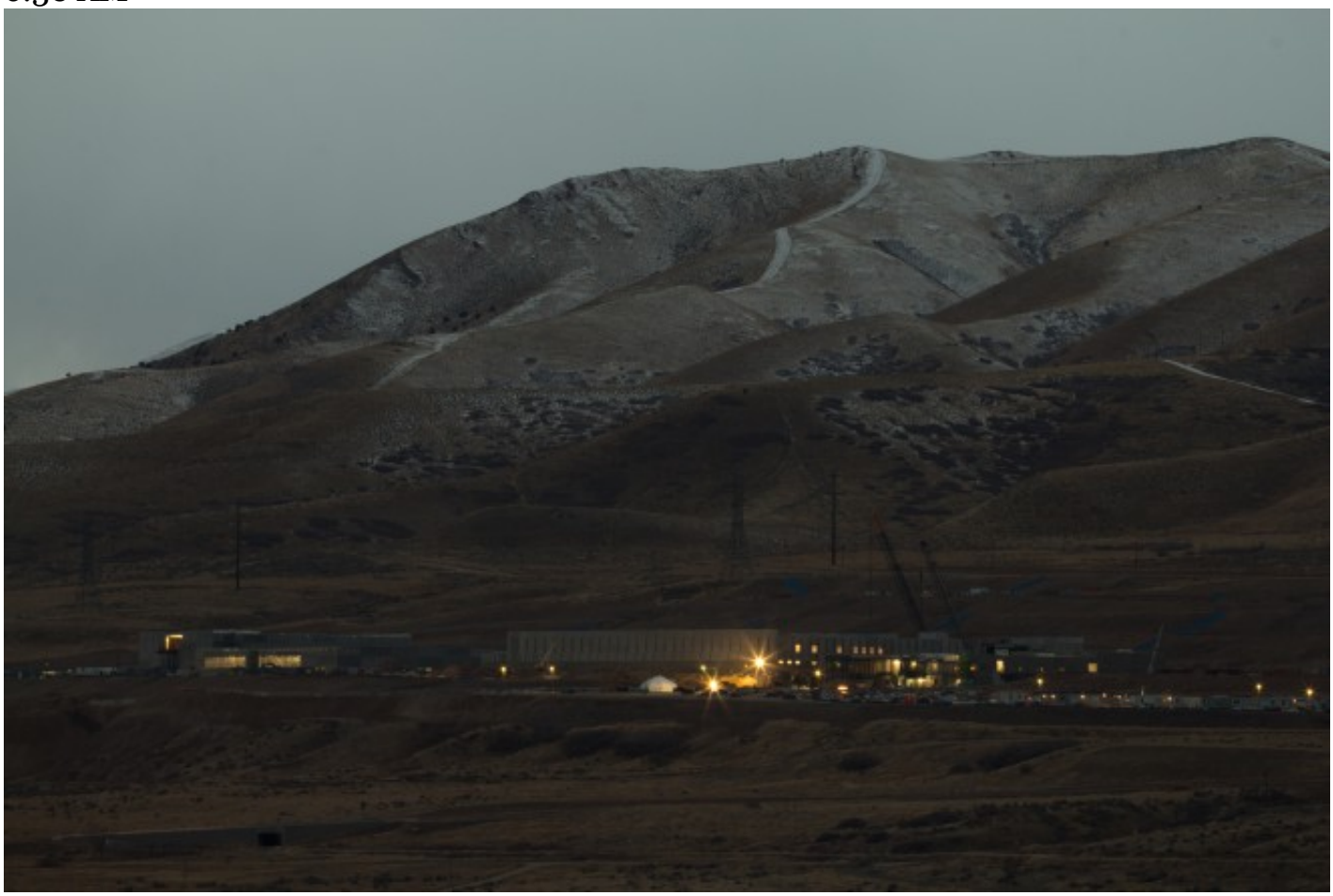
Threat Level
Privacy, Crime and Security Online
NSA

Shady Companies With Ties to Israel Wiretap the U.S. for the NSA

By James Bamford
04.03.12
6:30 AM



The NSA's new super-secret 1-million-square-foot data center in Utah. *Photo: Name Withheld*

Army General Keith Alexander, the director of the NSA, is having a busy year — hopping around the country, cutting ribbons at secret bases and bringing to life the agency's greatly expanded eavesdropping network.

In January he dedicated the new $358 million CAPT Joseph J. Rochefort Building at NSA Hawaii, and in March he unveiled the 604,000-square-foot John Whitelaw Building at NSA Georgia. Designed to house about 4,000 earphone-clad intercept operators, analysts and other specialists,

many of them employed by private contractors, it will have a 2,800-square-foot fitness center open 24/7, 47 conference rooms and VTCs, and "22 caves," according to an NSA brochure from the event. No television news cameras were allowed within two miles of the ceremony.

Overseas, Menwith Hill, the NSA's giant satellite listening post in Yorkshire, England that sports 33 giant dome-covered eavesdropping dishes, is also undergoing a multi-million-dollar expansion, with $68 million alone being spent on a generator plant to provide power for new supercomputers. And the number of people employed on the base, many of them employees of Lockheed Martin and Northrop Grumman, is due to increase from 1,800 to 2,500 in 2015, according to a study done in Britain. Closer to home, in May, Fort Meade will close its 27-hole golf course to make room for a massive $2 billion, 1.8-million-square-foot expansion of the NSA's headquarters, including a cybercommand complex and a new supercomputer center expected to cost nearly $1 billion.

