# LYING KEITH ALEXANDER TO SHACK UP WITH PROMONTORY AND PROFIT OFF HIS FEARMONGERING

Man, I knew Keith Alexander was going to cash in after he retired. And I probably would have placed all my chips on him profiting off his cyber fearmongering.

> Former National Security Agency chief Gen. Keith Alexander is launching a consulting firm for financial institutions looking to address cybersecurity threats, POLITICO has learned.
>
> Less than two months since his retirement from the embattled agency at the center of the Edward Snowden leak storm, the retired four-star general is setting up a Washington-based operation that will try to attract clients based on his four decades of experience in the military and intelligence — and the continued levels of access to senior decision-makers that affords.

But the part of this story that even I couldn't have predicted — but makes so much sense it brings tears to my eyes — is that he's shacking up with Promontory Financial Group, the revolving door regulator to hire that has been caught underestimating its clients' crimes for big money.

> Alexander will lease office space from the global consulting firm Promontory Financial Group, which confirmed in a statement on Thursday that it plans to partner with him on cybersecurity matters.

> “He and a firm he’s forming will work on the technical aspects of these issues, and we on the risk-management compliance and governance elements,” said Promontory spokesman Chris Winans.

I’m impressed, Lying Keith: You’ve done my very low expectations even one better!

---

# THE IP POLICE ARMED WITH INTERNET VULNERABILITIES

The White House Cybersecurity Coordinator, Michael Daniel, has a post purporting to lay out “established principles” on when the Administration would and would not disclose software and hardware vulnerabilities.

I’ve got a more thorough read below the rule, but I want to focus on one particular line. Daniel describes the downside of disclosing vulnerabilities as losing intelligence.

> Disclosing a vulnerability can mean that we forego an opportunity to collect crucial intelligence that could thwart a terrorist attack [sic] stop the theft of our nation’s intellectual property, or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries to exploit our networks.

That is, Daniel lays out three threats — terrorism, “hackers or other adversaries,” and IP thieves — that require we use vulnerabilities to combat.

The inclusion of terrorism is not a surprise. That’s the excuse NSA has been using since last

June to justify its work.

Cybersecurity ("hackers or other [presumably far more threatening] adversaries") is the threat that NSA was focused on until such time as it needed to chant terror terror terror to get people to buy into the dragnet. Not only is it not a surprise, but it's probably the most urgent reason to use vulnerabilities (even if the threat in question is really far more serious than hackers).

But IP thieves?

To be fair, by this Daniel may be meaning Lockheed-Martin's intellectual property, by which he really means that intellectual property that we fetishize as private property but is really national security. (I've got a question in with the White House on this point.) But stated as he does, it could as easily mean Monsanto and Pfizer and even Disney.

In fact, he may well mean that. As I noted, in its original statement, the Administration made quite clear they would use Zero Days for law enforcement as well as national security purposes. Moreover, as I have also noted, NSA rewrote the legally mandated minimization standards in its secret procedures to equate threats to property with threats to life and body, thereby permitting itself to keep data that reveals threats to property that are not otherwise evidence of crime indefinitely (with DIRNSA approval).

And all that's assuming only NSA will exploit Zero Days. There's no reason to assume that the FBI (and other law enforcement agencies, including DEA) aren't using them.

I'm not sure that's a bad thing either. Several great security experts recently endorsed using hacks for law enforcement, though insisted that overall security must not be compromised.

That's the point though: how low is the bar for exploiting vulnerabilities? And if they are going to be used for law enforcement purposes —

to chase IP thieves rather than threats to our nation — why isn't it more public?

---

Here are some additional comments:

Note how Daniel refers to NSA's denial in Heartbleed:

> Earlier this month, the NSA sent out a Tweet making clear that it did not know about the recently discovered vulnerability in OpenSSL known as Heartbleed.

I find it notable that he was that specific given allegations of other NSA knowledge of SSL vulnerabilities.

Here's how Daniel describes the interagency process that was rolled out in secret in response to the Presidential Review Group.

> This spring, we re-invigorated our efforts to implement existing policy with respect to disclosing vulnerabilities — so that everyone can have confidence in the integrity of the process we use to make these decisions.
>
> [snip]
>
> We have also established a disciplined, rigorous and high-level decision-making process for vulnerability disclosure. This interagency process helps ensure that all of the pros and cons are properly considered and weighed.

He makes no mention, though, that it came in response to the PRG (which in turn came in response to Edward Snowden's disclosures, including disclosures about the Bullrun program aiming to create back doors). Nor does he describe us an even more basic detail: what entities get included in that interagency process (the PRG was quite specific about the

entities that should be involved).

