He also wrote that he had "serious doubts about the efficacy" of the program, saying that the government had failed to cite "a single instance in which analysis of the N.S.A.'s bulk metadata collection actually stopped an imminent attack, or otherwise aided the government in achieving any objective that was time-sensitive."

Judge Leon rejected the Obama administration's argument that a 1979 case, Smith v. Maryland, had established there are no Fourth Amendment protections for call metadata — information like the numbers dialed and the date, time and duration of calls, but not their content. The 1979 case, which involved collecting information about a criminal defendant's calls, helped establish the principle that people do not have a reasonable expectation of privacy for information they have exposed to a third party, like the phone company, which knows about their calls.

The surveillance court, which issues secret rulings after hearing arguments from only the Justice Department and without opposing lawyers, has maintained that the 1979 decision is a controlling precedent that shields the N.S.A. call data program from Fourth Amendment review. But Judge Leon, citing the scope of the program and the evolving role of phones and technology, distinguished the bulk collection from the 34-year-old case.

Last month, a federal judge declined to grant a new trial to several San Diego men convicted of sending money to a terrorist group in Somalia. Government officials have since acknowledged that investigators became interested in them because of the call records program. Citing Smith v. Maryland, the judge said the defendants had "no legitimate expectation of privacy" over their call data.

David Rivkin, a White House lawyer in the administration of the elder President George Bush, criticized Judge Leon's reasoning.

"Smith v. Maryland is the law of the land," Mr. Rivkin said. "It is not for a District Court judge to question the continuing validity of a Supreme Court precedent that is exactly on point."

Judge Leon also pointed to a landmark privacy case decided by the Supreme Court in 2012 that held it was unconstitutional for the police to use a GPS tracking device to monitor a suspect's public movements without a warrant.

Although the court decided the case on narrow grounds, five of the nine justices separately questioned whether the 1979 precedent was still valid in an era of modern technology, which enables long-term, automated collection of information.

The New York Times http://nyti.ms/1dWj6P3

POLITICS

Watchdog Report Says N.S.A. Program Is Illegal and Should End

By CHARLIE SAVAGE JAN. 23, 2014

WASHINGTON — An independent federal privacy watchdog has concluded that the National Security Agency's program to collect bulk phone call records has provided only "minimal" benefits in counterterrorism efforts, is illegal and should be shut down.

The findings are laid out in a 238-page report, scheduled for release by Thursday and obtained by The New York Times, that represent the first major public statement by the Privacy and Civil Liberties Oversight Board, which Congress made an independent agency in 2007 and only recently became fully operational.

The report is likely to inject a significant new voice into the debate over surveillance, underscoring that the issue was not settled by a high-profile speech President Obama gave last week. Mr. Obama consulted with the board, along with a separate review group that last month delivered its own report about surveillance policies. But while he said in his speech that he was tightening access to the data and declared his intention to find a way to end government collection of the bulk records, he said the program's capabilities should be preserved.

The Obama administration has portrayed the bulk collection program as useful and lawful while at the same time acknowledging concerns about privacy and potential abuse. But in its report, the board lays out what may be the most detailed critique of the government's once-secret legal theory behind the program: that a law known as Section 215 of the Patriot Act, which allows the F.B.I. to obtain

business records deemed "relevant" to an investigation, can be legitimately interpreted as authorizing the N.S.A. to collect all calling records in the country.

The program "lacks a viable legal foundation under Section 215, implicates constitutional concerns under the First and Fourth Amendments, raises serious threats to privacy and civil liberties as a policy matter, and has shown only limited value," the report said. "As a result, the board recommends that the government end the program."

While a majority of the five-member board embraced that conclusion, two members dissented from the view that the program was illegal. But the panel was united in 10 other recommendations, including deleting raw phone records after three years instead of five and tightening access to search results.

The report also sheds light on the history of the once-secret bulk collection program. It contains the first official acknowledgment that the Foreign Intelligence Surveillance Court produced no judicial opinion detailing its legal rationale for the program until last August, even though it had been issuing orders to phone companies for the records and to the N.S.A. for how it could handle them since May 2006.

The privacy board's legal critique of the program was approved by David Medine, the board's chairman and a former Federal Trade Commission official in the Clinton administration; Patricia M. Wald, a retired federal appeals court judge named to the bench by President Jimmy Carter; and James X. Dempsey, a civil liberties advocate who specializes in technology issues.

But the other two members — Rachel L. Brand and Elisebeth Collins Cook, both of whom were Justice Department lawyers in the George W. Bush administration — rejected the finding that the program was illegal.

They wrote in separate dissents that the board should have focused exclusively on policy and left legal analysis to the courts. Last month, two Federal District Court judges reached opposite legal conclusions in separate lawsuits challenging the program.