More NSA Coverage by James Bamford

The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)

NSA Chief Denies Domestic Spying But Whistleblowers Say Otherwise

The climax, however, will be the opening next year of the NSA's mammoth 1-million-square-foot, $2 billion Utah Data Center. The centerpiece in the agency's decade-long building boom, it will be the "cloud" where the trillions of millions of intercepted phone calls, e-mails, and data trails will reside, to be scrutinized by distant analysts over highly encrypted fiber-optic links.

Despite the post-9/11 warrantless wiretapping of Americans, the NSA says that citizens should trust it not to abuse its growing power and that it takes the Constitution and the nation's privacy laws seriously.

But one of the agency's biggest secrets is just how careless it is with that ocean of very private and very personal communications, much of it to and from Americans. Increasingly, obscure and questionable contractors — not government employees — install the taps, run the agency's eavesdropping infrastructure, and do the listening and analysis.

And with some of the key companies building the U.S.'s surveillance infrastructure for the digital age employing unstable employees, crooked executives, and having troubling ties to foreign intelligence

services, it's not clear that Americans should trust the secretive agency, even if its current agency chief claims he doesn't approve of extrajudicial spying on Americans. His predecessor, General Michael V. Hayden, made similar claims while secretly conducting the warrantless wiretapping program.

Until now, the actual mechanics of how the agency constructed its highly secret U.S. eavesdropping net, code-named Stellar Wind, has never been revealed. But in the weeks following 9/11, as the agency and the White House agreed to secretly ignore U.S. privacy laws and bypass the Foreign Intelligence Surveillance Court, J. Kirk Wiebe noticed something odd. A senior analyst, he was serving as chief of staff for the agency's Signals Intelligence Automation Research Center (SARC), a sort of skunkworks within the agency where bureaucratic rules were broken, red tape was cut, and innovation was expected.

"One day I notice out in the hallway, stacks and stacks of new servers in boxes just lined up," he said. Passing by the piles of new Dell 1750 servers, Wiebe, as he often did, headed for the Situation Room, which dealt with threat warnings. It was located within the SARC's Lab, on the third floor of Operations Building 2B, a few floors directly below the director's office. "I walk in and I almost get thrown out by a guy that we knew named Ben Gunn," he said. It was the launch of Stellar Wind and only a handful of agency officials were let in on the secret.

"He was the one who organized it," said Bill Binney of Gunn. A former founder and co-director of SARC, Binney was the agency official responsible for automating much of the NSA's worldwide monitoring networks. Troubled by the unconstitutional nature of tapping into the vast domestic communications system without a warrant, he decided to quit the agency in late 2001 after nearly forty years.

Gunn, said Binney, was a Scotsman and naturalized U.S. citizen who had formerly worked for GCHQ, Britain's equivalent of the NSA, and later become a senior analyst at the NSA. The NSA declined Wired's request to interview Gunn, saying that, as policy, it doesn't confirm or deny if a person is employed by the agency.

Shortly after the secret meeting, the racks of Dell servers were moved to a room down the hall, behind a door with a red seal indicating only those specially cleared for the highly compartmented project could enter. But rather than having NSA employees putting the hardware and software together and setting up walls of monitors showing suspected terrorism threats and their U.S. communications, the spying room was filled with a half-dozen employees of a tiny mom-and-pop company with a bizarre and troubling history.

"It was Technology Development Corporation," said Binney.

The agency went to TDC, he says, because the company had helped him set up a similar network in SARC — albeit one that was focused on foreign and international communications — the kind of spying the NSA is chartered to undertake.

"They needed to have somebody who knew how the code works to set it up," he said. "And then it was just a matter of feeding in the attributes [U.S. phone numbers, e-mail addresses and personal data] and any of the content you want." Those "attributes" came from secret rooms established in large telecom switches around the country. "I think there's 10 to 20 of them," Binney says.

Formed in April 1984, TDC was owned by two brothers, Randall and Paul Jacobson, and largely run out of Randall's Clarkesville, Maryland house, with his wife acting as bookkeeper. But its listed address is a post office box in Annapolis Junction, across the Baltimore-Washington Parkway from the NSA, and the company's phone number in various business directories is actually an NSA number in Binney's old office.

The company's troubles began in June 1992 when Paul lost his security clearance. "If you ever met this guy, you would know he's a really strange guy," Binney said of Paul. "He did crazy stuff. I think they thought he was unstable." At the time, Paul was working on a contract at the NSA alongside a rival contractor, Unisys Corporation. He later blamed Unisys for his security problems and sued it, claiming that Unisys employees complained about him to his NSA supervisors. According to the suit, Unisys employees referred to him as "weird" and that he "acted like a robot," "never wore decent clothes," and was mentally and emotionally unstable. About that time, he also began changing his name, first to Jimmy Carter, and later to Alfred Olympus von Ronsdorf.

With "von Ronsdorf's" clearance gone and no longer able to work at the NSA, Randy Jacobson ran the company alone, though he kept his brother and fellow shareholder employed in the company, which led to additional problems.