Note the description of the Internet's role in US power, including "projecting power."

> We rely on the Internet and connected systems for much of our daily lives. Our economy would not function without them. Our ability to project power abroad would be crippled if we could not depend on them. For these reasons, disclosing vulnerabilities usually makes sense. We need these systems to be secure as much as, if not more so, than everyone else.

That's a hint of an admission of the Internet's role in our own hegemonic position, though not an explanation of all that entails. Again, that's something that should be part of the public discussion.

Finally, here's the list of the questions Daniel says unnamed stakeholders in this process will ask.

- How much is the vulnerable system used in the core internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems?
- Does the vulnerability, if left unpatched, impose significant risk?
- How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
- How likely is it that we would know if someone else was exploiting it?
- How badly do we need the

intelligence we think we can get from exploiting the vulnerability?

- Are there other ways we can get it?
- Could we utilize the vulnerability for a short period of time before we disclose it?
- How likely is it that someone else will discover the vulnerability?
- Can the vulnerability be patched or otherwise mitigated?

Folks on Twitter yesterday suggested that some of these questions — especially the one purporting to know whether anyone else will find a vulnerability — betray a real arrogance about our ability to know these things.

I guess that makes it easier to use this stuff for law enforcement, as well as larger national security, problems.

---

# OBAMA'S LEGAL HACKS

I have a piece over at The Week on the unusually credible denial the government issued on Friday, claiming they did not know of the Heartbleed vulnerability until earlier this month. In it, I note that Obama adopted a much lower bar for using software vulnerability than his hand-picked Review Group recommended in December. Most troubling, Obama admits he will use exploits for law enforcement, in addition to national security.

> But the announcement's discussion of the interagency review also made clear that the process will, sometimes, approve such a use — which means that the next Heartbleed could be exploited by the NSA. Furthermore, the standard the administration claims to have adopted — "a clear national security or *law enforcement* need" (italics mine) — is lower than the "urgent and significant national security priority" recommended by the Review Group.
>
> In other words, in very clear language, the government has confessed that it does and will continue to keep secret Heartbleed-style vulnerabilities not just for national security purposes, but also for mere law enforcement.

The idea that the government might hack in the name of law enforcement is not new.

As WSJ reported last month, DOJ is trying to get the Judicial Conference to approve language allowing it to get warrants to hack in multiple districts at once.

> The government's push for rule changes sheds light on law enforcement's use of remote hacking techniques, which are being deployed more frequently but have been protected behind a veil of secrecy for years.
>
> In documents submitted by the government to the judicial system's rule-making body this year, the government discussed using software to find suspected child pornographers who visited a U.S. site and concealed their identity using a strong anonymization tool called Tor.
>
> The government's hacking tools—such as sending an email embedded with code that installs spying software — resemble those used by criminal hackers. The

> government doesn't describe these methods as hacking, preferring instead to use terms like "remote access" and "network investigative techniques."
>
> Right now, investigators who want to search property, including computers, generally need to get a warrant from a judge in the district where the property is located, according to federal court rules.
>
> In a computer investigation, that might not be possible, because criminals can hide behind anonymizing technologies. In cases involving botnets—groups of hijacked computers—investigators might also want to search many machines at once without getting that many warrants.
>
> Some judges have already granted warrants in cases when authorities don't know where the machine is. But at least one judge has denied an application in part because of the current rules. The department also wants warrants to be allowed for multiple computers at the same time, as well as for searches of many related storage, email and social media accounts at once, as long as those accounts are accessed by the computer being searched.

I especially applaud the way WSJ highlighted DOJ's complaints about Orin Kerr calling what they do hacking.

Even more timely, a team of computer security experts — Steve Bellovin, Matt Blaze, Sandy Clark, and Susan Landau — just published a paper arguing that legal hacking is a better means to conduct law enforcement collection than a CALEA-type solution. But they argue that the government can and must achieve this law enforcement objective without compromising the security of the network.