Ms. Brand wrote that while the legal question was "difficult," the government's legal theory was "at least a reasonable reading, made in good faith by numerous officials in two administrations of different parties." She also worried that declaring that counterterrorism officials "have been operating this program

unlawfully for years" could damage morale and make agencies overly cautious in taking steps to protect the country.

But the privacy board was unanimous in recommending a series of immediate changes to the program. The three in the majority wanted those changes as part of a brief wind-down period, while the two in dissent wanted them to be structural for a program that would continue.

Some of those recommendations dovetailed with the steps Mr. Obama announced last week, including limiting analysts' access to the call records of people no further than two links removed from a suspect, instead of three, and creating a panel of outside lawyers to serve as public advocates in major cases involving secret surveillance programs.

Other recommendations — like deleting data faster — were not mentioned in the president's speech. And all members of the board expressed privacy concerns about requiring phone companies to retain call records longer than they normally would, which might be necessary to meet Mr. Obama's stated goal of finding a way to preserve the program's ability without having the government collect the bulk data.

The program began in late 2001 based on wartime authority claimed by President Bush. In 2006, the Bush administration persuaded the surveillance court to begin authorizing the program based on the Patriot Act under a theory the Obama administration would later embrace.

But the privacy board's report criticized that, saying that the legal theory was a "subversion" of the law's intent, and that the program also violated the Electronic Communications Privacy Act.

"It may have been a laudable goal for the executive branch to bring this program under the supervision" of the court, the report says. "Ultimately, however, that effort represents an unsustainable attempt to shoehorn a pre-existing surveillance program into the text of a statute with which it is not compatible."

Defenders of the program have argued that Congress acquiesced to that secret interpretation of the law by twice extending its expiration without changes. But the report rejects that idea as "both unsupported by legal precedent and unacceptable as a matter of democratic accountability."

The report also scrutinizes in detail a handful of investigations in which the program was used, finding "no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack."

Still, in her dissent, Ms. Cook criticized judging the program's worth based only on whether it had stopped an attack to date. It also has value as a tool that can allow investigators to "triage" threats and provide "peace of mind" if it uncovers no domestic links to a newly discovered terrorism suspect, she wrote.

A version of this article appears in print on January 23, 2014, on page A14 of the New York edition with the headline: Watchdog Report Says N.S.A. Program Is Illegal and Should End.

How the NSA's Surveillance Procedures Threaten Americans' Privacy

Newly released documents confirm what critics have long suspected—that the National Security Agency, a component of the Defense Department, is engaged in unconstitutional surveillance of Americans' communications, including their telephone calls and emails. The documents show that the NSA is conducting sweeping surveillance of Americans' international communications, that it is acquiring many purely domestic communications as well, and that the rules that supposedly protect Americans' privacy are weak and riddled with exceptions.

The FISA Amendment Act, signed into law by President Bush in 2008, expanded the government's authority to monitor Americans' electronic communications. Critics of the law feared the NSA would use the law to conduct broad surveillance of Americans' international communications and, in the process, capture an unknown quantity of purely domestic communications. Government officials contended that the law authorized surveillance of foreign nationals outside the United States—not of Americans—and that it included robust safeguards to protect Americans' privacy. Last year, in a successful effort to derail a constitutional challenge to the law, the Obama administration made these same claims to the U.S. Supreme Court.

Now *The Guardian* has published two previously secret documents that show how the FISA Amendments Act is being implemented. One document sets out the government's "targeting procedures"—the procedures it uses to determine whether it has the authority to acquire communications in the first place. The other sets out the government's "minimization procedures"—the procedures that govern the retention, analysis, and dissemination of the communications it acquires. Both documents—the "Procedures"—have apparently been endorsed by the Foreign Intelligence Surveillance Court, which oversees government surveillance in some national security cases.

The Procedures are complex, but at least some of their flaws are clear.

1. **The Procedures permit the NSA to monitor Americans' international communications in the course of surveillance targeted at foreigners abroad.**

The NSA "is not listening to Americans' phone calls or monitoring their emails," the Chairman of the House Intelligence Committee recently said, and many other government officials, including the president himself, have made similar assurances. But these statements are not true. While the FISA Amendments Act authorizes the government to target foreigners abroad, not Americans, it permits the government to collect Americans' communications with those foreign targets. Indeed, in advocating for the Act, government officials made clear that these "one-end-domestic" communications were the ones of most interest to them. The Procedures contemplate not only that the NSA will acquire Americans' international communications but that it will retain them and possibly disseminate them to other U.S. government agencies and foreign governments. Americans' communications that contain "foreign intelligence information" or evidence of a crime can be retained forever, and even communications that don't can be retained for as long as five years. Despite government officials' claims to the contrary, the NSA is building a growing database of Americans' international telephone calls and emails.

