SJR

22

<TARGET><BILL>SJR 22</BILL><SUBJECT>SJR 22</SUBJECT><COMM>HJUD28</COMM></TARGET>

OUSE COMMITTEE REPOR

(7)
Date Referred to Committee: April 1, 2014 **FURTHER REFERRALS:**

Date of Committee Action: 4/11/14

The JUDICIARY Committee considered: **SJR 22 am**

SENATE JOINT RESOLUTION NO. 22 am
Opposing the warrantless collection of telephone call data by the National Security Agency.
SJR 22 OPPOSE WARRANTLESS DATA COLLECTION

Recommends it be replaced with [✓] HCS *or* [ ] CS *for* SJR 22 (JUD)
***For Senate Bills with new title: [ ] Technical Title [ ] New Title: HCR*______** **[✓] Same Title [ ] New Title**

[ ] attach amendments
[ ] add new referral to ____________Committee
[ ] Letter of Intent___________Committee

List of Abbrev for Depts.:
ADM
CED
COR
CRT
EED
DEC
DFG
GOV
DHS
LWF
LAW
LEG
MVA
DNR
DPS
REV
DOT
UA

***NEW* FISCAL NOTES**
*FN# is assigned by Chief Clerk's Office

*FN#	List by Dept(s):	Fiscal	Indet.	Zero

***PREVIOUS* FISCAL NOTES**

FN#	List by Dept(s):	Fiscal	Indet.	Zero
1	LEG			✓

Signing with recommendations	Printed Last Name	DP	DNP	NR	AM
[signature]	LeDoux	X			
[signature]	Pruitt	X			
[signature]	Gruenberg	—			
[signature]	LYNN	X			
Chair: [signature]	Keller	X			
Chair:					

ALASKA STATE LEGISLATURE

Session
State Capitol Building
Juneau, Alaska 99801-1182
Phone: (907) 465-4843
Fax: (907) 465-3871

District
716 West 4th Avenue
Anchorage, Alaska 99501-2133
Phone: (907) 269-0181
Fax: (907) 269-0184

SENATOR CATHY GIESSEL

MEMORANDUM

DATE: April 1, 2014

TO: Representative Wes Keller, Chair, House Judiciary Committee

FROM: Senator Cathy Giessel

RE: Request for Hearing, SJR 22

I respectfully request that **SJR 22 Oppose Warrantless Collection of Data** be scheduled in the House Judiciary Committee at your earliest convenience.

SJR 22 urges the federal government to end the National Security Agency's (NSA) mass telephone data collection program and eliminate all stored metadata. This resolution opposes the secretive nature under which the Foreign Intelligence Surveillance Court operates under sec. 2156 of the USA PATRIOT Act and the court's sanctioning of warrantless data collection.

These NSA activities are yet another violation of statute and example of troubling federal overreach. SJR 22, rejects surrendering our liberty in the name of unconstitutional programs.

Attached you will find:

1. SJR 22
2. SJR 22 Sponsor Statement
3. Change Document from Senate Floor
4. News articles on NSA agency and related topics

Please contact Jane Conway, 465-8181, in my office if you need any further information.

ALASKA STATE LEGISLATURE

Senate District N
Anchorage Hillside, Turnagain Arm,
Cooper Landing, Sterling, Nikiski,
Moose Pass, Bear Creek, Seward

State Capitol, Room 427
Juneau AK 99801-1182
907-465-4843
Fax: 907-465-3871
800-892-4843

North to the Future

Senator Cathy Giessel

SJR 22 Oppose Warrantless Data Collection
Sponsor Statement

SJR 22 urges the federal government to end the National Security Agency's (NSA) mass telephone data collection program and eliminate all stored metadata. This resolution opposes the secretive nature under which the Foreign Intelligence Surveillance Court operates under sec. 2156 of the USA PATRIOT Act and the court's sanctioning of warrantless data collection.

The NSA, founded in 1952, is the nation's largest intelligence agency, with a strict focus on overseas, rather than domestic surveillance. Recently the news has been abuzz, revealing a number of concerning mass-surveillance programs undertaken by NSA.

On December 16, 2013 the United States District Court Judge Richard Leon ruled that the NSA program, bulk collection, and querying of telephone record metadata are likely unconstitutional, and "almost Orwellian" in nature. He suggested that James Madison would be "aghast" to learn of his government's encroachment on the liberty of its citizens. The Electronic Communications Privacy Act of 1986 prohibits telephone companies from sharing consumer data, except in special circumstances. The January 2014 Civil Liberties Oversight Board Report concluded that the NSA's telephone data collection program likely violates this act.

The Constitution of the United States protects individuals against the abuse of government authority and the Fourth Amendment guards against unreasonable searches and seizure and lays out specific requirements for warrants. The Fifth Amendment requires that individuals may not be deprived of life, liberty, or property without due process of law.

The executive branch has been given far too much power to invade individual privacy. Thomas Paine may have said it best, "Government, even in its best state, is but a necessary evil; in its worst state, an intolerable one."

As a legislator, I took an oath to uphold both the Constitution of the United States and the Alaska Constitution. These NSA activities are yet another violation of statute and example of troubling federal overreach. With SJR 22, I stand with Alaskans and reject surrendering our liberty in the name of unconstitutional programs.

Sen.Cathy.Giessel@akleg.gov

SJR 22 U.A Adopted Conceptual Amendment #1

Pg. 4, line 20: insert "and **the** Constitution of the State of Alaska"

Pg. 4, under "COPIES": add the chairs and ranking members of the US House and Senate Intelligence Committees to whom SJR 22 will be sent to.

FISCAL NOTE

STATE OF ALASKA
2014 LEGISLATIVE SESSION

Bill Version: **SJR 22**
Fiscal Note Number: 1
(S) Publish Date: 3/10/14

Identifier (file name)
Title: SJR 22-OPPOSE WARRANTLESS DATA COLLECTION
Sponsor: Senator Giessel
Requester: Senate Judiciary Committee

Dept. Affected
Appropriation
Allocation
OMB Component Number

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

	FY15 Appropriation Requested	Included in Governor's FY15 Request	Out-Year Cost Estimates				
OPERATING EXPENDITURES	**FY15**	**FY15**	**FY16**	**FY17**	**FY18**	**FY19**	**FY20**
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		(Thousands of Dollars)						
1002	Federal Receipts							
1003	GF Match							
1004	GF							
1005	GF/Prgm (DGF)							
1007	I/A Rcpts (Other)							
1156	Rcpt Svcs (DGF)							
		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 (FY14) operating costs _____ *(separate supplemental appropriation required)*
(discuss reasons and fund source(s) in analysis section)

Estimated CAPITAL (FY15) costs _____ *(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? _____

If yes, by what date are the regulations to be adopted, amended, or repealed? _____ Discuss details in analysis section.

Why this fiscal note differs from previous version (if initial version, please note as such)

Initial Version.

Prepared by: Senate Judiciary Committee — Phone 465-3719
Division: — Date/Time 3/7/14 12:00 AM
Approved by: Senator Coghill, Chair — Date 3/17/2014
Division:

(Revised 8/16/2013 OMB)

Politics

Are local police conducting NSA-style surveillance?

By William Patrick

Published March 06, 2014

TALLAHASSEE, Fla. – The National Security Agency apparently isn't the only government agency engaged in domestic spying.

Local law enforcement is playing the role of Big Brother, too, but to what extent is still unknown. ADVERTISEMENT

Recent court documents reveal a troubling cell phone surveillance program conducted by a Florida police department against unsuspecting cell phone users.

Attempts to keep the practice secret, even from judges, is raising questions as to just how prevalent police spying is within the Sunshine State.

The controversy stems from the arrest of James L. Thomas, a criminal suspect believed to be in possession of a stolen phone. Tallahassee police located and arrested Thomas by tracking a cell phone signal, then promptly searched his home.

It later became known that police didn't seek a warrant or admit to using a little-known surveillance device called a "Stingray."

Stingrays are small mobile devices that trick cell phones into connecting to them as if they were cell phone towers. The technology gives police the ability to track phone movements and intercept both phone calls and text messages of any cell phone within range.

Jane Conway

From: Jane Conway
Sent: Wednesday, March 05, 2014 2:53 PM
To: Jane Conway
Subject: NSA broke privacy rules thousands of times per year, audit finds - The Washington Post

The Washington Post

NSA broke privacy rules thousands of times per year, audit finds

By Barton Gellman,

The National Security Agency has broken privacy rules or overstepped its legal authority thousands of times each year since Congress granted the agency broad new powers in 2008, according to an internal audit and other top-secret documents.

Most of the infractions involve unauthorized surveillance of Americans or foreign intelligence targets in the United States, both of which are restricted by statute and executive order. They range from significant violations of law to typographical errors that resulted in unintended interception of U.S. e-mails and telephone calls.

The documents, provided earlier this summer to The Washington Post by former NSA contractor Edward Snowden, include a level of detail and analysis that is not routinely shared with Congress or the special court that oversees surveillance. In one of the documents, agency personnel are instructed to remove details and substitute more generic language in reports to the Justice Department and the Office of the Director of National Intelligence.

In one instance, the NSA decided that it need not report the unintended surveillance of Americans. A notable example in 2008 was the interception of a "large number" of calls placed from Washington when a programming error confused the U.S. area code 202 for 20, the international dialing code for Egypt, according to a "quality assurance" review that was not distributed to the NSA's oversight staff.

In another case, the Foreign Intelligence Surveillance Court, which has authority over some NSA operations, did not learn about a new collection method until it had been in operation for many months. The court ruled it unconstitutional.

[FISA judge: Ability to police U.S. spying program is limited]

The Obama administration has provided almost no public information about the NSA's compliance record. In June, after promising to explain the NSA's record in "as transparent a way as we possibly can," Deputy Attorney General James Cole described extensive safeguards and oversight that keep the agency in check. "Every now and then, there may be a mistake," Cole said in congressional testimony.

The NSA audit obtained by The Post, dated May 2012, counted 2,776 incidents in the preceding 12 months of unauthorized collection, storage, access to or distribution of legally protected communications. Most were unintended. Many involved failures of due diligence or violations of standard operating procedure. The most serious incidents included a violation of a court order and unauthorized use of data about more than 3,000 Americans and green-card holders.

In a statement in response to questions for this article, the NSA said it attempts to identify problems "at the earliest possible moment, implement mitigation measures wherever possible, and drive the numbers down." The government was made aware of The Post's intention to publish the documents that accompany this article online.

"We're a human-run agency operating in a complex environment with a number of different regulatory regimes, so at times we find ourselves on the wrong side of the line," a senior NSA official said in an interview, speaking with White House permission on the condition of anonymity.

"You can look at it as a percentage of our total activity that occurs each day," he said. "You look at a number in absolute terms that looks big, and when you look at it in relative terms, it looks a little different."

There is no reliable way to calculate from the number of recorded compliance issues how many Americans have had their communications improperly collected, stored or distributed by the NSA.

The causes and severity of NSA infractions vary widely. One in 10 incidents is attributed to a typographical error in which an analyst enters an incorrect query and retrieves data about U.S phone calls or e-mails.

But the more serious lapses include unauthorized access to intercepted communications, the distribution of protected content and the use of automated systems without built-in safeguards to prevent unlawful surveillance.

The May 2012 audit, intended for the agency's top leaders, counts only incidents at the NSA's Fort Meade headquarters and other facilities in the Washington area. Three government officials, speaking on the condition of anonymity to discuss classified matters, said the number would be substantially higher if it included other NSA operating units and regional collection centers.

Senate Intelligence Committee Chairman Dianne Feinstein (D-Calif.), who did not receive a copy of the 2012 audit until The Post asked her staff about it, said in a statement late Thursday that the committee "can and should do more to independently verify that NSA's operations are appropriate, and its reports of compliance incidents are accurate."

Despite the quadrupling of the NSA's oversight staff after a series of significant violations in 2009, the rate of infractions increased throughout 2011 and early 2012. An NSA spokesman declined to disclose whether the trend has continued since last year.

One major problem is largely unpreventable, the audit says, because current operations rely on technology that cannot quickly determine whether a foreign mobile phone has entered the United States.

In what appears to be one of the most serious violations, the NSA diverted large volumes of international data passing through fiber-optic cables in the United States into a repository where the material could be stored temporarily for processing and selection.

The operation to obtain what the agency called "multiple communications transactions" collected and commingled U.S. and foreign e-mails, according to an article in SSO News, a top-secret internal newsletter of

the NSA's Special Source Operations unit. NSA lawyers told the court that the agency could not practicably filter out the communications of Americans.

In October 2011, months after the program got underway, the Foreign Intelligence Surveillance Court ruled that the collection effort was unconstitutional. The court said that the methods used were "deficient on statutory and constitutional grounds," according to a top-secret summary of the opinion, and it ordered the NSA to comply with standard privacy protections or stop the program.