"What happened was Randy still let him have access to the funds of the company and he squandered them," according to Binney. "It was so bad, Randy couldn't pay the people who were working for him." According to court records, Ronsdorf allegedly withdrew about $100,000 in unauthorized payments. But Jacobson had troubles of his own, having failed to file any income tax statements for three years in the 1990s, according to tax court records. Then in March 2002, around the time the company was completing Stellar Wind, Jacobson fired his brother for improper billing and conversion of company funds. That led to years of suits and countersuits over mismanagement and company ownership.

Despite that drama, Jacobson and his people appeared to have serious misgivings about the NSA's program once they discovered its true nature, according to Binney. "They came and said, 'Do you realize what these people are doing?'" he said. "'They're feeding us other stuff [U.S.] in there.' I mean they knew it was unconstitutional right away." Binney added that once the job was finished, the NSA turned to still another contractor to run the tapping operation. "They made it pretty well known, so after they got it up and running they [the NSA] brought in the SAIC people to run it after that."

Jacobsen was then shifted to other work at the NSA, where he and his company are still employed. Randall Jacobsen answered his phone inside the NSA but asked for time to respond. He never called back.

In addition to constructing the Stellar Wind center, and then running the operation, secretive contractors with questionable histories and little oversight were also used to do the actual bugging of the entire U.S. telecommunications network.

According to a former Verizon employee briefed on the program, Verint, owned by Comverse Technology, taps the communication lines at Verizon, which I first reported in my book *The Shadow Factory* in 2008. Verint did not return a call seeking comment, while Verizon said it does not comment on such matters.

At AT&T the wiretapping rooms are powered by software and hardware from Narus, now owned by Boeing, a discovery made by AT&T whistleblower Mark Klein in 2004. Narus did not return a call seeking comment.

What is especially troubling is that both companies have had extensive ties to Israel, as well as links to that country's intelligence service, a country with a long and aggressive history of spying on the U.S.

In fact, according to Binney, the advanced analytical and data mining software the NSA had developed for both its worldwide and international eavesdropping operations was secretly passed to Israel by a mid-level employee, apparently with close connections to the country. The employee, a technical director in the Operations Directorate, "who was a very strong supporter of Israel," said

Binney, "gave, unbeknownst to us, he gave the software that we had, doing these fast rates, to the Israelis."

Because of his position, it was something Binney should have been alerted to, but wasn't.

"In addition to being the technical director," he said, "I was the chair of the TAP, it's the Technical Advisory Panel, the foreign relations council. We're supposed to know what all these foreign countries, technically what they're doing.... They didn't do this that way, it was under the table."

After discovering the secret transfer of the technology, Binney argued that the agency simply pass it to them officially, and in that way get something in return, such as access to communications terminals. "So we gave it to them for switches," he said. "For access."

But Binney now suspects that Israeli intelligence in turn passed the technology on to Israeli companies who operate in countries around the world, including the U.S. In return, the companies could act as extensions of Israeli intelligence and pass critical military, economic and diplomatic information back to them. "And then five years later, four or five years later, you see a Narus device," he said. "I think there's a connection there, we don't know for sure."

Narus was formed in Israel in November 1997 by six Israelis with much of its money coming from Walden Israel, an Israeli venture capital company. Its founder and former chairman, Ori Cohen, once told Israel's *Fortune Magazine* that his partners have done technology work for Israeli intelligence. And among the five founders was Stanislav Khirman, a husky, bearded Russian who had previously worked for Elta Systems, Inc. A division of Israel Aerospace Industries, Ltd., Elta specializes in developing advanced eavesdropping systems for Israeli defense and intelligence organizations. At Narus, Khirman became the chief technology officer.

A few years ago, Narus boasted that it is "known for its ability to capture and collect data from the largest networks around the world." The company says its equipment is capable of "providing unparalleled monitoring and intercept capabilities to service providers and government organizations around the world" and that "Anything that comes through [an Internet protocol network], we can record. We can reconstruct all of their e-mails, along with attachments, see what Web pages they clicked on, we can reconstruct their [Voice over Internet Protocol] calls."

Like Narus, Verint was founded by in Israel by Israelis, including Jacob "Kobi" Alexander, a former Israeli intelligence officer. Some 800 employees work for Verint, including 350 who are based in Israel, primarily working in research and development and operations, according to the *Jerusalem Post*. Among its products is STAR-GATE, which according to the company's sales literature, lets "service providers ... access communications on virtually any type of network, retain communication data for as long as required, and query and deliver content and data ..." and was "[d]esigned to manage vast numbers of targets, concurrent sessions, call data records, and communications."

In a rare and candid admission to *Forbes*, Retired Brig. Gen. Hanan Gefen, a former commander of the highly secret Unit 8200, Israel's NSA, noted his former organization's influence on Comverse, which owns Verint, as well as other Israeli companies that dominate the U.S. eavesdropping and surveillance market. "Take NICE, Comverse and Check Point for example, three of the largest high-tech companies, which were all directly influenced by 8200 technology," said Gefen. "Check Point was founded by Unit alumni. Comverse's main product, the Logger, is based on the Unit's technology."