2. **The Procedures allow the surveillance of Americans by failing to ensure that the NSA's surveillance targets are in fact foreigners outside the United States.**

The Act is predicated on the theory that foreigners abroad have no right to privacy—or, at any rate, no right that the United States should respect. Because they have no right to privacy, the U.S. government sees no bar to the collection of their communications, including their communications with Americans. But even if one accepts the government's premise, the Procedures fail to ensure that the NSA's surveillance targets are *in fact* foreigners outside the United States. This is because the Procedures permit the NSA to *presume* that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary—and to presume therefore that they are fair game for warrantless surveillance.

3. **The Procedures permit the government to conduct surveillance that has no real connection to the government's foreign intelligence interests.**

One of the fundamental problems with the Act is that it permits the government to conduct surveillance without probable cause or individualized suspicion. It permits the government to monitor people who aren't even thought to be doing anything wrong, and to do so without particularized warrants or meaningful review by impartial judges. Government officials have placed heavy emphasis on the fact that the Act allows the government to conduct surveillance only if one of its purposes is to gather "foreign intelligence information." That term, though, is defined very broadly to include not only information about terrorism but

also information about intelligence activities, the national defense, and even "the foreign affairs of the United States." The Procedures weaken the limitation further. Among the things the NSA examines to determine whether a particular email address or phone number will be used to exchange foreign intelligence information is whether it has been used in the past to communicate with foreigners. Another is whether it is listed in a foreigner's address book. In other words, the NSA seems to equate a propensity to communicate with foreigners with a propensity to communicate foreign intelligence information. The effect is to bring virtually every international communication within the reach of the NSA's surveillance.

4. The Procedures permit the NSA to collect international communications, including Americans' international communications, in bulk.

On its face, the Act permits the NSA to conduct dragnet surveillance, not just surveillance of specific individuals. Officials who advocated for the Act made clear that this was one of its principal purposes, and unsurprisingly, the Procedures give effect to that design. While they require the government to identify a "target" outside the country, once the target has been identified the Procedures permit the NSA to sweep up the communications of any foreigner who may be communicating "about" the target. The Procedures contemplate that the NSA will do this by "employ[ing] an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas," by "target[ing] Internet links that terminate in a foreign country," or by identifying "the country code of the telephone number." However the NSA does it, the result is the same: millions of communications may be swept up, Americans' international communications among them.

5. The Procedures allow the NSA to retain even purely domestic communications.

Given the permissive standards the NSA uses to determine whether prospective surveillance targets are foreigners abroad, errors are inevitable. Some of the communications the NSA collects under the Act, then, will be purely domestic. (Notably, a 2009 *New York Times* article discusses an episode in which the NSA used the Act to engage in "significant and systemic" overcollection of such domestic communications.) The Act should require the NSA to purge these communications from its databases, but it does not. The Procedures allow the government to keep and analyze even purely domestic communications if they contain significant foreign intelligence information, evidence of a crime, or encrypted information. Again, foreign intelligence information is defined exceedingly broadly. The result is that the NSA is steadily building a database of Americans' purely domestic calls and emails.

6. The Procedures allow the government to collect and retain communications protected by the attorney–client privilege.

The Procedures expressly contemplate that the NSA will collect attorney-client communications. In general, these communications receive no special protection—they can be acquired, retained, and disseminated like any other. Thus, if the NSA acquires the communications of lawyers representing individuals who have been charged before the military commissions at Guantanamo, nothing in the Procedures would seem to prohibit the NSA from sharing the communications with military prosecutors. The Procedures include a more restrictive rule for communications between attorneys and their clients who have been criminally indicted in the United States—the NSA may not share these communications with prosecutors. Even those communications, however, may be retained to the extent that they include foreign intelligence information.

7. The Procedures contemplate that the NSA will maintain "knowledge databases" containing sensitive information about Americans.

To determine whether a target is a foreigner abroad, the Procedures contemplate that the NSA will consult various NSA databases containing information collected by it and other agencies through signals intelligence, human intelligence, law enforcement, and other means. These databases—referred to as "NSA content repositories" and "knowledge databases"—apparently house internet data, including metadata that reveals online activities, as well as telephone numbers and email addresses that the agency has reason to believe are being used by U.S. persons. The Procedures' reference to "Home Location Registers," which receive updates whenever a phone "moves into a new service area," suggests that the NSA also collects some form of location information about millions of Americans' cellphones. The Procedures do not say what limits apply to these databases or what safeguards, if any, are in place to protect Americans' constitutional rights.