James R. Clapper Jr., the director of national intelligence, has acknowledged that the court found the NSA in breach of the Fourth Amendment, which prohibits unreasonable searches and seizures, but the Obama administration has fought a Freedom of Information lawsuit that seeks the opinion.

Generally, the NSA reveals nothing in public about its errors and infractions. The unclassified versions of the administration's semiannual reports to Congress feature blacked-out pages under the headline "Statistical Data Relating to Compliance Incidents."

Members of Congress may read the unredacted documents, but only in a special secure room, and they are not allowed to take notes. Fewer than 10 percent of lawmakers employ a staff member who has the security clearance to read the reports and provide advice about their meaning and significance.

The limited portions of the reports that can be read by the public acknowledge "a small number of compliance incidents."

Under NSA auditing guidelines, the incident count does not usually disclose the number of Americans affected.

"What you really want to know, I would think, is how many innocent U.S. person communications are, one, collected at all, and two, subject to scrutiny," said Julian Sanchez, a research scholar and close student of the NSA at the Cato Institute.

The documents provided by Snowden offer only glimpses of those questions. Some reports make clear that an unauthorized search produced no records. But a single "incident" in February 2012 involved the unlawful retention of 3,032 files that the surveillance court had ordered the NSA to destroy, according to the May 2012 audit. Each file contained an undisclosed number of telephone call records.

One of the documents sheds new light on a statement by NSA Director Keith B. Alexander last year that "we don't hold data on U.S. citizens."

Some Obama administration officials, speaking on the condition of anonymity, have defended Alexander with assertions that the agency's internal definition of "data" does not cover "metadata" such as the trillions of American call records that the NSA is now known to have collected and stored since 2006. Those records include the telephone numbers of the parties and the times and durations of conversations, among other details, but not their content or the names of callers.

The NSA's authoritative definition of data includes those call records. "Signals Intelligence Management Directive 421," which is quoted in secret oversight and auditing guidelines, states that "raw SIGINT data . . . includes, but is not limited to, unevaluated and/or unminimized transcripts, gists, facsimiles, telex, voice, and some forms of computer-generated data, such as call event records and other Digital Network Intelligence (DNI) metadata as well as DNI message text."

In the case of the collection effort that confused calls placed from Washington with those placed from Egypt, it is unclear what the NSA meant by a "large number" of intercepted calls. A spokesman declined to discuss the matter.

The NSA has different reporting requirements for each branch of government and each of its legal authorities. The "202" collection was deemed irrelevant to any of them. "The issue pertained to Metadata ONLY so there were no defects to report," according to the author of the secret memo from March 2013.

The large number of database query incidents, which involve previously collected communications, confirms long-standing suspicions that the NSA's vast data banks — with code names such as MARINA, PINWALE and XKEYSCORE — house a considerable volume of information about Americans. Ordinarily the identities of people in the United States are masked, but intelligence "customers" may request unmasking, either one case at a time or in standing orders.

In dozens of cases, NSA personnel made careless use of the agency's extraordinary powers, according to individual auditing reports. One team of analysts in Hawaii, for example, asked a system called DISHFIRE to find any communications that mentioned both the Swedish manufacturer Ericsson and "radio" or "radar" — a query that could just as easily have collected on people in the United States as on their Pakistani military target.

The NSA uses the term "incidental" when it sweeps up the records of an American while targeting a foreigner or a U.S. person who is believed to be involved in terrorism. Official guidelines for NSA personnel say that kind of incident, pervasive under current practices, "does not constitute a . . . violation" and "does not have to be reported" to the NSA inspector general for inclusion in quarterly reports to Congress. Once added to its databases, absent other restrictions, the communications of Americans may be searched freely.

In one required tutorial, NSA collectors and analysts are taught to fill out oversight forms without giving "extraneous information" to "our FAA overseers." FAA is a reference to the FISA Amendments Act of 2008, which granted broad new authorities to the NSA in exchange for regular audits from the Justice Department and the Office of the Director of National Intelligence and periodic reports to Congress and the surveillance court.

Using real-world examples, the "Target Analyst Rationale Instructions" explain how NSA employees should strip out details and substitute generic descriptions of the evidence and analysis behind their targeting choices.

"I realize you can read those words a certain way," said the high-ranking NSA official who spoke with White House authority, but the instructions were not intended to withhold information from auditors. "Think of a book of individual recipes," he said. Each target "has a short, concise description," but that is "not a substitute for the full recipe that follows, which our overseers also have access to."

Julie Tate and Carol D. Leonnig contributed to this report.

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

POLITICS

Rand Paul Files Lawsuit Over N.S.A. Call Surveillance

By CHARLIE SAVAGE FEB. 12, 2014

WASHINGTON — Senator Rand Paul, Republican of Kentucky, on Wednesday filed a lawsuit against President Obama and the leaders of several intelligence agencies. The suit challenges as unconstitutional the National Security Agency's once-secret program that is collecting bulk records about Americans' phone calls.

Mr. Paul, who had announced his intention to file the lawsuit in early January, joins an increasingly crowded set of plaintiffs, with several similar cases already pending.

But because of Mr. Paul's status as a rising star of the Tea Party faction of the Republican Party — one who staged a nearly 13-hour filibuster on the floor of the Senate in March raising concerns about the rules governing "targeted killings" using drone strikes — his lawsuit may attract particular attention.

"Today we ask the question for every phone user in America: can a single warrant allow the government to collect all your records, all the time?" Mr. Paul said in a statement. "I don't think so."

FreedomWorks, the conservative and libertarian advocacy group, is listed as a co-plaintiff in the lawsuit. The lead lawyer is Kenneth T. Cuccinelli II, the former attorney general of Virginia. Bruce Fein, a former Reagan administration attorney, is also among the lawyerson the case.

The Obama administration has defended the program as lawful, noting that 15 judges on the Foreign Intelligence Surveillance Court have authorized it for 90-day intervals dating back to 2006. A 1979 Supreme Court ruling held that

"metadata" — records showing that calls took place, but not their content — is not protected by the Fourth Amendment.

"We remain confident that the program is legal, as at least 15 judges have previously found," Peter Carr, a Justice Department spokesman, said on Wednesday.

The Bush administration began the bulk call records program in 2001 based on a secret claim of presidential power, and it operated outside of any statutory or judicial framework until the court in 2006 granted a Justice Department motion to issue orders to phone companies for the records. The Justice Department motion was based on the argument that a provision of the Patriot Act that allows the F.B.I. to collect business records deemed relevant to an investigation could allow the N.S.A. to collect records in bulk.

Mr. Paul filed his lawsuit in the Federal District Court for the District of Columbia. In December, Judge Richard J. Leon of that court ruled in a similar lawsuit brought by Larry Klayman, a conservative legal activist, that the program probably violates the Fourth Amendment because its expansive scope makes it different from case considered by the Supreme Court in 1979. The Justice Department has appealed the decision.

In a separate case brought by the American Civil Liberties Union in the Southern District of New York, Judge William H. Pauley III in December concluded that the program is legal and complies with the Fourth Amendment. The A.C.L.U. has appealed that ruling.

There are also similar cases in the Northern District of California and the District of Idaho that are raising similar claims, including litigation in California that dates back to earlier revelations during the Bush administration era about domestic surveillance programs and has been stalled in disputes over state secrets.

A version of this article appears in print on February 13, 2014, on page A19 of the New York edition with the headline: Rand Paul Sues Over Phone Program.

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

POLITICS

Spy Chief Says Snowden Took Advantage of 'Perfect Storm' of Security Lapses

By DAVID E. SANGER and ERIC SCHMITT FEB. 11, 2014

WASHINGTON — The director of national intelligence acknowledged Tuesday that nearly a year after the contractor Edward J. Snowden "scraped" highly classified documents from the National Security Agency's networks, the technology was not yet fully in place to prevent another insider from stealing top-secret data on a similarly large scale.

The director, James R. Clapper Jr., testifying before the Senate Armed Services Committee, said Mr. Snowden had taken advantage of a "perfect storm" of security lapses. He also suggested that as a highly trained systems administrator working for Booz Allen Hamilton, which provides computer services to the agency, Mr. Snowden knew how to evade the protections in place.

"He knew exactly what he was doing," Mr. Clapper said. "And he was pretty skilled at staying below the radar, so what he was doing wasn't visible."

But Mr. Clapper confirmed the outlines of a New York Times report that the former N.S.A. contractor had used a web crawler, a commonly available piece of software, to sweep up a huge trove of documents.

Mr. Clapper also said, for the first time, that some of the information Mr. Snowden is believed to possess could expose the identities of undercover American operatives as well as foreigners who have been recruited by United States spy agencies. The information Mr. Snowden has released so far through several newspapers and a new digital news organization that began publishing on Monday has not revealed the names of agents or operatives, and it is unclear how much of

that information he took with him when he fled the United States. He is now in Russia.

Under questioning, Mr. Clapper made clear that while the N.S.A. has installed security upgrades, not all locations have the software and warning systems that could detect mass downloads of information. He did not address why the agency was not able to detect the web crawler, which indexed and copied all the data in its path.

He said it was likely Mr. Snowden would have been caught if he had been taking the information from inside N.S.A. headquarters at Fort Meade, Md., instead of at an outpost in Hawaii.

"We are going to proliferate deployment of auditing and monitoring capabilities to enhance our insider threat detection," he said. Such systems have already been widely used at some intelligence agencies, including the C.I.A., officials said.

The continuing revelations have posed a particular challenge to Mr. Clapper, a retired Air Force general and longtime intelligence expert, who has made no secret of his dislike for testifying in public. Critics have charged that he deliberately misled Congress and the public last year when asked if the intelligence agencies collected information on domestic communications. He was forced by the Snowden revelations to correct his statements, and he has been somewhat more careful in his testimony.

On Tuesday, for example, he warned that "there are no mousetraps that we could say that we can guarantee that we'll never have another Edward Snowden."

"Our whole system is based on personal trust," he continued.

Over the long term, Mr. Clapper said, all 16 of the nation's intelligence agencies will put a complex system in place that is intended to tag every piece of information in their databases, and then tag who accesses it. That would allow a kind of real-time monitoring missing when Mr. Snowden was freely moving through the N.S.A. system.

The agency has imposed other rules intended to sharply restrict the sharing and downloading of top-secret material.

First is a "two-man rule" — based on the model of how nuclear weapons are handled — that requires two computer systems administrators to work

simultaneously when they are inside systems that contain highly classified material.

At Tuesday's hearing, Mr. Clapper and Lt. Gen. Michael T. Flynn, the director of the Defense Intelligence Agency, also disclosed that American analysts believe that Iran will be ready to test an intercontinental ballistic missile by next year, a crucial milestone in the country's military program. It will still be an undetermined amount of time before Iran will be able to perfect the important next step of designing and miniaturizing a nuclear weapon to fit atop a long-range missile, Mr. Clapper said.

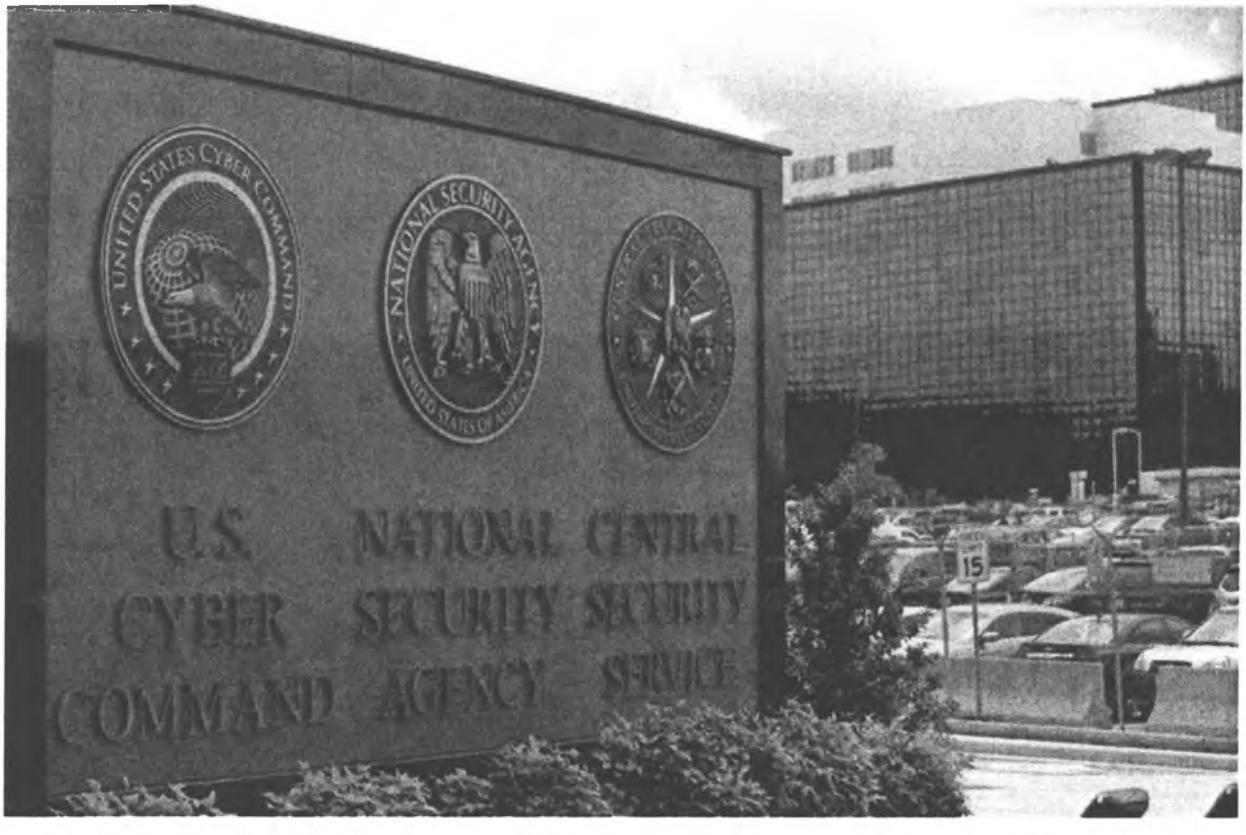
A version of this article appears in print on February 12, 2014, on page A8 of the New York edition with the headline: Data Security and Snowden in Testimony of Spy Chief.