According to a former chief of Unit 8200, both the veterans of the group and much of the high-tech intelligence equipment they developed are now employed in high-tech firms around the world. "Cautious estimates indicate that in the past few years," he told a reporter for the Israeli newspaper *Ha'artez* in 2000, "Unit 8200 veterans have set up some 30 to 40 high-tech companies, including 5

to 10 that were floated on Wall Street." Referred to only as "Brigadier General B," he added, "This correlation between serving in the intelligence Unit 8200 and starting successful high-tech companies is not coincidental: Many of the technologies in use around the world and developed in Israel were originally military technologies and were developed and improved by Unit veterans."

Equally troubling is the issue of corruption. Kobi Alexander, the founder and former chairman of Verint, is now a fugitive, wanted by the FBI on nearly three dozen charges of fraud, theft, lying, bribery, money laundering and other crimes. And two of his top associates at Comverse, Chief Financial Officer David Kreinberg and former General Counsel William F. Sorin, were also indicted in the scheme and later pleaded guilty, with both serving time in prison and paying millions of dollars in fines and penalties.

When asked about these contractors, the NSA declined to "verify the allegations made."

But the NSA did "eagerly offer" that it "ensures deliberate and appropriate measures are taken to thoroughly investigate and resolve any legitimate complaints or allegations of misconduct or illegal activity" and "takes seriously its obligation to adhere to the U.S. Constitution and comply with the U.S. laws and regulations that govern our activities."

The NSA also added that "we are proud of the work we do to protect the nation, and allegations implying that there is inappropriate monitoring of American communications are a disservice to the American public and to the NSA civilian and military personnel who are dedicated to serving their country."

However, that statement elides the voluminous reporting by the *New York Times*, *Washington Post*, *USA Today*, *Los Angeles Times* and Wired on the NSA's warrantless wiretapping program. Also not reflected is that in the only anti-warrantless wiretapping lawsuit to survive the government's use of the "state secrets" privilege to throw them out, a federal judge ruled that two American lawyers had been spied on illegally by the government and were entitled to compensation.

So take the NSA's assurances as you will.

But as NSA director Alexander flies around the country, scissors in hand, opening one top-secret, outsourced eavesdropping center after another, someone might want to ask the question no one in Congress seems willing to ask: Who's listening to the listeners?

Pages: 1 2 View All

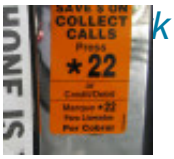
Related
You Might Like
Story Resources
Related Links by Contextly

nate Net Monitoring Tool

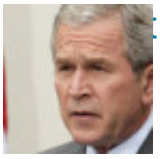
peal Warrantless-Wiretapping Defeat

bie's Guide to Detecting the NSA

Blower Outs NSA Spy Room



k Times' NSA Whistleblower Reveals Himself



, Senate Panel May Re-Up Vast Surveillance Dragnet

ns Spy Bill, ACLU Sues

Is Building the Country's Biggest Spy Center (Watch What You Say)

CIA Chief Says Obama's War on Terror Same As Bush's, But With More Killing

ys Bush Illegally Wiretapped Two Americans

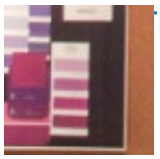
Stands Behind 'State Secrets' in Spy Case

no Author to America: No Apologies for Tapping You

py Court To Consider ACLU Request For Bush Spying Orders

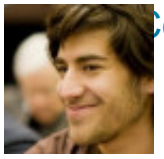
AT&T Whistleblower: How I Learned of Internet Spy Room

Show More



his Translucent Ruler Animates Math Homework

hities and Singed Teddy Bears: Breaking Bad Props Get a Museum Exhibit



onquer NYC, In 9 Clever Drawings Done with Reddit's Guidance

Pages of Aaron Swartz's Secret Service File Released

ss Release - NSA Launches New Crypto Mobile Game Appr

nwith Hill - Wikipedia, the free encyclopedia

tates Foreign Intelligence Surveillance Court - Wikipedia, the free encyclopedia

Show More

James Bamford is the author of the **The Shadow Factory: the Ultra-Secret NSA from 9/11 to the Eavesdropping on America**.

Read more by James Bamford

Post Comment | 247 Comments | Permalink

Back to top

Comments for this thread are now closed.

247 comments

10

Best Community Share

Guest • a year ago

The NSA also added that “we are proud of the work we do to protect the nation, and allegations implying that there is inappropriate monitoring of American communications are a disservice to the American public and to the NSA civilian and military personnel who are dedicated to serving their country.”

Clever jab, couched in careful wording by some PR flunky, by the NSA that if you don't place 100% trust in them to do the right thing, you are un-American.

69 Share ›

TopsyKrets → Guest • a year ago

Dissent is patriotic.
True Americans understand that.

61 Share ›

AcneVulgaris → TopsyKrets • a year ago

True Americans are to frightened of their own terroristy shadows to even contemplate dissent.

23 2 Share ›

Fortis Imago → AcneVulgaris • a year ago

"Terroristy" Is Baskin Robbin's 65th flavor....Mmm

12 Share ›

Soylent Green Is People → Fortis Imago • a year ago

The flavour explodes on your tongue.