8. The Procedures allow the NSA to retain encrypted communications indefinitely.

The Procedures permit the NSA to retain, forever, all communications—even purely domestic ones—that are encrypted. The use of encryption to protect data is a routine and sometimes legally required practice by financial organizations, health care providers, and real-time communications services (like Skype and Apple's FaceTime). Accordingly, the Procedures permit the NSA to retain huge volumes of Americans' most sensitive information.

Republican National Committee Resolution on NSA Surveillance

RESOLUTION TO RENOUNCE THE NATIONAL SECURITY AGENCY'S SURVEILLANCE PROGRAM

WHEREAS, the secret surveillance program called PRISM targets, among other things, the surveillance of communications of U.S. citizens on a vast scale and monitors searching habits of virtually every American on the internet;

WHEREAS, this dragnet program is, as far as we know, the largest surveillance effort ever launched by a democratic government against its own citizens, consisting of the mass acquisition of Americans' call details encompassing all wireless and landline subscribers of the country's three largest phone companies*;

WHEREAS, every time an American citizen makes a phone call, the NSA gets a record of the location, the number called, the time of the call and the length of the conversation; all of which are an invasion into the personal lives of American citizens that violates the right of free speech and association afforded by the First Amendment of the United States Constitution;

WHEREAS, the mass collection and retention of personal data is in itself contrary to the right of privacy protected by the Fourth Amendment of the United States Constitution, which guarantees the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, that warrants shall issue only upon probable cause, and generally prevents the American government from issuing modern-day writs of assistance;

WHEREAS, unwarranted government surveillance is an intrusion on basic human rights that threatens the very foundations of a democratic society and this program represents a gross infringement of the freedom of association and the right to privacy and goes far beyond even the permissive limits set by the Patriot Act; and

WHEREAS, Republican House Representative Jim Sensenbrenner, an author of the Patriot Act and Chairman of the House Judiciary Committee at the time of Section 215's passage, called the Section 215 surveillance program "an abuse of that law," writing that, "based on the scope of

the released order, both the administration and the FISA (Foreign Intelligence Surveillance Act) court are relying on an unbounded interpretation of the act that Congress never intended;" therefore be it

RESOLVED, the Republican National Committee encourages Republican lawmakers to enact legislation to amend Section 215 of the USA PATRIOT Act, the state secrets privilege, and the FISA Amendments Act to make it clear that blanket surveillance of the Internet activity, phone records and correspondence – electronic, physical, and otherwise - of any person residing in the U.S. is prohibited by law and that violations can be reviewed in adversarial proceedings before a public court;

RESOLVED, the Republican National Committee encourages Republican law makers to call for a special committee to investigate, report, and reveal to the public the extent of this domestic spying and the committee should create specific recommendations for legal and regulatory reform to end unconstitutional surveillance as well as hold accountable those public officials who are found to be responsible for this unconstitutional surveillance; and

RESOLVED, the Republican National Committee calls upon Republican lawmakers to immediately take action to halt current unconstitutional surveillance programs and provide a full public accounting of the NSA's data collection programs.

What is the NSA domestic spying program?

In October 2001, President Bush issued a secret presidential order authorizing the NSA to conduct a range of surveillance activities inside of the United States without statutory authorization or court approval, including electronic surveillance of Americans' telephone and Internet communications. This program of surveillance continues through today, although the legal justifications have changed over time, and works with the major telecommunications and Internet companies.

In 2005, after the *New York Times* broke the story of the surveillance program, the President publicly admitted one portion of it—warrantless surveillance of Americans believed to be communicating with people connected with terrorism suspects—Senior Bush Administration officials later confirmed that the President's authorization went beyond the surveillance of terrorists and conceded that the program did not comply with the Foreign Intelligence Surveillance Act (FISA). The President, invoking a theory of limitless executive power to disregard the mandates of Congress, reauthorized this warrantless surveillance more than thirty times, including after the Department of Justice found the program to violate criminal laws. President Obama has continued the program, but with differing secret legal justifications. Obama has given no public legal justification for it and, in some situations, appears to be strategically denying certain portions of it. For other portions, including the collection of telecommunications records, the Obama Administration said it could neither confirm nor deny its actions until May, 2013, when the DNI finally admitted additional portions of it. Members of Congress have confirmed that additional domestic surveillance by the NSA still remains a secret.

Shortly after the initial revelations, a whistleblower named Mark Klein came forward with evidence describing the specific AT&T facilities, including one on Folsom Street in San Francisco, where the handoff of customer communications is occurring. Mr. Klein's evidence confirmed what was already indicated by numerous newspaper reports and Congressional admissions—that the NSA is intercepting and analyzing millions of ordinary Americans' communications off of the fiber optic cables that carry our communications, with the help of the country's largest phone and Internet companies. EFF has brought two lawsuits to stop this illegal surveillance. In 2012, three NSA whistleblowers came forward to confirm Mr. Klein's evidence, as well as other information about the warrantless surveillance.