Anchorage Daily News

Americans find swift stonewall on whether NSA vacuumed their data

By Marisa Taylor and Jonathan S. Landay

McClatchy Washington Bureau February 11, 2014



The sign outside the National Security Agency (NSA) campus in Fort Meade, Md.

PATRICK SEMANSKY — ASSOCIATED PRESS

WASHINGTON — Since last year's revelations about the National Security Agency's massive communications data dragnets, the spy agency has been inundated with requests from Americans and others wanting to know if it has files on them. All of them are being turned down .

The denials illustrate the bind in which the disclosures have trapped the Obama administration. While it has pledged to provide greater transparency about the NSA's communications collections, the NSA says it cannot respond to individuals' requests without tipping off terrorists and other targets.

As a result, Americans whose email and telephone data may have been improperly vacuumed up have no way of finding that out by filing open records requests with the agency. Six McClatchy reporters who filed requests seeking any information kept by the NSA on them all received the same response.

"Were we to provide positive or negative responses to requests such as yours, our adversaries' compilation of the information provided would reasonably be expected to cause exceptionally grave damage to the national security," the NSA wrote last month in response to a McClatchy national security reporter who requested his own records. "Therefore, your request is denied because the fact of the existence or non-existence of responsive records is a currently and properly classified matter."

In an apparent reaction to former NSA contractor Edward Snowden's revelations of the NSA's data collections, the number of open records requests filed with the agency more than tripled – from 1,065 to 4,060 – between 2010 and 2013, according to data supplied by the NSA. The denial rate during the same period skyrocketed from an estimated 33 percent to 82 percent because of the higher number of people seeking their own intelligence records. The NSA does approve other types of records requests, such as academics asking for historic records and former workers seeking their employment records.

The high rejection rate of requests seeking individuals' own records sharply contrasts with Director of National Intelligence James R. Clapper's pledge to "lean in the direction of transparency, wherever and whenever we can." It also clashes with the NSA's own public assertion that laws enacted in 1974 entitle "individuals to access federal agency records or to request an amendment to records that are maintained in a file retrievable by an individual's name."

In what is known as a Glomar denial, the NSA and other federal agencies can respond to records requests that by acknowledging the existence of relevant documents, vital secrets would be disclosed. The term stems from a salvage ship, the Glomar Explorer, which was built with the secret mission of recovering a Soviet nuclear submarine that sank in the Pacific Ocean in 1968.

A subsequent Freedom of Information court suit seeking CIA records on the operation established the loophole when a court upheld the CIA's refusal to confirm or deny the existence of those files on national security grounds.

"Theoretically, these agencies could argue that al Qaida could get everyone on Earth to file a request (for documents) and by process of elimination find out who they're really spying on," said Kel McClanahan, an attorney who specializes in suing intelligence agencies under open records laws. "It may be a ludicrous argument, but it's one that the agencies are able to assert."

NSA spokeswoman Vanee Vines said that although her agency must deny individuals' requests for their own intelligence files, her agency releases as much information as it deems possible in other cases.

"The administration's push for transparency is taken very seriously by the FOIA (Freedom of Information Act) Office at NSA," she said. "Because it is not possible to use discretion to release classified information, the FOIA Office does its best to release other information that could potentially be protected under another exemption if a specific harm to the agency is not identified."

Vines also said the numbers cited by McClatchy might be misleading because they do not reveal the number of pages of documents or the significance of the information released. The number of cases where the NSA released all of the documents requested has increased from 49 in 2010 to 82 in 2013, she pointed out.

"Looking at the growing numbers of partial denials or full denials does not mean that NSA is releasing less information," Vines said.

Some transparency advocates, however, said the NSA's ability to sidestep individuals' requests allows the agency to hide its own abuses.

"This is part of the reason why intelligence agencies are spiraling out of control," said Mark Rumold, an attorney with the Electronic Frontier Foundation, a nonprofit group that has pressed the administration to release documents related to surveillance. "These agencies have an ability to operate in utter secrecy."

Documents released by the administration in response to Snowden's leaks have confirmed that the NSA violated its own rules in some cases, including by improperly collecting at least 56,000 domestic emails as part of its massive surveillance program to combat terrorism. A federal court ruled the program unconstitutional, forcing the NSA to change its practices by segregating collections most likely to contain Americans' emails.

The NSA has not publicly revealed details about those cases, however.

Other agencies have kept such collection under wraps as well.

The Drug Enforcement Administration trained its agents how to conceal evidence used in criminal investigations but gathered from various sources, including from NSA intercepts, the Reuters news agency found last year. As a result, the DEA did not notify defendants and even some prosecutors and judges how it had obtained the evidence.

Separately, the Justice Department had concluded that some criminal defendants did not need to be told about NSA surveillance unless email or telephone records gathered during the intercepts were filed as evidence in a criminal case, according to a New York Times report. The policy applied to surveillance authorized under the 2008 law that permitted warrantless eavesdropping on overseas communications.

After media reports drew attention to the loophole, the Justice Department late last year for the first time notified a criminal defendant that evidence against him would include NSA intercepts. The defendant, Jamshid Muhtorov, was accused in 2012 of providing material support to an Uzbek terrorist group. The American Civil Liberties Union is now seeking to have the evidence thrown out as part of its challenge to the constitutionality of the NSA's programs.

During the George W. Bush administration, the Justice Department's inspector general uncovered widespread abuses in FBI programs that relied on administrative or emergency orders to obtain telephone records. As a result of the scrutiny, the FBI disclosed in 2008 that it had improperly collected the phone records of Washington Post and New York Times reporters four years earlier. It's unknown whether other journalists have been monitored improperly.

Last month, the FBI refused to rule out whether it had information about several McClatchy journalists, although it's likely that the FBI had records at some point related to one of the reporters. In 2007, the FBI opened a leak investigation to determine the sources for the reporter's stories on a public corruption investigation.

"We were unable to identify main file records," the bureau said in its responses to that reporter and others, adding that it could neither confirm nor deny that any of the journalists were on watch lists.

To prevent future surveillance abuses, Congress might need to allow certain categories of American citizens to request their records, such as in cases where there is evidence of misconduct by an agency, some experts said.

"You can't do effective oversight of NSA surveillance on a retail basis by submitting lots and lots of individual Freedom of Information Act requests," said Steven Aftergood, head of the Federation of the American Scientists' Project on Government Secrecy. "This is a policy issue that needs to be debated and resolved in Congress."

Email: mtaylor@mcclatchydc.com; jlanday@mcclatchydc.com.

ADN.com

Anchorage Daily News

Snowden used low-cost tool to best NSA

By DAVID E. SANGER and ERIC SCHMITT

The New York TimesFebruary 8, 2014

WASHINGTON -- Intelligence officials investigating how Edward J. Snowden gained access to a huge trove of the country's most highly classified documents say they have determined that he used inexpensive and widely available software to "scrape" the National Security Agency's networks, and he kept at it even after he was briefly challenged by agency officials.

Using "Web crawler" software designed to search, index and back up a website, Snowden "scraped data out of our systems" while he went about his day job, according to a senior intelligence official.

"We do not believe this was an individual sitting at a machine and downloading this much material in sequence," the official said. The process, he added, was "quite automated."

The NSA's mission includes protecting the nation's most sensitive military and intelligence computer systems from cyberattacks, especially the sophisticated attacks that emanate from Russia and China. Snowden's "insider attack," by contrast, was hardly sophisticated and should have been easily detected, investigators found.

Moreover, Snowden succeeded nearly three years after the WikiLeaks disclosures, in which military and State Department files, of far less sensitivity, were taken using similar techniques.

A Web crawler, also called a spider, automatically moves from website to website, following links embedded in each document and can be programmed to copy everything in its path.

From his first days working as a contractor inside the NSA's underground Hawaii facility for Dell, a computer maker, and then at a different Hawaiian location for Booz Allen Hamilton, a technology consulting firm that sells and operates computer security services used by the government, Snowden learned something critical about the NSA's culture: While the organization built enormously high electronic barriers to keep out foreign invaders, it had rudimentary protections against insiders.

"Once you are inside the assumption is that you are supposed to be there, like in most organizations," said Richard Bejtlich, the chief security strategist for FireEye, a Silicon Valley

computer security firm, and a senior fellow at the Brookings Institution. "But that doesn't explain why they weren't more vigilant about excessive activity in the system."

Officials said the Web crawler functioned like Googlebot, a widely used Web crawler that Google developed to find and index new pages on the web. What officials cannot explain is why the presence of such software in a highly classified system was not an obvious tip-off to unauthorized activity.

ABA Journal.com

NSA phone records collection program is illegal and ineffective, government oversight board says

Posted Jan 23, 2014 2:34 PM CST
By Martha Neil

A National Security Agency program that collects and stores so-called metadata on nearly every U.S. phone call is both illegal and largely ineffective, the majority of a bipartisan executive branch agency concluded in a lengthy report (PDF) released Thursday.

"We have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counter-terrorism investigation," writes the Privacy and Civil Liberties Oversight Board. Three of the five members agreed with the report's conclusions and two disagreed, the Associated Press reports.

The majority said the program, which collects records of phone numbers, when calls were made and how long they lasted, as well as similar information about emails, isn't authorized by Section 215 of the Patriot Act as proponents claim, and that they may also violate constitutional protections concerning free speech, unreasonable searches and seizures and privacy.

"When the government collects all of a person's telephone records, storing them for five years in a government database that is subjected to high-speed digital searching and analysis, the privacy implications go far beyond what can be revealed by the metadata of a single telephone call," the majority stated. It includes the board's executive director David Medine; a former federal judge, Patricia Wald; and James Dempsey, an advocate for civil liberties, the AP reported.

In the minority were two former Department of Justice lawyers in the Bush administration, Rachel Brand and Elisebeth Collins Cook. They said the surveillance program is lawful and necessary.

A White House spokeswoman said Thursday that "the administration believes the program is lawful," but that President Barack Obama "believes we can and should make changes in the program that will give the American people greater confidence in it." The president has previously announced that he will limit the surveillance program, as an earlier ABAJournal.com post details.

The board lacks enforcement power, so its findings lend weight to a privacy debate over the phone records surveillance program but are not expected to result in any immediate change, CNN reports.

U.S. Relaxes Some Data Disclosure Rules

By MATT APUZZO and NICOLE PERLROTHJAN. 27, 2014

WASHINGTON — The Obama administration says it will allow Internet companies to give customers a better idea of how often the government demands their information, but will not allow companies to disclose what is being collected or how much.

The new rules — which have prompted Google, Microsoft, Yahoo and Facebook to drop their respective lawsuits before the nation's secret surveillance court — also contain a provision that bars start-ups from revealing information about government requests for two years.

Attorney General Eric H. Holder Jr. and James R. Clapper, director of national intelligence, said the new declassification rules were prompted by President Obama's speech on intelligence reform earlier this month.

"Permitting disclosure of this aggregate data addresses an important area of concern to communications providers and the public," Mr. Holder and Mr. Clapper said in a joint statement.

The companies' dispute began last year after a former government contractor, Edward J. Snowden, revealed that F.B.I. and National Security Agency surveillance programs rely heavily on data from United States email providers, video chat services and social networking companies.

"We filed our lawsuits because we believe that the public has a right to know about the volume and types of national security requests we receive," a representative for Google, Microsoft, Yahoo and Facebook said in a joint statement. "While this is a very positive step, we'll continue to encourage Congress to take additional steps to address all of the reforms we believe are needed."

Privacy advocates, however, say the new rule will prevent the public from knowing if the government is snooping on an email platform or chat service provided by a young tech outfit.