5 Share ›

Bill Hansel ➔ AcneVulgaris • a year ago

Ir a tener sexo con usted

1 ^ | 4 v Share ›

Bill Hansel ➔ TopsyKrets • a year ago

True Americans have nothing to hide, take your tent to Mexico,

2 ^ | 10 v Share ›

Ross Faircloth ➔ Bill Hansel • a year ago

Has there ever been a more blatantly irrelevant and false statement then "True Americans have nothing to hide". We have, *Cough* had, freedom of speech and many other freedoms [I believe it was called the Bill of Rights] that protected US the citizen from our own governments control. This is the real danger to any civilization or society that our True PATRIOT founders realized. This new, propaganda driven "patriotism for the sake of safety" is complete bullsh!t, our founding fathers never would have stood for this complete disregard for its citizens rights. It's a slap in the face of anyone with real intelligence of their own and a beginning of the end for our once great country.

70 ^ | v Share ›

Archil ➔ Ross Faircloth • a year ago

Thanks Ross to remember "Bill of Rights" - it's rarely mentioned last decade or so on!

21 ^ | v Share ›

cus_bus ➔ Bill Hansel • a year ago

Really? Let's post all your text messages, phone conversations, internet search history, and every place you've been in the last year in public, so every single person you know can see.

Just because I have things I prefer certain people don't know, doesn't mean I am breaking the law.

Novel idea, rather than us moving to Mexico, how about you move yourself to China. I hear their government takes the exact same approach as you with respect to "freedom."

31 ^ | v Share ›

Advocate4Liberty ➔ Bill Hansel • a year ago

True Americans? It was one of our founders, Thomas Paine who said "It is

the duty of every patriot to protect his country from its government." Brownshirts don't qualify as patriots. Bill.

18 Share ›

Soylent Green Is People → Bill Hansel • a year ago

How do you even have time to post anything online? I mean, shouldn't you be mucking the shit of the stalls or something, Farmer Brown?

8 Share ›

das → Guest • a year ago

You don't have to place 100% trust in them.

But if you place 0% trust in them, and believe that they are doing the wrong thing 100% of the time, that's equally ignorant (and false).

10 1 Share ›

Dave → das • a year ago

And how are we supposed to be able to tell where their lies, their obfuscations, their illegal activity ends and their proper mission begins? They have corrupted themselves and are no longer a constitutional or American organization. While I agree that there is legitimate intelligence work that needs to be conducted, they are no longer operating in a way which makes them accountable for their actions. There is no way to fix this except to start over. The insane bloat of the NSA, DHS, FBI, CIA, DEA, ATF, etc. etc. is another reason why the situation is so ridiculous. We just keep adding more and more layers.

It doesn't matter, though. The American people are too ignorant to ever fix the situation. The government will become totalitarian, and then will fall. It's inevitable.

45 Share ›

bukkakeninja → Dave • a year ago

On a positive note: 40% of every dollar this nation spends is borrowed. The United States will be bankrupt and collapse under the weight of our own bureaucracy before any of your fears find traction.

15 Share ›

Atom Davis → bukkakeninja • a year ago

well they could just keep it up till they collapse like the stasi did, and then we'll be like eastern europe was! yay!

..fuck i hate that thought, but not because it isnt true or our government wont have deserved it. its because of how badly it will fuck up the citizens here who didnt know any better.

12 Share ›

maddcribbage ➚ Dave • a year ago

Consider that at one point our nation split in half and promptly went to war with itself. Consider that our nation was founded by a comparably ragtag group battling against the greatest empire in the world.

Past Americans would probably laugh to the point of tears if modern day Americans such as yourself tried to explain how "bad" our situation has gotten, and how there is "no hope".

Sadly, people like you are the one's who don't care. Who claim to have all the answers, and seem to fully understand our "situation", and yet do nothing except complain and complain.

3 | 2 Share ›

cus_bus ➚ maddcribbage • a year ago

Nice logic. If I understand, you're saying that unless your situation can't possibly get worse, then you don't have a right to complain? Taken to the logical conclusion, only dead people can claim that right.

12 Share ›

maddcribbage ➚ cus_bus • a year ago

"If I understand..." No offense but you didn't understand. I was pointing out that he forsees the "fall" of our government, when our nation has been through far worse before.

Glad I could clear that up for you.

1 | 1 Share ›

Bill Hansel ➚ Dave • a year ago

I look forward to this day, Go Obama!

| 2 Share ›

Sothis ➚ das • a year ago

What percent of the Fourth Amendment don't you understand?

29 Share ›

das ↗ Sothis • a year ago

I don't have any issues with the Fourth Amendment, or the fact that collecting the communications of US Persons requires a warrant, or that there is a body of law that supports foreign intelligence work. Do you?

Or are you saying if there is ever any wrongdoing, any perception/assumption of wrongdoing, or even something that's not illegal but with which you disagree, then we should throw the baby out with the bathwater?

2 ^ | 2 v Share ›

nick rambo ↗ das • a year ago

if the constitution is willfully violated by "domestic enemies" then not only should the baby be thrown out with the bathwater, the baby needs to be tried for treason.

willfully violating the fourth amendment, regardless of the justification, is treason. ive had this very argument with a family member; he swore an oath to 'uphold the constitution against enemies both foreign and domestic' but somewhere along the lines he got slipped some gov. issued kool-aid.