Today, the warrantless surveillance program started under Bush remains largely intact under the Obama administration, and, in June 2013, reports in the Guardian and Washington Post confirmed key facts alleged in our cases, and provided supporting documents.

While the full legal justifications remain secret, the Obama administration apparently uses strained interpretations of the Patriot Act and FISA Amendments Act to try to justify the mass collection of data on US persons, but the reality is the same as it was under the Bush administration: these program are illegal and unconstitutional.

https://www.eff.org/nsa-spying/faq#37

TENTH Amendment CENTER

P.O. Box 13458
Los Angeles, CA 90013
213.935.0553

Jan. 30, 2015
Re: Support for SB13

Dear members of the Alaska legislature,

The Tenth Amendment Center fully supports passage of SB13, prohibiting the state and municipalities from using assets to assist a federal agency in collecting certain telephone records or electronic data without a warrant.

In 1975, Sen. Frank Church warned us about the NSA, saying it had the potential for 'total tyranny. That was before widespread public access to the Internet, before everybody used cell phones, and before the widespread use of email and text messaging. Imagine the threat the spy agency poses today.

Forty years later, Congress still hasn't done anything to address the surveillance state. In fact, it has given the NSA more power and made it more intrusive.

Congress won't act to protect our privacy, so you must. By refusing to provide "material support or resources" to the NSA, you will not only support efforts to turn off the NSA's water in Utah, but will also end some practical effects of warrantless spying in Alaska. As more states take action, it will box the agency in and force the reforms D.C. politicians seem unwilling to pursue.

SB13 will address the NSA in three important ways.

- Practically-speaking, the legislation would almost certainly stop the NSA from ever setting up a new facility in Alaska.
- It would prohibit the state from obtaining or utilizing data gathered by the NSA without a warrant and shared with state and local law enforcement, a practice revealed in a 2013 Reuters article. Former NSA Chief Technical Director William Binney called data sharing the country's "greatest threat since the Civil War."
- It would set the stage to end partnerships between the NSA and state universities.

SB13 rests on a rock-solid legal principle known as the anti-commandeering doctrine. The Supreme Court has repeatedly upheld the principle that the federal government cannot required states to expend resources or manpower to help carry out its acts or programs.

In fact, SB13 merely builds on anti-commandeering legislation already passed by the Alaska legislature. Whether or not Alaska can refuse material support and resources to the federal government stands as a settled issue. The only question remaining is whether or not the Alaska will continue to support unconstitutional, warrantless spying.

You have the opportunity to do what Congress has failed to do for 40 years – protect the privacy of Alaskans, preserve the Fourth Amendment and help rein in an unaccountable and out of control federal spy agency.

We strongly urge you to vote yes on SB13.

Sincerely,

Michael Boldin, Tenth Amendment Center founder and executive director
Mike Maharrey, Tenth Amendment Center national communications director

Alaska Bill Would Ban "Material Support or Resources" to NSA

By Michael Boldin

JUNEAU, Alaska (Jan. 21, 2015) - A bill filed in Alaska late last week would ban "material support or resources" to the NSA. This would not only support efforts to turn off NSA's water in Utah, but have practical effects on federal surveillance programs if passed.

Alaska Sen. Bill Wielechowski prefiled SB13 on Jan. 16. The legislation would prohibit the state and its municipalities from using assets, including personnel, to assist a federal agency in collecting certain telephone records or electronic data without a warrant, making it the fourth state to introduce legislation similar to a bill up for consideration in Utah this year.

Wielechowski took a little different approach to protecting the Fourth Amendment in the way he crafted his bill.

In 2013, Alaska Gov. Sean Parnell signed anti-commandeering legislation into law prohibiting the state from assisting the federal government in the enforcement of laws that violate the right to keep and bear arms, in implementing indefinite detention without due process under the National Defense Authorization Act, and in enforcing or implementing the Real ID Act of 2005. Instead of drafting a standalone law to ban state assistance to federal spies, the Alaska bill amends this 2013 law to include a prohibition of state assistance to any federal agency engaging in warrantless spying.

A state or municipal agency may not use or authorize the use of an asset to implement or aid in... the collection by a federal agency of electronic data without a search warrant; in this paragraph, "electronic data" includes electronic mail and text messages; or the collection by a federal agency of telephone records without a search warrant, unless the records are collected in a manner consistent with state law.