Sometimes, F.B.I. agents demand data with administrative subpoenas known as national security letters. Other times, the Justice Department makes the demand under the authority of the surveillance court but without a specific warrant.

Either way, the justification is typically secret and companies are prohibited from saying much.

The companies wanted to be able to say how many times they received court orders, known as FISA orders, for the Foreign Intelligence Surveillance Act. The government opposed that.

Currently, they are allowed to disclose only the number of administrative subpoenas known as national security letters, but only in increments of 1,000. That made it impossible for users to know whether government agents grabbed data from their email provider once or 999 times.

Companies say that has hurt their businesses. Forrester Research projected the fallout from Mr. Snowden's disclosures could cost the so-called cloud computing industry as much as $180 billion — a quarter of its revenue — by 2016.

Under the new agreement, companies will be able to disclose the existence of FISA court orders. But they must choose between being more specific about the number of demands or about the type of demands.

Companies that want to disclose the number of FISA orders and national security letters separately can do so as long as they publish only in increments of 1,000.

Or, companies can narrow the figure to increments of 250 if they lump FISA court orders and national security letters together.

The technology firms will be allowed to publish the information every six months, with a six-month delay. So data published at midyear would cover the last half of the previous year.

Companies will also be allowed to release the number of "selectors" — user names, email addresses or Internet addresses, for instance — that the government sought information about.

On Monday, Apple became the first technology company to amend its latest transparency report to reflect the new guidelines.

The Justice Department had endorsed the new rules months ago but intelligence officials argued they still revealed too much. But the new rule for start-ups persuaded intelligence officials, a United States official with knowledge of the discussions said. The Justice Department proposed the changes to the companies late last week and, by the end of the weekend, they agreed to drop their case before the FISA court.

Privacy advocates point out that the new rules still fall short of various proposals before Congress, including the Surveillance Order Reporting Act, a bill introduced by Zoe Lofren, Democrat of California, and several other bills proposed by both Democrats and Republicans.

"The bottom line is that this is a positive step forward but still falls short of proposals before Congress right now," said Harley Geiger, a deputy director for the Center for Democracy and Technology. "It's a good step, but a temporary step towards greater transparency."

But Ladar Levison, the founder of Lavabit, a secure email service used by Mr. Snowden, said the new rules cast doubt on young companies and didn't provide the information consumers really need.

"They could be ordered to turn over their source code to the government. A single request could cover 1,000 different user accounts," Mr. Levison

said. "Just simply disclosing the number of FISA court orders doesn't tell you how pervasive the request is or how much information is being turned over."

UNITED STATES GOVERNMENT
Memorandum

OC-034-12

DATE: 3 May 2012

REPLY TO
ATTN OF: SID Oversight & Compliance

SUBJECT: (U//FOUO) NSAW SID Intelligence Oversight (IO) Quarterly Report – First Quarter Calendar Year 2012 (1 January – 31 March 2012) – EXECUTIVE SUMMARY

TO: SIGINT Director

I. (U) Overview

(U//FOUO) The attached NSAW SID Intelligence Oversight (IO) Quarterly Report for the First Quarter Calendar Year 2012 (1 January – 31 March 2012) identifies NSAW SID compliance with E.O. 12333, DoD Regulation 5240.1-R, NSA/CSS Policy 1-23, USSID SP0018, and all related policies and regulations.

(U//FOUO) Detailed incident narratives are provided in the attached annexes. The number of incidents in each category and a reference to the annex related to each incident category are contained in the body of the report.

(U//FOUO) As part of SID Oversight and Compliance's (SV) charge to provide comprehensive trends and analysis information as it pertains to incidents of non-compliance, this Executive Summary provides analysis and evaluation of incidents reported throughout the current quarter to better address the "whys" and "hows" behind NSAW SID's compliance posture.

(U//FOUO) Section II, Metrics, has been broken down into several sub-sections: metrics and analysis of NSAW SID-reported incidents by authority, type, root cause, and organization. Also included is an assessment of how incidents were discovered (i.e., methods of discovery) for SID-reported incidents (see **Figure 7**).

(U//FOUO) Significant Incidents of Non-compliance and Report Content follow in Sections III and IV, respectively.

(S//REL) Overall, the number of incidents reported during 1QCY12 increased by 11% as compared to the number of incidents reported during 4QCY11. This included a rise in the number of E.O. 12333 incidents, as well as for incidents across all FISA authorities. The majority of incidents in all authorities were database query incidents due to human error. Of note, S2 continued to be the NSAW SID organization with the largest number of reported incidents (89%), although S2 experienced an overall decrease in reported incidents. SV noted an overall improvement in timeliness regarding 1QCY12 IO Quarterly Report submissions from the SID elements.

II. (U) Metrics

a. (U//FOUO) NSAW SID-reported Incidents by Authority

(TS//SI//REL TO USA, FVEY) **Figures 1a-b** compares all categories of NSAW SID-reported incidents (collection, dissemination, unauthorized access, and retention) by Authority for 2QCY11 – 1QCY12. From 4QCY11 to 1QCY12, there was an overall increase in incidents of 11%. There was also an increase of 11% for both E.O. 12333 and FISA incidents. The increase in incidents reported for 1QCY12 was due to an increase in the number of reported Global System for Mobile Communications (GSM) roamer[1] incidents, which may be attributed to an increase in Chinese travel to visit friends and family for the Chinese Lunar New Year holiday.

(U//FOUO) **Figure 1a**: Table of the Number of NSAW SID-reported Incidents by Authority

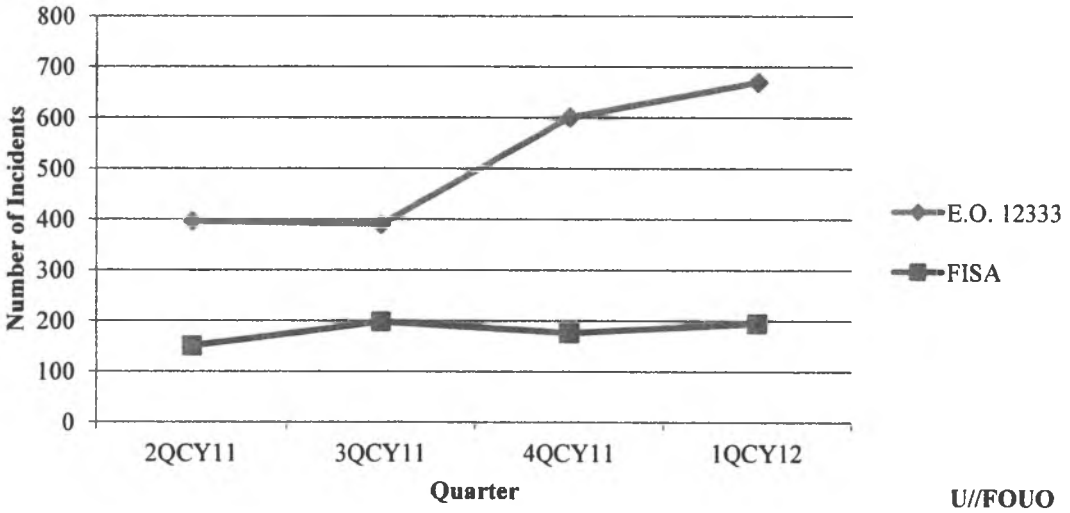
(U//FOUO)

	2QCY11	3QCY11	4QCY11	1QCY12
E.O. 12333	396	390	601	670
FISA	150	198	176	195
TOTAL	**546**	**588**	**777**	**865**

(U//FOUO)

(U//FOUO) **Figure 1b**: Line Graph of the Number of NSAW SID-reported Incidents by Authority

U//FOUO



U//FOUO

(TS//SI//NF) **FISA Incidents:** As reflected in **Figures 1a-b**, during 1QCY12, NSAW SID reported a total of 195 FISA incidents, 185 of which were associated with unintentional collection. NSAW SID also reported 6 incidents of unintentional dissemination under FISA authority and 4 incidents of unauthorized access to Raw

[1] (U//FOUO) Roaming incidents occur when a selector associated with a valid foreign target becomes active in the U.S.

SIGINT FISA data. **Figure 2** illustrates the most common root causes for incidents involving FISA authorities as determined by SV.

- 63% (123) of 1QCY12 FISA incidents can be attributed to Operator Error as the root cause, and involved:
  - Resources (i.e., inaccurate or insufficient research information and/or workload issues (60);
  - Lack of due diligence (i.e., failure to follow standard operating procedures) (39);
  - Human error (21) which encompassed:
    - Broad syntax (i.e., no or insufficient limiters / defeats / parameters) (12);
    - Typographical error (6);
    - Query technique understood but not applied (2); and
    - Incorrect option selected in tool (1); and
  - Training and guidance (i.e., training issues) (3).

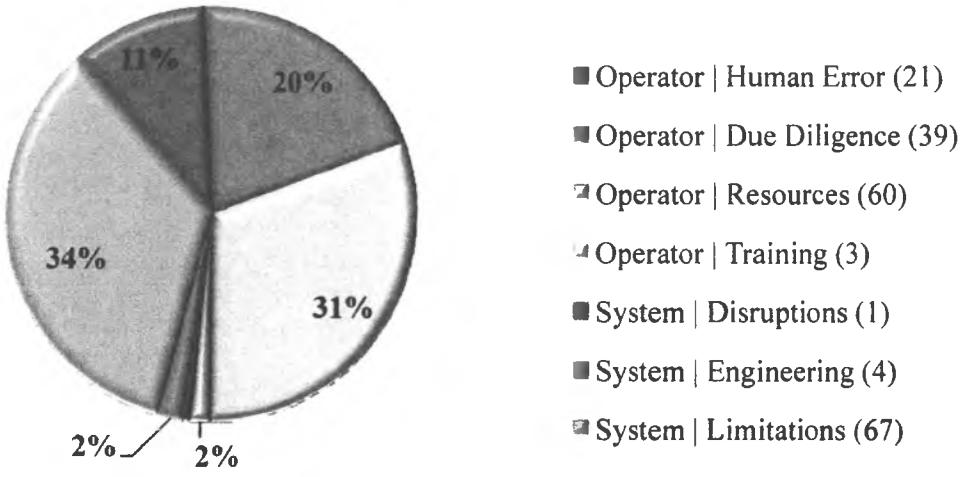
(U//FOUO) The Resources root cause category accounted for the largest percentage of Operator Error incidents under FISA authorities for 1QCY12. Analysis identified that these incidents could be reduced if analysts had more complete and consistent information available about selectors and/or targets at the time of tasking and if analysts consistently applied rules for conducting queries.

- 37% (72) of 1QCY12 FISA incidents can be attributed to System Error as the root cause, and involved:
  - System limitations (i.e., system lacks the capability to 'push' real-time travel data out to analysts, system/device unable to detect changes in user) (67);
  - System engineering (i.e., system/database developed without the appropriate oversight measures, data flow issues, etc.) (4); and,
  - System disruptions (i.e., glitches, bugs, etc.) (1).

(U//FOUO) The System Limitations root cause category accounted for the largest percentage of System Error incidents under FISA authorities for 1QCY12. The largest number of incidents in the System Limitations category account for roamers where there was no previous indications of the planned travel. These incidents are largely unpreventable. Consistent discovery through the Visitor Location Register (VLR) occurs every quarter and provides analysts with timely information to place selectors into candidate status or detask. Analysis identified that these incidents could be reduced if analysts removed/detasked selectors more quickly upon learning that the status of the selector had changed and more regularly monitored target activity. This analysis indicates that continued research on ways to exploit new technologies and researching the various aspects of personal communications systems to include GSM, are an important step for NSA analysts to track the travel of valid foreign targets.

(U//FOUO) **Figure 2**: 1QCY12 FISA Incidents – Root Causes

U//FOUO



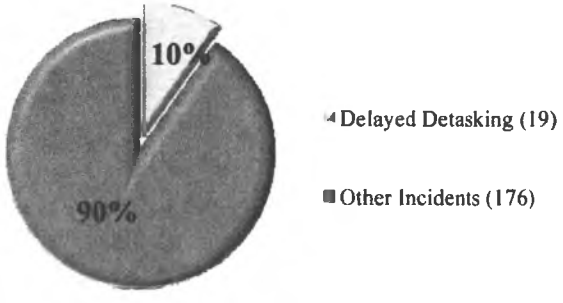
Total: 195

U//FOUO

(TS//SI//REL TO USA, FVEY) Delayed Detasking **FISA Incidents:** As reflected in **Figures 1a-b**, during 1QCY12, NSAW SID reported a total of 195 FISA incidents. 19 (10%) of the total FISA incidents were associated with detasking delays. Of the 19 delayed detasking incidents, 12 (63%) of these incidents occurred under NSA FISA Authority, 5 (27%) occurred under FAA 702 Authority, 1(5%) occurred under FAA 704 Authority, and 1 (5%) occurred under FAA 705(b) Authority. **Figure 3a** illustrates the detasking delay incidents versus all other FISA incidents reported during 1QCY12. **Figure 3b** illustrates the detasking delay incidents by FISA Authority reported during 1QCY12.