> ¶162 As we alluded to earlier, this is a clash of competing social goods between the security obtained by patching as quickly as possible and the security obtained by downloading the exploit to enable the wiretap to convict the criminal. Although there are no easy answers, we believe the answer is clear. In a world of great cybersecurity risk, where each day brings a new headline of the potential for attacks on critical infrastructure,239 where the Deputy Secretary of Defense says that thefts of intellectual property "may be the most significant cyberthreat that the United States will face over the long term,"240 public safety and national security are too critical to take risks and leave vulnerabilities unreported and unpatched. We believe that law enforcement should always err on the side of caution in deciding whether to refrain from informing a vendor of a vulnerability. Any policy short of full and immediate reporting is simply inadequate. "Report immediately" is the policy that any crime-prevention agency should have, even though such an approach will occasionally hamper an investigation.241
>
> ¶163 Note that a report immediately policy does not foreclose exploitation of the reported vulnerability by law enforcement. Vulnerabilities reported to vendors do not result in immediate patches; the time to patch varies with each vendor's patch release schedule (once per month, or once every six weeks is common), but, since vendors often delay patches,242 the lifetime of a vulnerability is often much longer. Research shows that the average lifetime of a zero-day exploit is 312 days.243 Furthermore, users frequently do not patch their systems promptly, even when critical updates are available.24

> ¶164 Immediate reporting to the vendor of vulnerabilities considered critical will result in a shortened lifetime for particular operationalized exploits, but it will not prevent the use of operationalized exploits. Instead, it will create a situation in which law enforcement is both performing criminal investigations using the wiretaps enabled through the exploits, and crime prevention through reporting the exploits to the vendor. This is clearly a win/win situation.
>
> [snip]
>
> ¶166 The tension between exploitation and reporting can be resolved if the government follows both paths, actively reporting and working to fix even those vulnerabilities that it uses to support wiretaps. As we noted, the reporting of vulnerabilities (to vendors and/or to the public) does not preclude exploiting them.247 Once a vulnerability is reported, there is always a lead time before a “patch” can be engineered, and a further lead time before this patch is deployed to and installed by future wiretap targets. Because there is an effectively infinite supply of vulnerabilities in software platforms,248 provided new vulnerabilities are found at a rate that exceeds the rate at which they are repaired, reporting vulnerabilities need not compromise the government’s ability to conduct exploits. By always reporting, the government investigative mission is not placed in conflict with its crime prevention mission. In fact, such a policy has the almost paradoxical affect that the more active the law enforcement exploitation activity becomes, the more zero-day vulnerabilities are reported to and repaired by vendors.

They go on to propose a legal regime that can provide clear guidance on which vulnerabilities should be reported, even analogizing the emergency period in which an agency can wiretap before getting a warrant.

But here's the thing: NSA's Bull Run program got reported in September, and since then the government has remained coy about whether it uses or even seeds vulnerabilities in software, even though anyone paying attention knew it does. It took claims that the government had been using the Heartbleed vulnerability for two years for the Administration to admit, tacitly, the earlier reports were correct.

The kind of legal regime Bellovin et al recommend requires that this law enforcement function operate within a legal — and therefore publicly acknowledged — framework, rather than piggy backing on the NSA's executive authorities in secret.

While Friday's admission is a start, and while it may be true that hacking presents a better solution to law enforcement needs than CALEA, these questions need to be openly discussed.

Otherwise, DOJ not only is hacking — in the dictionary definition Orin Kerr applied — but hacking in the reckless manner that DOJ prosecutes.

---

# FINGERPRINTS AND THE PHONE DRAGNET'S SECRET "CORRELATIONS"

# ORDER

Yesterday, I noted that ODNI is withholding a supplemental opinion approved on August 20, 2008 that almost certainly approved the tracking of "correlations" among the phone dragnet (though this surely extends to the Internet dragnet as well).

I pointed out that documents released by Edward Snowden suggest the use of correlations extends well beyond the search for "burner" phones.

At almost precisely the same time, Snowden was testifying to the EU. The first question he answered served to clarify what "fingerprints" are and how XKeyscore uses them to track a range of innocent activities. (This starts after 11:16, transcription mine.)

> It has been reported that the NSA's XKeyscore for interacting with the raw signals intercepted by mass surveillance programs allow for the creation of something that is called "fingerprints."
>
> I'd like to explain what that really means. The answer will be somewhat technical for a parliamentary setting, but these fingerprints can be used to construct **a kind of unique signature** for any individual or group's communications which are often **comprised of a collection of "selectors" such as email addresses, phone numbers, or user names**.
>
> This allows State Security Bureaus to instantly identify the movements and activities of you, your computers, or other devices, your personal Internet accounts, or even key words or other uncommon strings that indicate an individual or group, out of all the communications they intercept in the world are associated with that particular communication. Much like a fingerprint that you would leave on a

handle of your door or your steering wheel for your car and so on.

However, though that has been reported, that is the smallest part of the NSA's fingerprinting capability. You must first understand that any kind of Internet traffic that passes before these mass surveillance sensors can be analyzed in a protocol agnostic manner – metadata and content, both. And it can be today, right now, searched not only with very little effort, via a complex regular expression, which is a type of shorthand programming. But also via any algorithm an analyst can implement in popular high level programming languages. Now, this is very common for technicians. It not a significant work load, it's quite easy.