"This is a great strategic move," OffNow executive director Mike Maharrey said. "By piggybacking onto existing anti-commandeering law, Wielechowski eliminates any debate about whether or not the state can prohibit material support to federal agencies. That's been settled in Alaska. Now it simply becomes a question of whether the state wants to cooperate

with unconstitutional NSA spying or not. Anybody who opposes this bill is essentially saying, 'Why yes, I think we should help the feds violate your rights.'"

SB13 also adds an additional provision to state law limiting home rule municipality powers stipulating that "a municipality or an agent of a municipality may not assist, cooperate with, or participate with a federal agency in the collection of" electronic data or telephone records without a search warrant, and prohibits the "use, in a criminal investigation or prosecution, records or data that are provided by a federal agency or an officer or employee of a federal agency that were collected by the federal agency without a search warrant or in another manner inconsistent with state law."

"With all of its provisions amending various existing statutes, the bill seems rather complex," Maharrey said. "But it really isn't when you get down to it. Simply put, if passed, this legislation will end any cooperation by state or local agencies in warrantless spying. It does exactly what our Fourth Amendment Protection Act does. It simply takes a different legislative approach. This is a solid bill and a great strategy."

LEGALITY

As mentioned earlier, Wielechowski's bill adds to an anti-commandeering law already on the books in Alaska. The Supreme Court has repeatedly upheld the principle that the states cannot be required to expend resources or manpower to help the federal government carry out its acts or programs.

Known as the anti-commandeering doctrine, the legal principle rests primarily on four Supreme Court opinions dating back to 1842. In *Prigg v. Pennsylvania* (1842), Justice Joseph Story held that the federal government could not force states to implement or carry out the Fugitive Slave Act of 1793. He said that it was a federal law, and the federal government ultimately had to enforce it.

The fundamental principle applicable to all cases of this sort, would seem to be, that where the end is required, the means are given; and where the duty is enjoined, the ability to perform it is contemplated to exist on the part of the functionaries to whom it is entrusted. The clause is found in the national Constitution, and not in that of any state. It does not point out any state functionaries, or any state action to carry its provisions into effect. The

states cannot, therefore, be compelled to enforce them; and it might well be deemed an unconstitutional exercise of the power of interpretation, to insist that the states are bound to provide means to carry into effect the duties of the national government, nowhere delegated or instrusted to them by the Constitution.

Other key cases include *New York v. United States* (1992), *Printz v. United States* (1997), and *Independent Business v. Sebelius* (2012).

Noted Constitutional scholar Randy Barnett of Georgetown Law said, *"State governments are free to refrain from cooperating with federal authorities if they so choose. In general, states cannot attack federal operations, but that's not the same as refusing to help."*

RESOURCES, SUPPORT FOR UTAH

The original definition of "material support or resources" included providing tangible support such as money, goods, and materials and also less concrete support, such as "personnel" and "training." Section 805 of the PATRIOT Act expanded the definition to include "expert advice or assistance."

Practically-speaking, the legislation would almost certainly stop the NSA from ever setting up a new facility in Alaska.

In 2006, the agency maxed out the Baltimore-area power grid, creating the potential, as the Baltimore Sun reported, for a "virtual shutdown of the agency." Since then, the NSA aggressively expanded in states like Utah, Texas, Colorado and elsewhere, generally focusing on locations that can provide cheap and plentiful resources like water and power.

In a recent hearing on the Utah Fourth Amendment Protection Act, a Utah state rep, intentionally or not, made a plea to other states to help out. "If Utah goes through all this trouble to turn off the water, what's to stop the NSA from moving to another state?" he asked.

"What will stop the NSA from moving? Bills like this one introduced by Sen. Wielechowski ," Maharrey said. "The legislation pulls the welcome mat right out from under the NSA. And if enough states step up and pass bills like this, we can literally box them in and shut them down."

PRACTICAL EFFECT

By including a prohibition on participation in the illegal collection and use of electronic data by the state, SB13 would also prohibit what former NSA Chief Technical Director William Binney called the country's "greatest threat since the Civil War."

The bill would ban the state from obtaining or making use of electronic data or metadata obtained by the NSA without a warrant.

Reuters revealed the extent of such NSA data sharing with state and local law enforcement in an August 2013 article. According to documents obtained by the news agency, the NSA passes information to police through a formerly secret DEA unit known Special Operations Divisions and the cases "rarely involve national security issues." Almost all of the information involves regular criminal investigations, not terror-related investigations.

In other words, not only does the NSA collect and store this data. using it to build profiles, the agency encourages state and local law enforcement to violate the Fourth Amendment by making use of this information in their day-to-day investigations.

This is "the most threatening situation to our constitutional republic since the Civil War," Binney said.

The bill would also set the stage to end partnerships between the NSA and state universities.