(U//FOUO) Figure 3a: 1QCY12 Detasking FISA Incidents vs. All other FISA incidents

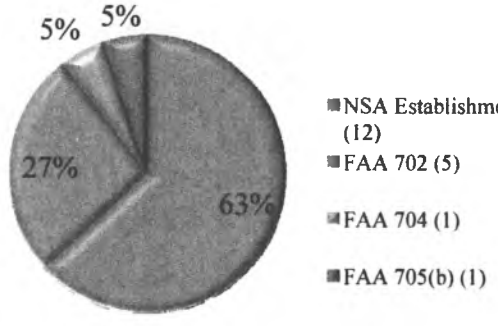
U//FOUO



Total: 195

(U//FOUO) Figure 3b: 1QCY12 FISA Incidents by Authority – Delayed Detaskings

U//FOUO



Total: 19

U//FOUO

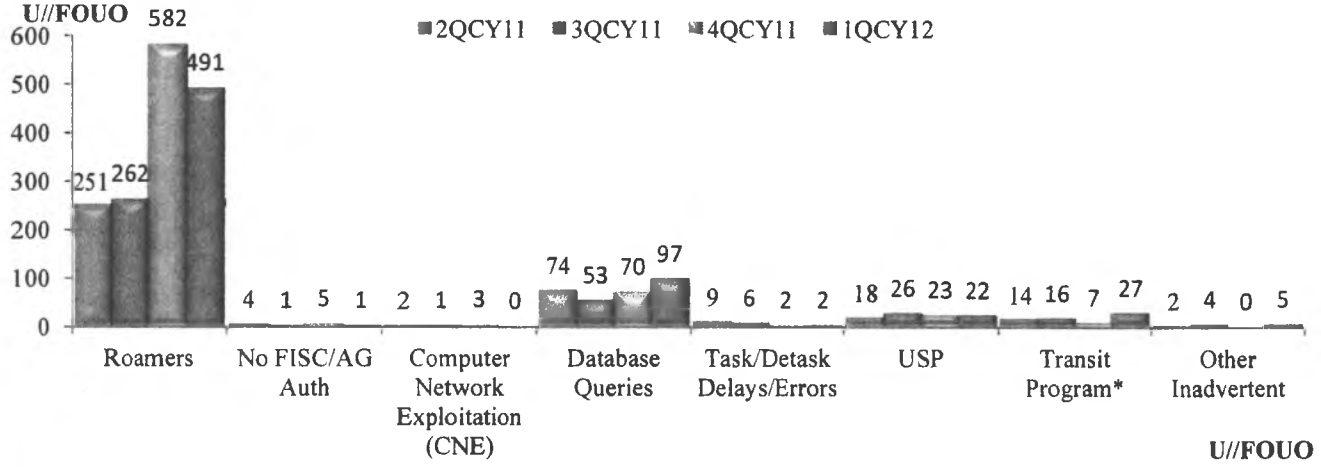
U//FOUO

(TS//SI//REL TO USA, FVEY) As depicted in Figures 3a and 3b, of the 19 delayed detasking FISA incidents, 15 (79%) resulted from a failure to detask all selectors, 2 (11%) resulted from analyst not detasking when required, 1 (5%) resulted from partner agency error, and 1 (5%) resulted from all tasking not terminated (e.g., dual route).

b. NSAW SID-reported Collection Incidents by Sub-Type and Authority

(U//FOUO) **Figures 4a-b** depicts NSAW SID-reported collection incidents by Authority (E.O. 12333 and all FISA Authorities), and identifies the primary sub-types for those incidents. An explanation of the more prominent collection incident sub-types follows the graphs.

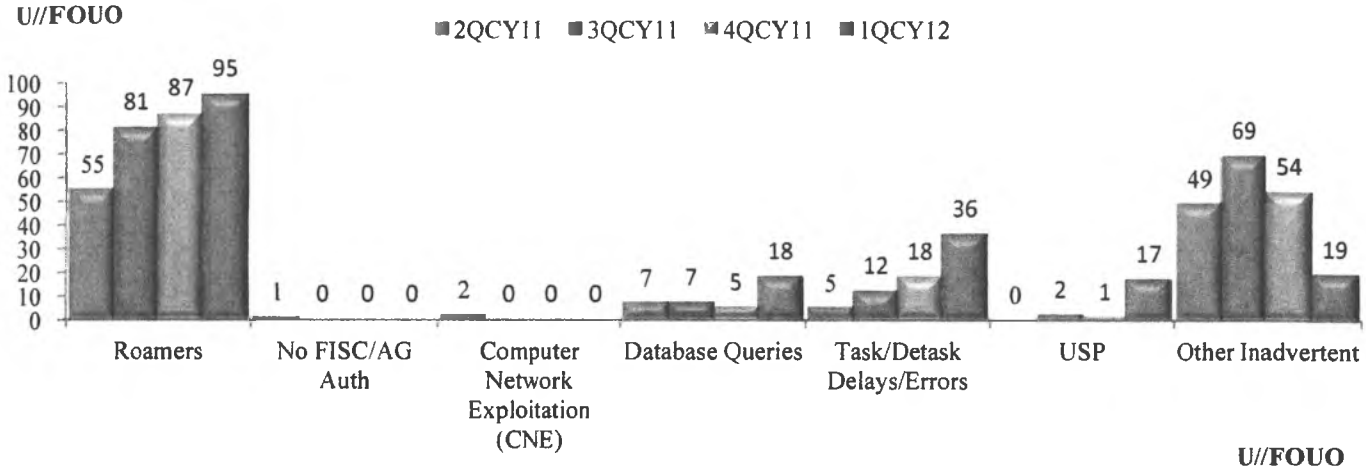
(U//FOUO) **Figure 4a**: NSAW SID-reported Collection Incidents Under E.O. 12333 Authority



(U//FOUO) **Figure 4a:** During 1QCY12, NSAW SID reported a 39% increase of database query incidents under E.O. 12333 Authority. Human Error accounted for 74% of E.O.12333 database query incidents.

(TS//SI//REL TO USA, FVEY) **International Transit Switch Collection*:** International Transit switches, FAIRVIEW (US-990), STORMBREW (US-983), ORANGEBLOSSOM (US-3251), and SILVERZEPHYR (US-3273), are Special Source Operations (SSO) programs authorized to collect cable transit traffic passing through U.S. gateways with both ends of the communication being foreign. When collection occurs with one or both communicants inside the U.S., this constitutes inadvertent collection. From 4QCY11 to 1QCY12, there was an increase of transit program incidents submitted from 7 to 27, due to the change in our methodology for reporting and counting of these types of incidents. (*See Annex G in SID's 1QCY12 IO Quarterly Report for additional details regarding these incidents.)

(U//FOUO) **Figure 4b**: NSAW SID-reported Collection Incidents Under All FISA Authorities



(U//FOUO) **Figure 4b:** During 1QCY12, NSAW SID reported an increase of 9% of roamer incidents under all FISA Authorities. There was also a 260% increase in database query FISA Authority incidents during 1QCY12. Human Error accounted for the majority of all FISA Authorities database query incidents (74%).

(U//FOUO) **Roamers:** Roaming incidents occur when valid foreign target selector(s) are active in the U.S. Roamer incidents continue to constitute the largest category of collection incidents across E.O. 12333 and FAA authorities. Roamer incidents are largely unpreventable, even with good target awareness and traffic review, since target travel activities are often unannounced and not easily predicted.

(S//SI//NF) **Other Inadvertent Collection:** Other inadvertent collection incidents account for situations where targets were believed to be foreign but who later turn out to be U.S. persons and other incidents that do not fit into the previously identified categories.

(TS//SI//REL TO USA, FVEY) **Database Queries:** During 1QCY12, NSAW SID reported a total of 115 database query incidents across all Authorities, representing a 53% increase from 4QCY11. E.O. 12333 Authority database query incidents accounted for 84% (97) of the total, and all FISA Authorities database query incidents accounted for 16% (18).

(U//FOUO) **Figure 5** illustrates the most common root causes for incidents involving database queries as determined by SV.

- 99% (114) of the 1QCY12 database query incidents are attributed to Operator Error as the root cause, and involved:
  - Human error (85) which encompassed:
    - Broad syntax (i.e., no or insufficient limiters / defeats / parameters) (55);
    - Typographical error (17);
    - Boolean operator error (6);
    - Query technique understood but not applied (4);
    - Not familiar enough with the tool used for query (2); and

- Incorrect option selected in tool (1)
- Lack of due diligence (i.e., failure to follow standard operating procedure) (13)
- Training and guidance (i.e., training issues) (9); and
- Resources (i.e., inaccurate or insufficient research information and/or workload issues) (7).

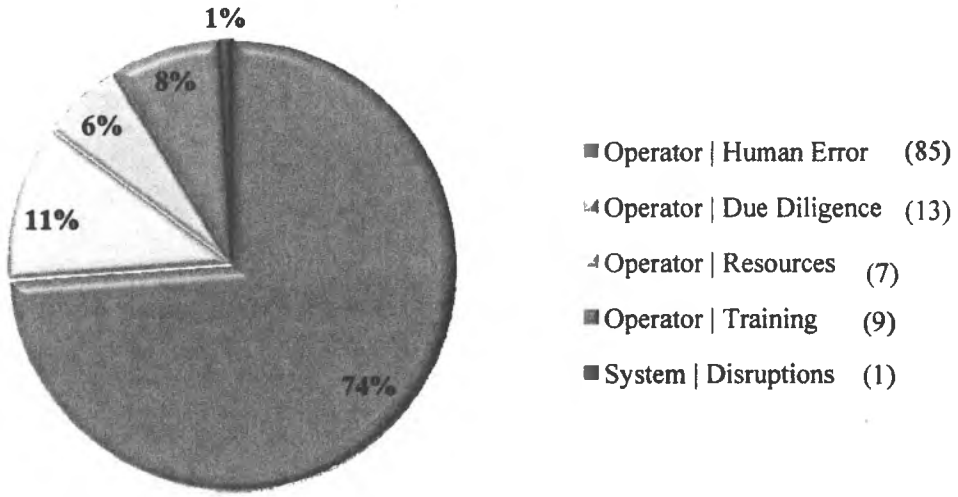
(U//FOUO) The remaining 1 database query incident can be attributed to System Error as the root cause and occurred due to a mechanical error with the tool.

(U//FOUO) Analysis identified that the number of database query incidents could be reduced if analysts more consistently applied rules/standard operating procedures (SOPs) for conducting queries.

(S//SI//NF) Auditors continue to play an important role in the discovery of database query incidents, identifying 70 (61%) of the 115 reported database query incidents.

(U//FOUO) **Figure 5**: 1QCY12 Database Query Incidents – Root Causes

U//FOUO



Total: 115

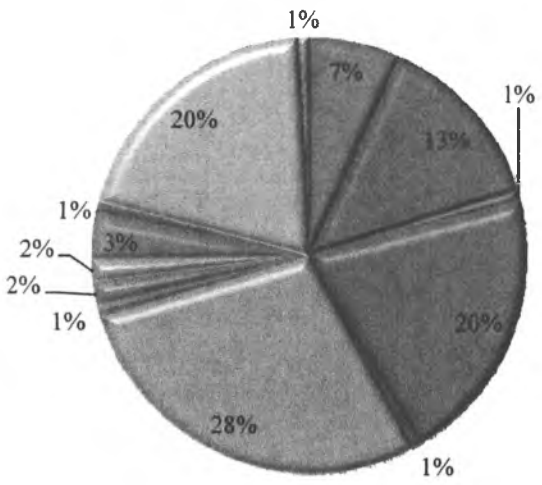
U//FOUO

(TS//SI//REL TO USA, FVEY) Of the 115 database query incidents reported for 1QCY12, **Figure 6** identifies the database involved and the associated percentage of the total. Databases considered to be Source Systems of Record (SSR) have been labeled as such.

(TS//SI//REL TO USA, FVEY) Note that the total number of databases involved in the database query incidents in **Figure 6** does not equal the number of database query incidents reflected in Figure 5 or in the 1QCY12 SID IO Quarterly Report because a database query incident may occur in more than one database.