This provides a capability for analysts to do things like associate unique identifiers assigned to untargeted individuals via unencrypted commercial advertising networks through cookies or other trackers – common tracking means used by businesses everyday on the Internet – with personal details, such as individuals' precise identity, personal identity, their geographic location, their political affiliations, their place of work, their computer operating system and other technical details, their sexual orientation, their personal interests, and so on and so forth. There are very few practical limitations to the kind of analysis that can be technically performed in this manner, short of the actual imagination of the analysts themselves.

And this kind of complex analysis is in fact performed today using these systems. I can say, with authority, that the US government's claim that "keyword filters," searches, or "about" analysis,

> had not been performed by its intelligence agencies are, in fact, false. I know this because I have personally executed such searches with the explicit authorization of US government officials. And I can personally attest that these kind of searches may scrutinize communications of both American and European Union citizens without involvement of any judicial warrants or other prior legal review.
>
> What this means in non-technical terms, more generally, is that I, an analyst working at NSA, or, more concerningly, an analyst working for a more authoritarian government elsewhere, can without the issue of any warrant, create an algorithm that for any given time period, with or without human involvement, sets aside the communications of not only targeted individuals, but even a class of individual, and that just indications of an activity – or even just indications of an activity that I as the analyst don't approve of – something that I consider to be nefarious, or to indicate nefarious thoughts, or pre-criminal activity, even if there's no evidence or indication that's in fact what's happening. that it's not innocent behavior. The nature of the mass surveillance – of these mass surveillance technologies – create a de facto policy of assigning guilt by association rather than on the basis of specific investigations based on reasonable suspicion.
>
> Specifically, mass surveillance systems like XKeyscore provide organizations such as the NSA with the technical ability to trivially track entire populations of individuals who share any trait that is discoverable from

> unencrypted communications. For example, these include religious beliefs, political affiliations, sexual orientations, contact with a disfavored individual or group, history of donating to specific or general causes, interactions of transactions with certain private businesses, or even private gun ownership. It is a trivial task, for example, to generate lists of home addresses for people matching the target criteria. Or to collect their phone numbers, to discover their friends, or even, to analyze the proximity and location of their social connections by automating the detection of factors such as who they share pictures of their children with, which is capable of machine analysis.
>
> I would hope that this goes without saying, but let me be clear that the NSA is not engaged in any sort of nightmare scenarios, such as actively compiling lists of homosexual individuals to round them up and send them into camps, or anything of that sort. However, they still deeply implicate our human rights. We have to recognize that the infrastructure for such activities has been built, and is within reach of not just the United States and its allies, but of any country today. And that includes even private organizations that are not associated with governments.
>
> Accordingly, we have an obligation to develop international standards, to protect against the routine and substantial abuse of this technology, abuses that are ongoing today. I urge the committee in the strongest terms to bear in mind that this is not just a problem for the United States, or the European Union, but that this is in fact a global problem, not an isolated issue of Europe versus the Five Eyes or any

> other [unclear]. These technical capabilities don't merely exist, they're already in place and actively being used without the issue of any judicial warrant. I state that these capabilities are not yet being used to create lists of all the Christians in Egypt, but let's talk about what they are used for, at least in a general sense, based on actual real world cases that I can assert are in fact true.
>
> Fingerprints — for example, the kind used of XKeyscore — have been used — I have specific knowledge that they have been used — to track and intercept, to track, intercept, and monitor the travels of innocent citizens, who are not suspected of anything worse than booking a flight. This was done, in Europe, against EU citizens but it is of course not limited to that geographic region, nor that population. Fingerprints have also been used to monitor untold masses of people whose communications transit the entire country of Switzerland over specific routes. They're used to identify people — Fingerprints are used to identify people who have had the bad luck to follow the wrong link on an Internet site, on an Internet forum, or even to download the wrong file. They've been used to identify people who simply visit an Internet sex forum. They've also been used to monitor French citizens who have never done anything wrong other than logging into a network that's suspected of activity that's associated with a behavior that the National Security Agency does not approve of.
>
> This mass surveillance network, constructed by the NSA, which, as I pointed out, is an Agency of the US military Department of Defense, not a civilian agency, and is also enabled by