WHAT'S NEXT

Alaska joins South Carolina, Indiana and Missouri, along with Utah, in considering this type of legislation for 2015. Legislators in seven other states have committed to doing the same. Sources close to OffNow indicate even more states will likely follow. The bill in Utah is being prepared for debate and discussion in the state House right now.

SB13 has yet to be assigned to a committee.

Alaska State Legislature

Please enter into the record my testimony to the _Senate Community and Regional Affairs Committee

on ____SB13 _____ dated _____032415_____.

Dear Senators,

I write to urge you to support SB13 regarding the Warrantless Search of Electronic Data. It is important to safeguard the privacy of ALL Alaskans from government intrusion and over reach. The federal government has repeatedly shown blatant disregard for our privacy and liberty. This measure is a limited attempt to protect Alaskans from any further such abuses.

Peace & Blessings, J.R. Myers
Chairman, Alaska Constitution Party

POB 2086 Soldotna AK 99669
907-690-5200.

SENATE BILL 13: WARRANTLESS SEARCH OF ELECTRONIC DATA

SENATOR WIELECHOWSKI

STAFF: SARAH EVANS

WHAT IS THE NSA?

- NSA stands for National Security Agency
- NSA is a U.S. intelligence agency responsible for the global monitoring, collection, decoding, translation and analysis of information and data for foreign intelligence and counterintelligence purposes.
- The NSA was created in 1952

WHY SHOULD ALASKANS BE CONCERNED ABOUT THE NSA?

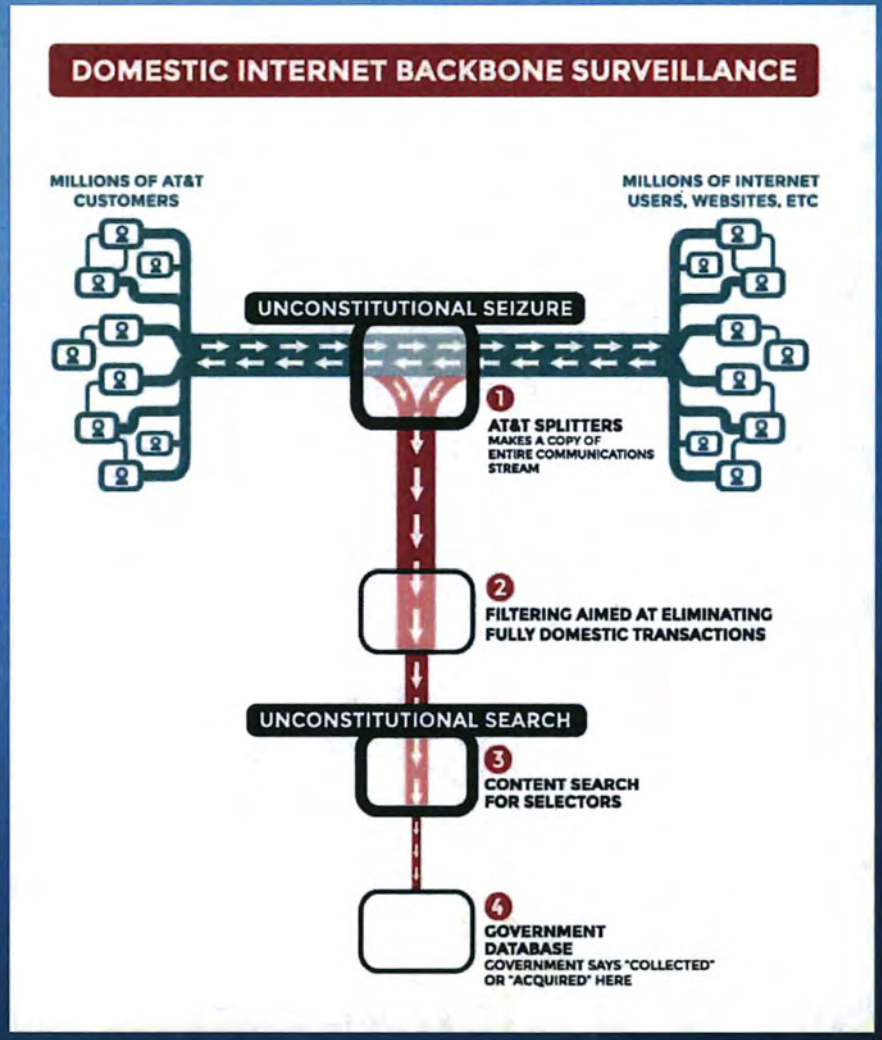
- The NSA has the ability to collect every American's phone records
- The PRISM Program lets the NSA access private user data on leading online services
- The NSA taps long-distance internet connection
- The NSA tracks cell phone locations around the world

HOW DID WE GET HERE?