(U//FOUO) **Figure 6**: 1QCY11 Database Query Incidents – Database(s) Involved

U//FOUO



CLOUD/ABR	(8)
DISHFIRE	(16)
FASTSCOPE	(1)
MARINA (SSR)	(24)
OCTAVE	(1)
PINWALE (SSR)	(34)
SIGINT NAVIGATOR	(1)
TRACFIN	(2)
TRANSX	(2)
TUNINGFORK	(4)
UTT	(1)
XKEYSCORE	(24)
Unknown	(1)

Total: 119

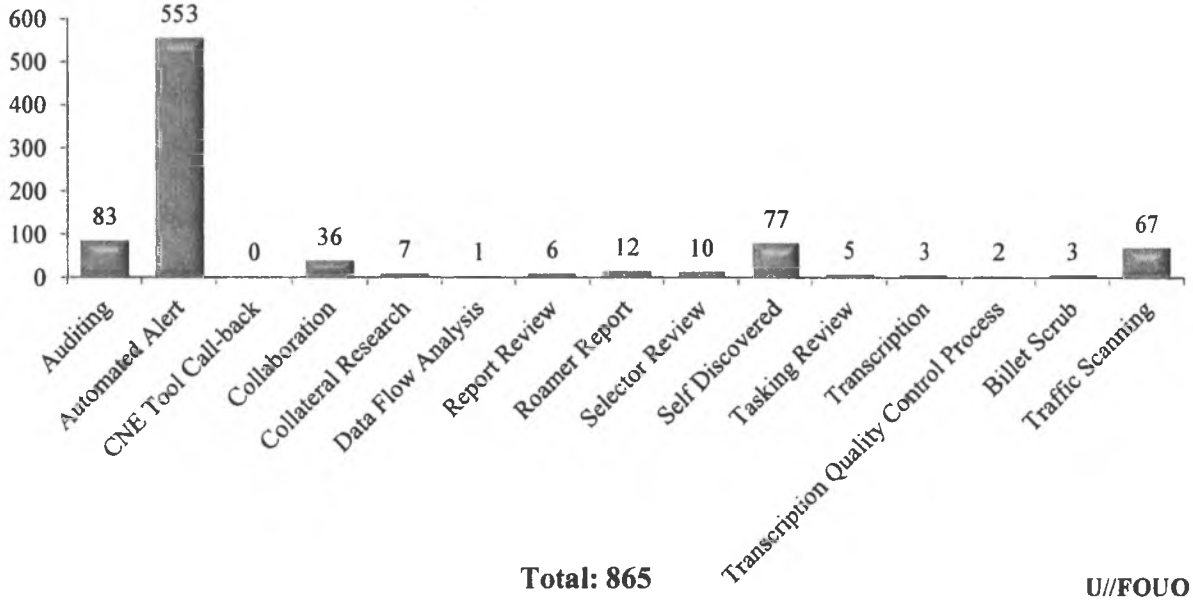
U//FOUO

(U//FOUO) NSAW SID-reported Incidents – Method of Discovery

(U//FOUO) **Figure 7** depicts the most prominent method(s) of discovery for incidents reported by NSAW SID elements for 1QCY12. As SV's assessment of root causes matures, and as corrective measures are implemented, identification of how incidents are discovered will provide additional insight into the effectiveness of those methods.

(U//FOUO) **Figure** 7: 1QCY12 Incidents – How Discovered

U//FOUO



Total: 865

U//FOUO

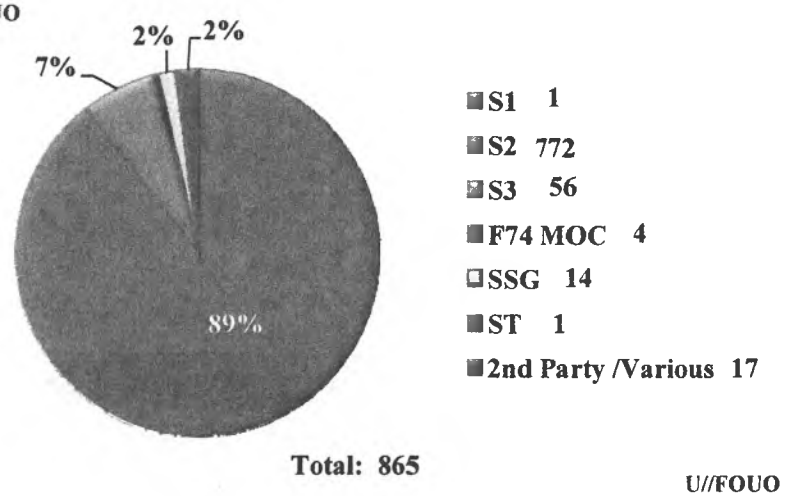
(U//FOUO) For 1QCY12, of the 865 reported incidents, 553 (64%) were discovered by automated alert. 444, (80%) of the 553 incidents that were discovered by automated alert occurred via the VLR and other analytic tools, such as SPYDER, CHALKFUN, and TransX.

c. (U//FOUO) NSAW SID-reported Incidents by Organization

(U//FOUO) **Figure 8** illustrates the total 1QCY12 NSAW SID-reported incidents by primary SID Deputy Directorate (DD) level organization. S2, having the largest NSAW SID contingent of reported incidents, accounted for 89% of the total incidents for the quarter, a proportion consistent with the overall size of the S2 organization. As compared to 4QCY11, S2 experienced an overall 8% reduction in incidents occurrences.

(U//FOUO) **Figure 8**: 1QCY12 Incidents by NSAW SID Organization

U//FOUO



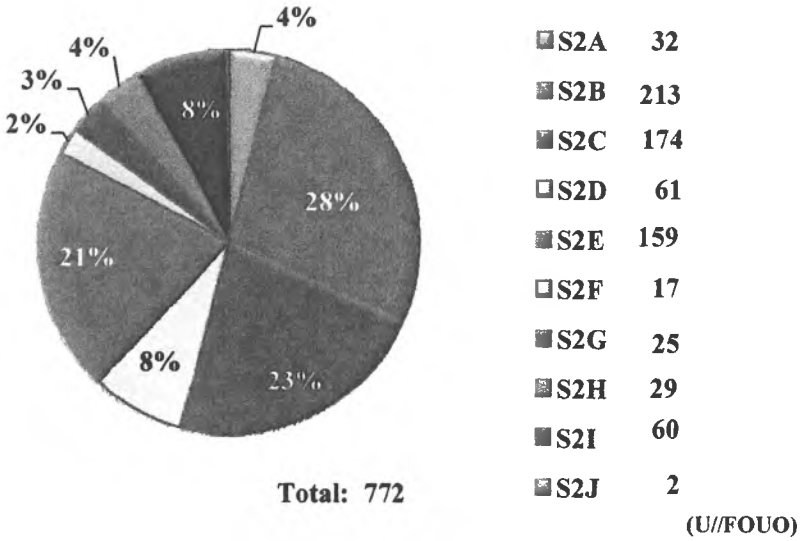
Total: 865

U//FOUO

(U//FOUO) **Figure 9** provides a look into S2 (by Product Line) as the NSAW SID organization with the largest number of reported incidents. For 1QCY12, three Product Lines accounted for 72% of S2's reported incidents. These Product Lines were: the and Korea Division (S2B) with 28% of the reported incidents, the International Security Issues Division (S2C) with 23% of the reported incidents, and the China, and the Office of Middle East & Africa (S2E) with 21% of the incidents. As compared to 4QCY11, this resulted in an increase of 16% for S2B, a reduction of 35% for S2C, and an increase of 9% for S2E. The number of incidents reported by the remaining seven Product Lines held relatively steady from 4QCY11 to 1QCY12.

(U//FOUO) **Figure 9**: 1QCY12 S2 Incidents by Product Line

(U//FOUO)

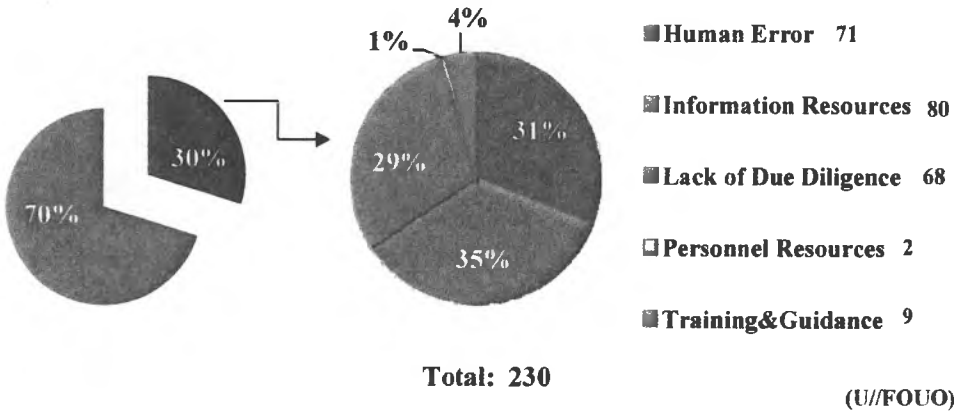


(U//FOUO)

(U//FOUO) **Figures 10a-b** illustrates the operator related (**Figure 10a**) and system related (**Figure 10b**) root causes associated with the 772 incidents reported by S2. 30% of the incidents were due to operator related errors that resulted in an incident. 70% of the incidents were due to system related issues that resulted in an incident.

(U//FOUO) **Figure 10a**: 1QCY12 S2 Incidents – Operator Related Root Causes

(U//FOUO)



(U//FOUO)

(U//FOUO) 30% of the S2-reported incidents during 1QCY12 are attributed to Operator Error as the root cause, and involved:

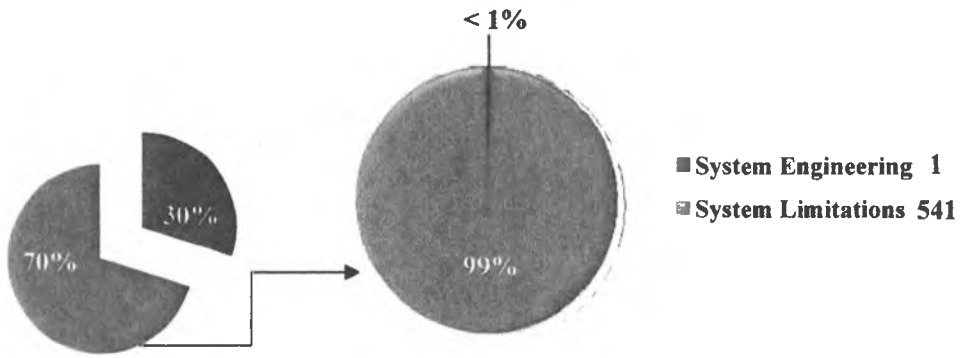
- Resources (i.e., inaccurate or insufficient research information and/or workload issues, and personnel resource issues) (82);

- Human error (i.e., selector mistypes, incorrect realm, or improper query) (71);
- Lack of due diligence (i.e., failure to follow standard operating procedures) (68); and
- Training and guidance (i.e., training issues) (9).

(U//FOUO) Analysis found that analysts could reduce the number of incidents if there was more comprehensive research information available at the time of tasking as well as through better use of defeats, more careful review of data entry to avoid typographical errors and omissions, and by following SOPs more consistently.

(U//FOUO) **Figure 10b**: 1QCY12 S2 Incidents – System Related Root Causes

(U//FOUO)



Total: 542

(U//FOUO)

(U//FOUO) 70% of the S2-reported incidents during 1QCY12 are attributed to system issues as the root cause, and involved:

- System limitations (i.e., system lacks the capability to 'push' real-time travel data out to analysts, system/device unable to detect changes in user) (541); and
- System engineering (i.e., data tagging, configuration, design flaws, etc.) (1).

(TS//SI//REL TO USA, FVEY) System Limitations, the largest percentage of System Error root cause, can be attributed to situations where a valid foreign target is found roaming in the United States without indication in raw traffic.

III. (U) Significant Incidents of Non-compliance

(TS//SI//NF) **Business Record (BR) FISA**. As of 16 February 2012, NSA determined that approximately 3,032 files containing call detail records potentially collected pursuant to prior BR Orders were retained on a server and been collected more than five years ago in violation of the 5-year retention period established for BR collection. Specifically, these files were retained on a server used by technical personnel working with the Business Records metadata to maintain documentation of provider feed data formats and performed background analysis to document why certain contain chaining rules were created. In addition to the BR

work, this server also contains information related to the STELLARWIND program and files which do not appear to be related to either of these programs. NSA bases its determination that these files may be in violation of docket number BR 11-191 because of the type of information contained in the files (i.e., call detail records), the access to the server by technical personnel who worked with the BR metadata, and the listed "creation date" for the files. It is possible that these files contain STELLARWIND data, despite the creation date. The STELLARWIND data could have been copied to this server, and that process could have changed the creation date to a timeframe that appears to indicate that they may contain BR metadata. Additional details regarding this incident can be found in the "Bulk Metadata FISA" Annex, ANNEX R (Item R1) in SID's 1QCY12 IO Quarterly Report.