27 ^ | v Share ›

Not ↗ nick rambo • a year ago

@das

Das, obviously we cannot have the full range of evidence in front of us to objectively analyze as that would never happen because of national security.

What we do have is information from whistleblowers, and from insiders, who essentially have risked a lot to let us know something isn't right.

Your statement is predicated on a position of inherent trust in government.

Personally, I believe we must start from the position of inherent distrust.

We don't have access to the facts, but that doesn't mean we don't have inklings of what is going on.

In this particular case, we now know that the NSA is building a massive data capture and analyzation facility, and they have a long track record of violating existing law, so I think the healthy assumption to make is that they will once again violate the law

will once again violate the law.

Again, we don't really have any way of knowing what exactly the NSA is doing because it operates in the dense haze of national security, but based on past abuses I think it's fairly safe to say they will abuse whatever power they are given.

It should also be said that just because something might be law, doesn't mean it's right or just.

18 Share ›

Guest ➚ nick rambo • a year ago

@ das,

I think the problem a lot of people have is that a misunderstanding exists because they do not and cannot ever have direct or indirect knowledge of what is actually occurring. It's the national security letters that cannot be questioned, it's the GPS surveillance, it's NDAA. And it's not merely affronts to our privacy--it's scandals like gunwalking and general screw-ups by federal authorities that nobody ever seems to be able to clearly and concisely explain or provide accountability for. The relationship between we the people and they the authorities is predicated upon a great deal of trust that we are asked to place in them that no wrongdoing will be done. And that trust has worn quite thin.

18 Share ›

Guest ➚ nick rambo • a year ago

Is this in the same vein as "yelling fire in a crowded theater is allowed by the First Amendment"? ie, the belief that all rights are absolute?

2 1 Share ›

das ➚ nick rambo • a year ago

I don't think you're going to get any disagreement from anyone who cares about the law and the Constitution. But I'll note this: many of the things that some people declare as "unconstitutional" are either 1. actually not "unconstitutional", and sometimes are even explicitly lawful, or 2. are things they think are unconstitutional, based on a gross misunderstanding of the facts or personal assumptions about what must be happening, with no direct knowledge of what is actually occurring.

2 1 Share ›

Bill Hansel ➚ nick rambo • a year ago

If the reason saves my family then I am OK with it, you on the other hand should be destroyed.

3 Share ›

Guest → das • a year ago

That "baby" is not a baby anymore. It has grown into a huge bloated middle aged guy with kids of his own, all sitting in the same dirty bathwater. So yeah, time to throw out the "baby" with the bathwater and start over...

11 Share ›

beam57 → das • a year ago

DAS, all this relentless reasoning doesn't change the fact that there is a system in place for wholesale spying on everyone. If, when, or how is not the point. We have witnessed the government pass dictatorship NDAA laws, enslave the economy to private hands of Federal Reserve and others, engage in horrible programs such as MKULTRA and the list goes on and on. So in the big picture, this is just another piece. Another brick in the wall.

10 Share ›

Not → das • a year ago

The problem is that they have shown repeatedly an absolute disdain for the rights of American Citizens.

They don't respect the constitution. How can they say they respect the constitution when they are drag-net capturing all telecommunications without a warrant? It's a complete joke, and I think they know it behind the PR smokescreen.

The mere existence of the data center in Utah is a direct threat to the very core of American Freedom.

They say they will encrypt the data and only decrypt with a warrant.

For an agency that has shown repeated disregard for privacy, and little respect for the law, I think we must fairly assume that they mean the data will be readily available for dissemination to any interested parties.

The whole scheme is ripe for abuse. What's to stop a president from deeming a political enemy a threat, and requesting all data from the NSA on that person?

The database could be used as a massive blackmail system to consolidate

executive power.

I think the most healthy point of view is to treat everything the NSA says as a lie, and work from there. On the rare occasion they are telling the truth, backed by irrefutable evidence, it should be met with surprise.

Deception is their baseline, truth is the exception.

23 Share ›

Bill Hansel ➚ Not • a year ago

How many of your citizens pay taxes?

1 Share ›

Brandon Spencer ➚ Bill Hansel • a year ago

Bill. Every person who experiences the unique pleasure of reading one of your comments understands several things about you:
1. Your responses are either sarcastic or obvious political propaganda you heard somewhere.
2. You are living in a state of being wrong at every conceivable scale of resolution. That
is, from a distance, your worldview is incorrect;
and furthermore, if you zoom in on any small part of your
worldview, that part is just as wrong as the whole worldview. This is known a fractal wrongness.
3. Nothing at all can be done about who and what you are.

26 Share ›

henry balfour ➚ Brandon Spencer • a year ago

Mate ... could NOT have said it better myself. Bill is close to my ideal Useful Dupe. How many more of this cretin do you have over in the USA ?

13 Share ›

Anonymous Person ➚ Bill Hansel • a year ago

100% of the citizenry pay taxes of some sort, Medicare Medicaid SS income and/or sales tax.

6 Share ›

Not ➚ Bill Hansel • a year ago

I don't understand what tax payments have to do with blatant 4th amendment violations, care to clarify?