- 2001 President Bush signed order beginning NSA's Domestic Spying Program after 9/11 attacks
- October 2001 the NSA had major telecommunication companies in the US hand over "call-detail records" which included customers names, street addresses and other personal information
- 2005 The NY Times exposed the NSA Spy Program for the first time.
- 2006 The NSA maxed out the Baltimore-area power gird
- 2008 President Bush signed into law the FISA Amendment Act

HOW PHONE SPYING WORKS

- In 2003 AT&T Tech. Mark Kline finds fiber-optic splitter installed by the NSA
- Thirty-Year NSA veteran, William Binney, estimates that the NSA installed between 10-20 intercept centers within the US.
- He also estimates NSA has collected between 15-20 trillion transactions over the past 11 years.

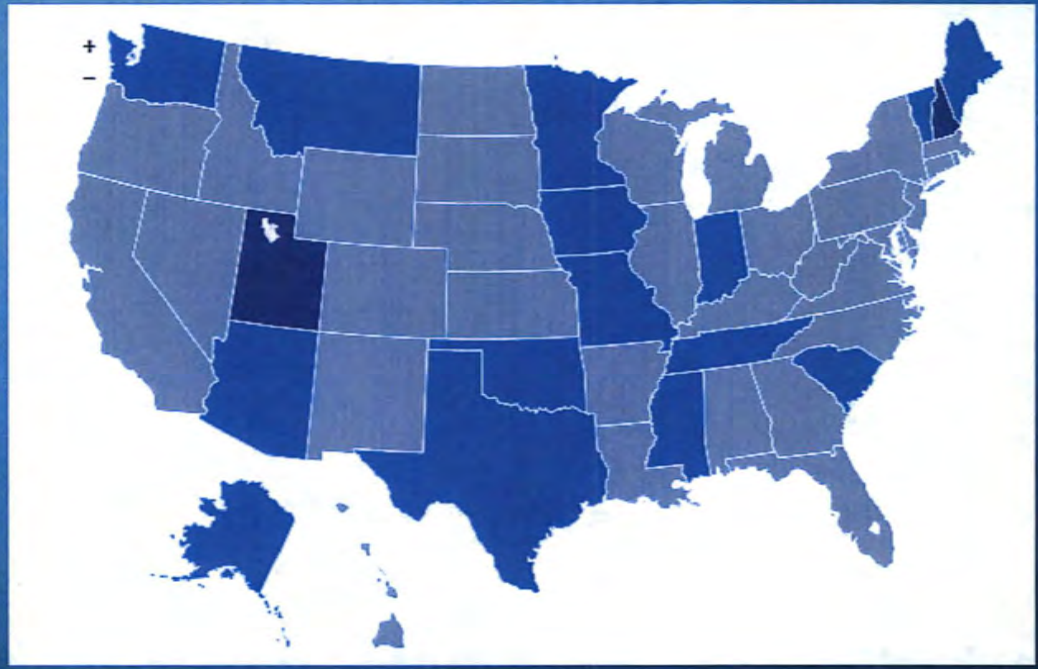


HOW DO WE KNOW THIS?

- The Guardian receives thousands of top secrets documents on American phone records and internet use that were leaked by an NSA employee
- In June of 2013 The Guardian beings to publish the documents revealing what information the NSA had been gathering

WHAT STATES ARE TAKING ACTION?

- The NSA sometimes relies on state and local government's resources to carry out their mass surveillance programs.
- 4th Amendment Protection Act bans all material support or resources to federal warrantless surveillance programs.
- Electronic Data Privacy Act prohibits states from obtaining data collected without a warrant



- Blue means legislation has been introduced in those states
- Purple means Electronic Data Privacy Law

WHAT DOES SB 13 DO?

- Section 1 provides that a home rule municipality may not adopt an ordinance inconsistent with the provisions of sec. 2 of the bill
- Section 2 prohibits a municipality or an agent of a municipality from cooperating with a federal data collection and surveillance agency in collecting electronic data without a search warrant or collecting telephone records without a warrant unless the collection is consistent with state law, and from using such records in a criminal investigation or prosecution
- Section 3 prohibits a state of municipal agency from using state or municipal assets to aid a federal data collection and surveillance agency in the collection of electronic data without a search warrant, or the collection of telephone records without a warrant unless the collection is consistent with state law

WHAT DOES SB 13 DO?

- Section 4 defines "electronic data" and "federal data collection and surveillance agency"
- Section 5 prohibits the state or an agent of the state from cooperating with a federal data collection and surveillance agency in collecting data without a search warrant, or collecting telephone records without a warrant unless the collection is consistent with state law, and from using such records in a criminal investigation or prosecution
- Section 6 provides that the bill has an immediate effective date


QUESTIONS?