(S//SI//REL TO USA, FVEY) **Detasking Delay**. Four selectors [redacted] remained active after multiple indications were received that the target held a U.S. green card. On 09 March 2012, a South Asia Language Analysis Branch (S2A51) senior linguist was preparing [redacted] Division) selectors for OCTAVE migration when it was discovered that the tasking record for [redacted] showed that there were four selectors [redacted] that were in active status even though his tasking file indicated he held a U.S. green card as of 03 October 2011. On 09 March 2012, the S2A51 senior linguist detasked the four selectors, and on 13 March 2012, the S2A51 senior linguist requested the 881 cuts in NUCLEON based on collection from those four selectors be purged. On 13 March 2012, a senior reporter in the [redacted] Reporting Branch (S2A52) researched S2A52's locally held file of [redacted] who hold U.S. person status and learned that an S2A52 analyst had indications in intercept on 09 September 201[redacted] might have a U.S. green card. It was also recorded in the same S2A52 file that S2A52 had submitted a request to the Department of Homeland Security (DHS [redacted] (N.B., the date of the S2A52 request to DHS was not recorded) and learned from DHS on 28 September 2011 that [redacted] had obtained a U.S. green card as o[redacted] 2010. The S2A52 senior reporter then checked ANCHORY and discovered that S2A52 had issued 32 reports betwee[redacted] 2010 and [redacted] 2011. On 14 March 2012, S2A5 submitted a request for Retroactive Dissemination Authority for the 32 reports which contained the name of [redacted] The Customer Relationships, Information Sharing Services Branch (S12) approved ISS/BDA-068-12 on 16 March 2012. Serialized dissemination of U.S. person information did occur. On 13 March 2012, the S2A51 senior linguist who found that these number[redacted] had not been detasked reminded the other two members of the Governmental Unified Targeting Tool (UTT) Group for S2A5 to check all S2A5 databases for [redacted] officials who have U.S. (and Second Party person) status before submitting selectors for tasking. Additional details regarding this incident can be found in the Unintentional Collection under E.O. 12333 Authority Annex, "Collection as a Result of Tasking Errors or Detasking Delays", ANNEX E (Item E1) and in the "Unintentional Dissemination of U.S. Person Information Collected Under E.O. 12333, FISA, and FAA Authorities", Annex M (Item M15) in SID's 1QCY12 IO Quarterly Report.

(C//REL TO USA, FVEY) **Unauthorized Access**. On 29 December 2011, a Cryptanalysis and Exploitation (CES)/Office of Target Pursuit (S31174) Branch Chief discovered that CES personnel had likely been inappropriately granted access to NSA Establishment FISA data. Multiple external factors contributed to this situation. First, in 2002, RAGTIME was changed to encompass both NSA Establishment FISA and FBI FISA, but due to insufficient notice regarding this modification, CES continued to apply the earlier rule that RAGTIME applied only to NSA Establishment FISA data. Second, CES relied on the RAGTIME label in CASPORT for granting access to NSA Establishment FISA data but discovered that CASPORT does not accurately reflect NSA Establishment FISA briefing status. Third, CASPORT often lists NSA-FISA in the

"Oversight" section even though this has nothing to do with a particular user's access. CES has alerted its workforce to look in the CASPORT "Briefing" section for the NSA Establishment FISA entry and CES-controlled software is being updated regarding data access control. Additional details regarding this incident can be found in the "Unauthorized Access to Raw SIGINT" Annex, ANNEX P (Item P2) in SID's 1QCY12 IO Quarterly Report.

(U) Report Content

- **Upcoming Initiatives**

(U//FOUO) During CY12, SV plans to develop 'score cards' to capture and illustrate an organization's reported quarterly activities. SV plans to use this information during scheduled feedback sessions with SID reporting organizations to provide a detailed view into specific areas of high interest or concern arising from analyzing IO Quarterly Report metrics.

- **NSAW SID 1QCY12 IOQ Report Challenges:**

(U//FOUO) SV noted an overall improvement in timeliness regarding 1QCY12 IO Quarterly Report submissions from the SID elements. SV received late submissions from SIGDEV Strategy & Governance (SSG) and SID/Deputy Directorate for Data Acquisition (S3), delaying SV's preparation of the NSAW SID IO Quarterly Report. SV will continue to focus on outreach with SSG and S3 in order to ensure more complete and timely report submissions.

[redacted]
Chief, SID Oversight & Compliance

The Facts About the Metadata 'Menace'

by K. Jack Riley
January 26, 2014

photo by Reuters/Larry Downing
Member of the protest group, Code Pink, protests against U.S. President Barack Obama and the NSA before his arrival at the Department of Justice, Jan. 17, 2014

President Obama has announced several significant changes to U.S. counter-terrorism intelligence-collection programs, including an overhaul of the way the National Security Agency stores and accesses telephone metadata. But what has sometimes been overlooked in the firestorm created by Edward Snowden's leaks about the program is a clear definition of what metadata is, and what it is not.

On the eve of the president's announcement, I took part in a daylong session of briefings, discussion and debate at the NSA. The session, arranged by Carnegie Mellon University professor Kiron Skinner and Emily Goldman of the Pentagon's Cyber Command, involved a small group of computer scientists and other researchers and the top leadership of the NSA. The meetings were spectacular for their clarity and candor.

Much of what Snowden leaked has proved controversial, but probably nothing more so than the metadata program authorized by the Patriot Act. This program permits the collection and — under limited circumstances — analysis of metadata on American phone numbers and thus American citizens for counter-terrorism purposes.

Metadata from a phone call include information such as the direction (who called whom), length, date and time. The program does not record the location or the name associated with a call. No one is listening to the call and no content is recorded. And the metadata are segregated and stored separately from all the other signals data the NSA collects.

Here's a typical way the metadata are used: An intelligence community client, say the FBI, will send the NSA an official request for investigation of a certain phone number that it believes might be associated with suspected terrorists. In order to examine the metadata associated with a phone number, the NSA has to "make RAS" — that is, to show "reasonably articulable suspicion."

For a phone number that meets the RAS standard, the NSA can examine metadata two hops, or two call generations, away from the original number. Think of a phone bill that displays calls made and received. It can look at metadata for every phone number on the original bill, plus the phone numbers on the bills for the numbers that show up on the bill of the original number. That's two hops. Among the reforms unveiled by Obama was the reduction in the number of permitted hops from three to two.

What prevents the NSA from relentlessly hopping from one "interesting" number to the next? There are a number of checks: Subsequent generations of metadata and phone numbers cannot be investigated without making RAS on them, which means new review and new approvals; only 22 NSA managers are authorized to approve examination of metadata; the Justice Department audits the program every 90 days; and the program has to undergo reauthorization with the Foreign Intelligence Surveillance Court every quarter. That means at least 15 different federal judges have looked at — and approved — the program since its inception.

What is not happening with the metadata? There's no freewheeling data-mining, no Facebook-style graphing of social networks and no unrestricted exploratory data analysis.

The president has proposed a number of reforms, including requiring judicial approval before the NSA can access metadata. He also proposed a transition that would shift storage of the metadata from NSA to a third party, possibly the telephone companies.

Judicial review of metadata use is already occurring, albeit after the fact in quarterly court reviews. Integrating judicial review into each explicit accessing of the metadata is a prudent and reasonable step, though it has the potential to slow investigations.

At first glance, shifting data-retention responsibilities to a third party might appear to keep Americans' metadata one additional step removed from prying NSA eyes. But there are potential risks associated with this move. Private retention could be technically complex and could slow investigations. Even with the NSA providing storage standards and guidance, the data may be less secure simply because they are spread across more organizations and locations.

The reforms sought by the administration may or may not ease the privacy concerns many Americans have about the metadata collection program. Understanding what metadata is, and isn't, might.

Jack Riley is vice president of the nonpartisan, nonprofit Rand Corp. and director of the RAND National Security Research Division.

This commentary appeared in *Los Angeles Times* on January 26, 2014.

CNN Justice

Judge: NSA domestic phone data-mining unconstitutional

By **Bill Mears** and **Evan Perez**, CNN
updated 8:52 PM EST, Mon December 16, 2013

STORY HIGHLIGHTS

- Snowden says he knew the surveillance would not withstand legal review
- The limited ruling opens the door to possible further legal challenges
- The NSA data-mining can continue, pending a likely appeal
- Classified leaks by Edward Snowden revealed the extent of the data-mining

Washington (CNN) -- A federal judge said Monday that he believes the government's once-secret collection of domestic phone records is unconstitutional, setting up likely appeals and further challenges to the data mining revealed by classified leaker Edward Snowden.
U.S. District Judge Richard Leon said the National Security Agency's bulk collection of metadata -- phone records of the time and numbers called without any disclosure of content -- apparently violates privacy rights.

His preliminary ruling favored five plaintiffs challenging the practice, but Leon limited the decision only to their cases.

NSA phone surveillance unconstitutional?

"I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every citizen for purposes of querying and analyzing it without prior judicial approval," said Leon, an appointee of President George W. Bush. "Surely, such a program infringes on 'that degree of privacy' that the Founders enshrined in the Fourth Amendment."

Leon's ruling said the "plaintiffs in this case have also shown a strong likelihood of success on the merits of a Fourth Amendment claim," adding "as such, they too have adequately demonstrated irreparable injury."

He rejected the government's argument that a 1979 Maryland case provided precedent for the constitutionality of collecting phone metadata, noting that public use of telephones had increased dramatically in the past three decades.

Leon also noted that the government "does not cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the government in achieving any objective that was time-sensitive in nature."

However, he put off enforcing his order barring the government from collecting the information, pending an appeal by the government.
A Justice Department spokesman said Monday that "we believe the program is constitutional as previous judges have found," but said the ruling is being studied.

Democratic Sen. Mark Udall of Colorado, a critic of the NSA data mining, said Leon's ruling showed that "the bulk collection of Americans' phone records conflicts with Americans' privacy rights under the U.S. Constitution and has failed to make us safer."

He called on Congress to pass legislation he proposed to "ensure the NSA focuses on terrorists and spies - and not innocent Americans."
Explosive revelations earlier this year by Snowden, a former NSA contractor, triggered new debate about national security and privacy interests in the aftermath of the September 2001 terrorist attacks.

Snowden's revelations led to more public disclosure about the secretive legal process that sets in motion the government surveillance.
In a statement distributed by journalist Glenn Greenwald, who first reported the leaks, Snowden said he acted on the belief that the mass surveillance program would not withstand a constitutional challenge, and that Americans deserved a judicial review.

"Today, a secret program authorized by a secret court was, when exposed to the light of day, found to violate Americans' rights. It is the first of many," according to Snowden, who is living in Russia under a grant of asylum to avoid prosecution over the leaks in the United States.
Greenwald said the judge's ruling vindicates what Snowden did.

"I think it's not only the right, but the duty of an American citizen in Edward Snowden's situation to come forward, at great risk to himself, and inform his fellow citizens about what it is their government is doing in the dark that is illegal," the journalist told CNN's "Anderson Cooper 360" Monday night.

The NSA has admitted it received secret court approval to collect vast amounts of metadata from telecom giant Verizon and leading Internet companies, including Microsoft, Apple, Google, Yahoo and Facebook.

The case before Leon involved approval for surveillance in April by a judge at the Foreign Intelligence Surveillance Court (FISC), a secret body that handles individual requests for electronic surveillance for "foreign intelligence purposes."

Verizon Business Network Services turned over the metadata to the government.

Leon's ruling comes as the Obama administration completes a review of NSA surveillance in the aftermath of the Snowden leaks.
CNN's Jake Tapper reported Monday that tech company executives would meet with President Barack Obama at the White House on Tuesday to discuss the issue.

Obama plans to sit down with Tim Cook of Apple and Eric Schmidt of Google, as well as executives from Twitter, Microsoft, Facebook, Salesforce, Netflix , Etsy, Dropbox, Yahoo!, Zynga, Sherpa Global, Comcast, LinkedIn and AT&T, a White House official said.
Some of those companies issued a joint letter last week calling on the government to change its surveillance policies in the wake of the Snowden revelations.

Last month, the Supreme Court refused to take up the issue when it denied a separate petition, which was filed by the Electronic Information Privacy Center. Prior lawsuits against the broader NSA program also have been unsuccessful.

Days after the Snowden disclosure in June, some Verizon customers filed legal challenges in the D.C. federal court.
The left-leaning American Civil Liberties Union also filed a separate, pending suit in New York federal court.

Under the Foreign Intelligence Surveillance Act of the 1970s, the secret courts were set up to grant certain types of government requests-- wiretapping, data analysis, and other monitoring of possible terrorists and spies operating in the United States.
The Patriot Act that Congress passed after the 9/11 attacks broadened the government's ability to conduct anti-terrorism surveillance in the United States and abroad, eventually including the metadata collection.

In order to collect the information, the government has to demonstrate that it's "relevant" to an international terrorism investigation.
However, the 1978 FISA law lays out exactly what the special court must decide: "A judge considering a petition to modify or set aside a nondisclosure order may grant such petition only if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person."

In defending the program, NSA Director Gen. Keith Alexander told the Senate Judiciary Committee last week that "15 separate judges of the FISA Court have held on 35 occasions that Section 215 (of the Patriot Act) authorizes the collection of telephony metadata in bulk in support of counterterrorism investigations."