6 Share ›

No Way ↗ das • a year ago

if you believe in the constitution and the principals of freedom.. in a world that hasn't changed in thousands of years... believe it or not..... then this is 100 percent wrong...

just because you let your master encroach on your freedom for the reasons you think are valid doesn't make it right.. it is still 100 percent illegal. and 100 percent forwarned by the founders... but the govt wants you to think that there are bigger evils out now than ever.. murderers have been around forever.. armies have fought forever.. and if you think that spying on us citizens will prevent a wmd attack you are a trained puppy on a leash..

14 ^ | v Share ›

No Way ↗ das • a year ago

you know nothing about the nature of power and mankind... das. If you think power is intersted in protecting anything but it's own power you are a shakespearian fool .

9 ^ | v Share ›

Hlaode • a year ago

I'd vote for any politician who would get rid of the NSA and isn't Ron Paul.

19 ^ | v Share ›

das ↗ Hlaode • a year ago

So what you're saying is, you don't think the US needs a foreign signals intelligence capability, or the ability to intercept foreign communications when they're traveling on US systems and networks, or an organization whose job it is to make secure cryptographic systems while breaking those of our adversaries? I'm interested in hearing what alternatives you might have for this capability.

You do realize that the current law explicitly says that a warrant is required to collect the *content* of the communications of US Persons anywhere on the globe (which is more strict than previous law), and that any previous "warrantless wiretapping" was done on very specific individuals for specific reasons under a specific Presidential order under the guise of Article II authority, briefed to Congress, and is no longer in existence?

I bring up the latter because people will invariably say, "But NSA has already proven it breaks the law and spies on Americans!" No, no it hasn't. NSA does the things it is directed to do by policy makers. It doesn't make up things as it goes along. The law and oversight are the same controls we have had on the Intelligence Community since its

inception. The IC exists to serve as an instrument of national policy, not for its own sake.

One of the assertions in Bamford's series of articles is that tapping US networks without

see more

11 2 Share ›

Pulse1 ➚ das • a year ago

"

So what you're saying is, you don't think the US needs a foreign signals intelligence capability, or the ability to intercept foreign communications when they're traveling on US systems and networks, or an organization whose job it is to make secure cryptographic systems while breaking those of our adversaries? I'm interested in hearing what alternatives you might have for this capability."

Not if they can't do it without, pretty obviously, violating the rights of US citizens, no.

Make all the caveats you want, set up all the scenarios you want, you're still making excuses for exchanging liberties (in this case the right to private communication) for a false sense of security.

"I asked this question on both prior NSA stories: is ANYONE interested in having a serious discussion about how the US should do foreign signals intelligence collection — which does NOT require a warrant — within the US?"

see more

38 Share ›

das ➚ Pulse1 • a year ago

No, the discussion can be had. To say that the FBI is the only entity that can do intelligence work in the US is false. Sure, the FBI can and does have a role. But there is also foreign intelligence work that can be done within the US, and foreign intelligence agencies like NSA and CIA have done this under various legal frameworks for decades. Just because there has been abuse (or perceived abuse) doesn't mean abuse is all that exists.

I'm perfectly willing to entertain how NSA might do foreign intelligence work on US networks. Why shouldn't that capability be colocated with US telecom operators? When foreign traffic traverses US networks, that should be the *easiest* scenario. If it's done secretly in its own facilities by, say, tapping US-owned or -leased fiber optic cable at the US border, how is

tapping US-owned or -leased fiber optic cable at the US border, how is that substantially different, given that they'd have access to the same traffic?

The FBI does not do foreign SIGINT. That is not their job. That is NSA's job, and there is traffic that belongs exclusively to non-US Persons traveling on US networks. The fact that no one actually knows if/where any "secret

see more

5 | 1 Share ›

Pulse1 ➔ das • a year ago

(This is where the conversation get's disjointed thanks to the reply limit)

"I think you're sort of missing my point. I'm not carefully choosing words so you can "catch" me parsing words somehow. What I said was that, "the argument that any capability interior to the nation must therefore only be used to spy on Americans is false." Nothing less, nothing more. People are jumping to the conclusion that the only reason a hypothetical "secret room" could exist anywhere but a border must obviously be because it's purpose is to spy on Americans. However, this is an erroneous conclusion."

I wasn't trying to "catch" you. I was pointing out the difference of opinion. You feel it's okay for the NSA to have this power, I do not.

And I never said that it would only be used for spying on Americans, I said that, if it could be used for that then the power should be stripped away from them.

We shouldn't have to wait for an abuse to happen before removing abusive powers ESPECIALLY from people who have proven they will lie to get what

see more

15 | Share ›

Pulse1 ➔ das • a year ago

"

No, the discussion can be had. To say that the FBI is the only entity that can do intelligence work in the US is false. Sure, the FBI can and does have a role. But there is also foreign intelligence work that can be done within the US, and foreign intelligence agencies like NSA and CIA have done this under various legal frameworks for decades. Just because there has been abuse (or perceived abuse) doesn't mean abuse is all that exists."

It doesn't matter if "abuse is all that exists", if they're abusing their power then that power should be removed. Period.

Until such time that they can be trusted to use the power 100% of the time, they don't get to have it, at all, not even a little bit.

