SJR

22

<TARGET><BILL>SJR 22</BILL><SUBJECT>SJR 22</SUBJECT><COMM>SJUD28</COMM></TARGET>

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

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 Division: Senate Judiciary Committee
Phone: 465-3719
Date/Time: 3/7/14 12:00 AM

Approved by Division: Senator Coghill, Chair
Date: 3/17/2014

(Revised 8/16/2013 OMB)

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."

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.

adn.com 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.