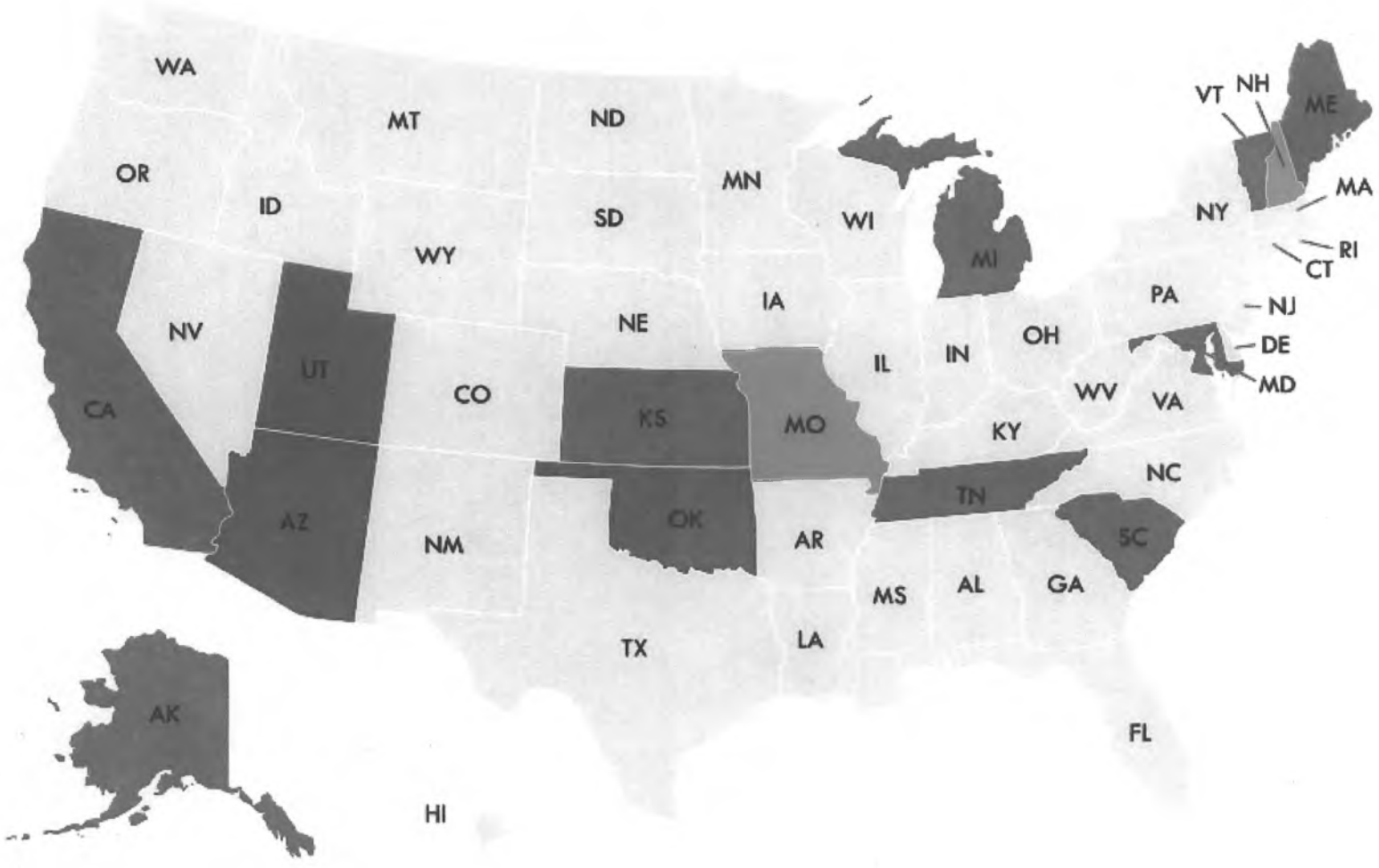
Initially, telecommunications companies such as Verizon, were the targets of legal action against Patriot Act provisions. Congress later gave retroactive immunity to those private businesses.

The revelations of the NSA program and the inner workings of the FISC court came after Snowden leaked documents to the Guardian newspaper. Snowden fled to Hong Kong and then Russia to escape U.S. prosecution.

The case is Klayman v. Obama (13-cv-881).

CNN's Tom Cohen contributed to this report.

Ban use of warrantless data in court: 14 States-Alaska, California, Arizona, Utah, Kansas, Oklahoma, Missouri, Tennessee, Michigan, South Carolina, Maryland, Vermont, New Hampshire, Maine

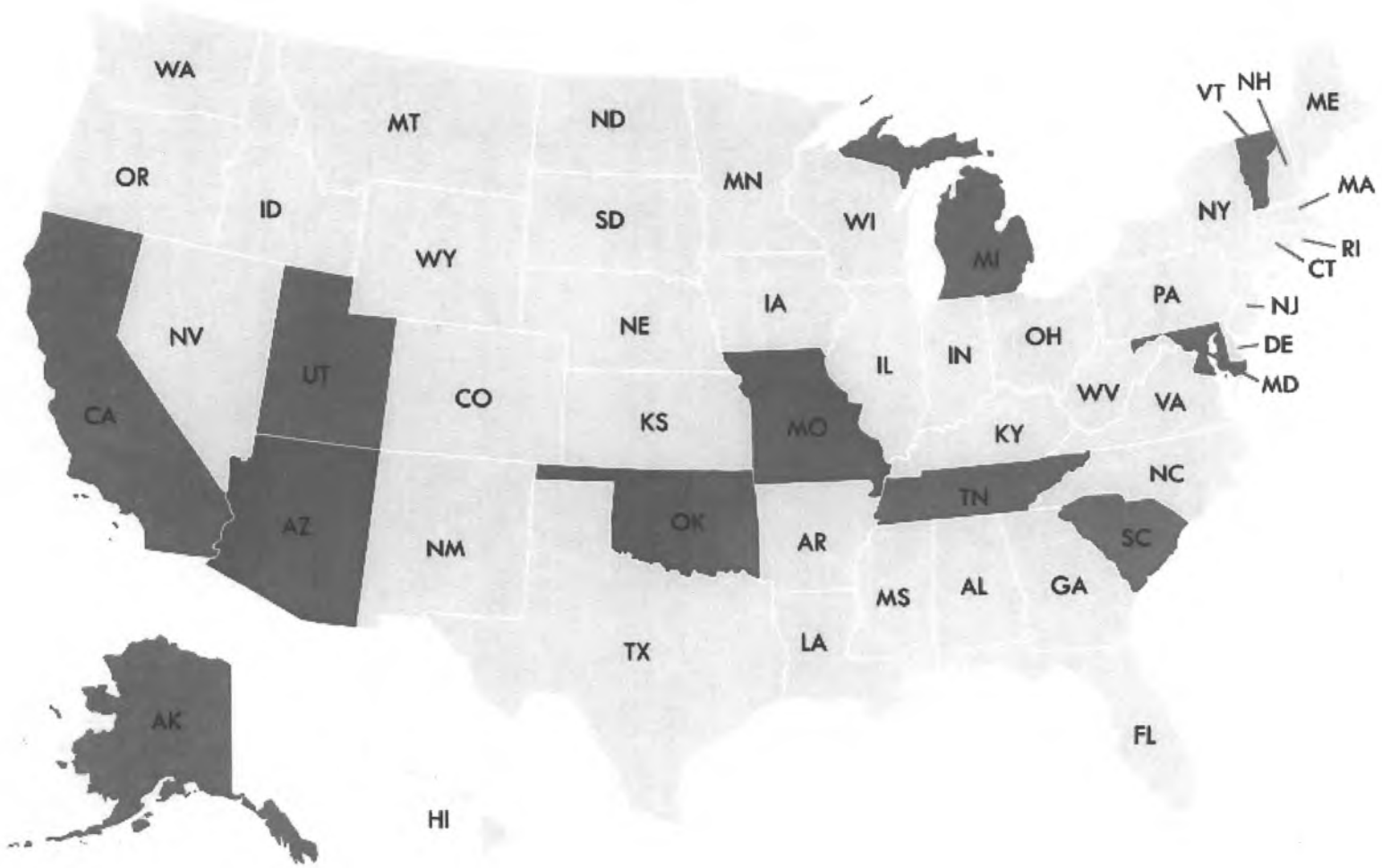


Color Code:

Teal = legislation on House/Senate floor
Blue = legislation in committee
Red = enacted into law
Orange = multiple bills passed

From offnow.org website

Ban material support and resources for federal facilities: 11 states-California, Alaska, Utah, Arizona, Oklahoma, Missouri, Michigan, Tennessee, South Carolina, Maryland, Vermont

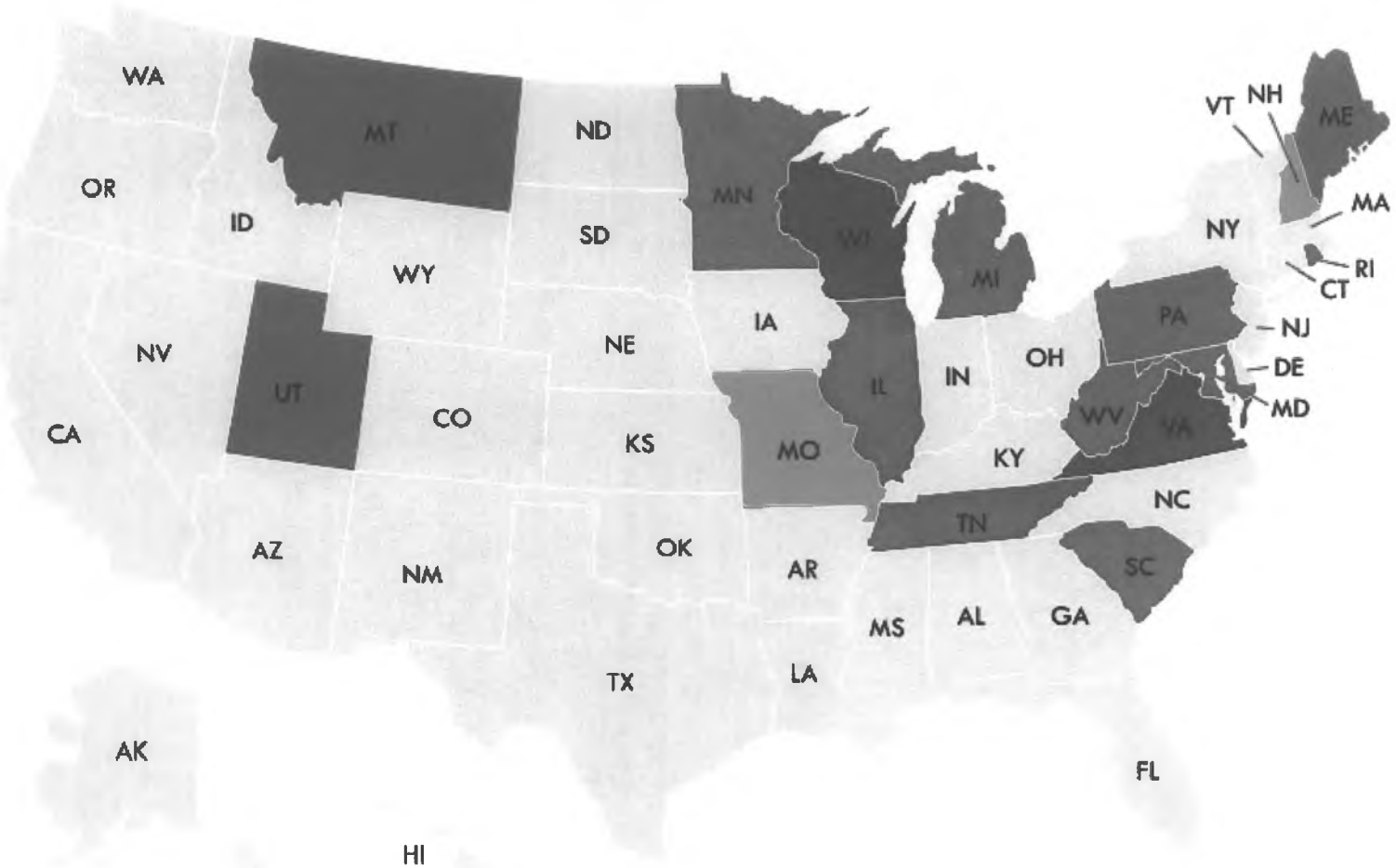


Color Code:

Teal = legislation on House/Senate floor
Blue = legislation in committee
Red = enacted into law
Orange = multiple bills passed

From offnow.org website

Ban obtaining cell phone tracking/location info without a warrant: 16 states-Montana, Utah, Minnesota, Wisconsin, Missouri, Illinois, Michigan, Tennessee, West Virginia, Virginia, South Carolina, Pennsylvania, Maryland, Rhode Island, New Hampshire, Maine



From offnow.org website

Color Code:

Teal = legislation on House/Senate floor
Blue = legislation in committee
Red = enacted into law
Orange = multiple bills passed