The entire rest of your post is a running reason for why the NSA (and to a lessor extent, the CIA) should be allowed to spy internally and we're never, ever, going to agree on that. Their power was supposed to, and should, end at the border.

---

see more

8 ^ | 1 v Share ›

das ➚ Pulse1 • a year ago

I think you're sort of missing my point. I'm not carefully choosing words so you can "catch" me parsing words somehow. What I said was that, "the argument that any capability interior to the nation must therefore only be used to spy on Americans is false." Nothing less, nothing more. People are jumping to the conclusion that the only reason a hypothetical "secret room" could exist anywhere but a border must obviously be because it's purpose is to spy on Americans. However, this is an erroneous conclusion.

Note, too, that the communications of US Persons CAN in fact be lawfully intercepted — with a properly adjudicated warrant. That doesn't change the fact that the primary mission of the foreign intelligence agencies such as NSA, CIA, and DIA, are just that: foreign intelligence. Sometimes foreign intelligence work involves US Persons (in which case a warrant is required), and yes, the FBI can and does become involved. If it isn't clear, I will say it again now: the content of the communications of US Persons is off limits without a warrant.

3 ^ | 1 v Share ›

das ➚ das • a year ago

@Pulse1 I appreciate your comments on this. As you say, we disagree on some issues. I do want to make it clear that agencies other than the FBI lawfully performing some tasks with respect to US Persons with a warrant is not a new construct. I'm not saying you claimed it was; I'm just stating that for the benefit of others and because many seem to believe these are related to "new" laws after 9/11 when in fact the current law with regard to

US Persons is stricter than it ever was.

I will say that your assertion that NSA is "not supposed to be doing this" is not correct. I understand that you believe they should not be doing it, and that is fine. I would simply point out that different agencies have different areas of expertise, and our focus from a standpoint of protecting the rights of Americans shouldn't be who is doing it, but judicious use of capabilities under the auspices of a clear legal framework. The current FISA law, as amended, is very clear.

2 | 1 Share ›

Pulse1 ➚ das • a year ago

"

I appreciate your comments on this. As you say, we disagree on some issues. I do want to make it clear that agencies other than the FBI lawfully performing some tasks with respect to US Persons with a warrant is not a new construct. I'm not saying you claimed it was; I'm just stating that for the benefit of others and because many seem to believe these are related to "new" laws after 9/11 when in fact the current law with regard to US Persons is stricter than it ever was."

I understand it's been going on for a while (the DEA is a prime example). My concern is with jurisdictional overreach. More specifically with an agency that's proven it will lie to the people who are supposed to be watching over it.

And anytime I see something like this, done in the name of "security", it's unsettling. Removing ones liberties is removing their ability to be secure from that agency.

As for the last part, I've read much of the patriot act (and the follow up bill)

see more

11 | Share ›

das ➚ das • a year ago

@Pulse1 (Disqus threading fail.)

To answer a couple of your questions (and this is not a value judgment on whether it is the right or wrong way to do things):

"[...] if the NSA is supposed to be monitoring all inter-state communication [...] then why would the FBI need the same powers?"

It's not that the NSA is "supposed to" monitor "all" inter-state communication; it's that NSA requires a CAPABILITY to target foreign communications anywhere it might exist, including on the internet, and including within US networks. The FBI does not have the same mission. You're making the distinction with respect to where collection occurs (inside or outside of the US) as opposed to the target (is or isn't a US Person).

"Our focus on protecting rights should always look at who is doing what and how. Always."

see more

3 | 1 Share ›

Michael Thomason ↗ das • a year ago

So, the NSA is able to copy our private communications, run them through sophisticated computer filter, generate meta data on them, analyze that meta data, and then listen to them to see if Siri's big brother flags them as inappropriate? That doesn't sound cool.

The *content* of the communication is exactly what they are collecting, when they reroute and record traffic. This mysterious meta data they speak of must be generated by their machines. What meta data does ATT need for voice calls it doesn't record? None, because they have no reason to save the voice calls; what a complete waste of effort it is to do such a thing. The meta data is generated by big-brother Siri after listening to the call, when it used to be generated by an officer after getting a warrant.

Don't let people like Officer Schroeder fool you into believing this is nothing but large scale collection of everything without warrant.

Do not forget that evidence exist that this information was formerly and likely is currently being used for political purposes. Most importantly, nothing has changed. The same corrupt people are using the same bogus excuses to cover the same corrupt behavior. But, thanks.

22 | Share ›

das ↗ Michael Thomason • a year ago

No. The metadata of communications is what defines a target. An email address. An IP address. A phone number. A DNS name. Some of these things are known or reasonably known to belong to individuals that either

things are known or reasonably known to belong to individuals that either are or are not US Persons. The metadata isn't "generated" by anything after "listening" to the content. The metadata already exists.

Yes, there are some nuances here: what is "collecting"? What is "storing"? Writing something for a fraction of a second to volatile memory while it is analyzed? Passing traffic headers through a database? YOU are making the assumption that traffic is being stored or recorded. There is absolutely no basis for that assertion beyond your own assumptions.

Previous Article

Global Payments Says 1.5 Million Cards Stolen; Won't Discuss Details of Breach

Next Article

On Profiling, And Google's Big Double-Cross