> agreements with countries such as the United Kingdom, Australia, and even Germany, is not restricted for being used strictly for national security purposes, for the prevention of terrorism, or even for foreign intelligence more broadly.
>
> XKeyscore is today secretly being used for law enforcement purposes, for the detection of even non-violent offenses, and yet this practice has never been declared to any defendant or to any open court.
>
> We need to be clear with our language. These practices are abusive. This is clearly a disproportionate use of an extraordinarily invasive authority, an extraordinarily invasive means of investigation, taken against entire populations, rather than the traditional investigative standard of using the least intrusive means or investigating specifically named targets, individuals, or groups. The screening of trillions – I mean that literally, trillions – of private communications for the vaguest indications of associations or some other nebulous pre-criminal activity is a violation of the human right to be free from unwarranted interference, to be secure in our communications and our private affairs, and it must be addressed. These activities – routine, I point out, unexceptional activities that happen every day – are only a tiny portion of what the Five Eyes are secretly doing behind closed doors, without the review, consent, or approval of any public body. This technology represents the most significant – what I consider the most significant.new threat to civil rights in modern times.

Now, this doesn't guarantee that the NSA correlates identifiers to dump them into

XKeyscore (which is, as far as I know, used only on data collected outside the US; the "about" 702 collection is a more limited version of what is done in the US, with returned data likely dumped into databases used with XKeyscore). But Snowden makes it clear such fingerprints involve precisely the identifiers, including phone numbers, used in the domestic dragnets.

Moreover, we know that data in the corporate store — all those people who are two or three degrees away from someone who has been digitally stop-and-frisked — is subject to all the analytical authorities the NSA uses, which clearly includes fingerprinting and use in XKeyscore.

"Correlations" — as the NSA uses in language with the FISC and Congress — are almost certainly either fingerprints, or subset of the fingerprinting process.

And this is, almost certainly, what the government is hiding in that August 20, 2008 order.

---

# US TRADE REP COMPLAINS OTHER COUNTRIES AREN'T LETTING NSA SPY

In the NYT, David Sanger describes US efforts to develop some common understanding over cyberattacks with China by briefing it on what our escalation process would be. Unsurprisingly, China (which hasn't had a massive data leak as an excuse to admit to information now in the public domain) has no reciprocated.

And while Sanger makes it clear the US is still not admitting to StuxNet, his US sources are

coming to understand that the rationalizations we use to excuse our spying aren't really as meaningful as we like to tell ourselves.

> Mr. Obama told the Chinese president that the United States, unlike China, did not use its technological powers to steal corporate data and give it to its own companies; its spying, one of Mr. Obama's aides later told reporters, is solely for "national security priorities." But to the Chinese, for whom national and economic security are one, that argument carries little weight.
>
> "We clearly don't occupy the moral high ground that we once thought we did," said one senior administration official.

I especially love the spectacle of an SAO coming to grips with this, but doing so anonymously.

Yet this anonymous admission will not stop the US from imposing such double standards. On Friday, the US Trade Representative issued its yearly report on barriers to trade in telecom and related industries. (Reuters reported on the report here.) None of these complaints are explicitly about the NSA. And some of USTR's demands — that Turkey stop shutting down services like Twitter — would make it harder for other countries to spy on their own citizens.

But many of the USTR's complaints single out measures that are either deliberately meant to undermine NSA's spying advantages, or would have the effect of doing so. So these complaints also amount to whining that other countries are making NSA's job harder.

Consider some of the complaints against China, whose top equipment manufacturer Huawei the US has excluded from not only the US, but also Korea and Australia.

It complains about China's limits on telecom providers — and pretends this is exclusively a

trade issue, not a national security issue.

> Moreover, the Chinese Government still owns and controls the three major basic telecom operators in the telecommunications industry, and appears to see these entities as important tools in broader industrial policy goals, such as promoting indigenous standards for network equipment.

USTR criticizes China's categorization of business that can be used for spying – such as cloud computing firms – as a telecoms subject to licensing restrictions.

> China's equity restrictions on foreign participation constitute a major impediment to market access in China. These restrictions are compounded by China's broad interpretation of services requiring a telecommunications license (and thus subject to equity caps) and narrow interpretation of the specific services foreign firms can offer in these sub-sectors.
>
> [snip]
>
> Several VAS definitions in the draft Catalog also raise trade restriction concerns. First, the draft Catalog created a new category of "Internet Resource Collaboration Services" that appears to covers all aspects of cloud computing. (Cloud computing is a computer service or software delivery model, and should not be misclassified as a telecommunications service.) MIIT approach to cloud computing generally raises a host of broad concerns. Second, the draft Catalog significantly expanded the definition of "Information Services" to include software application stores, software delivery platforms, social networking websites, blogs, podcasts, computer security products, and a number

> of other Internet and computing services. These services simply use the Internet as a platform for providing business and information to customers, and thus should not be considered as telecommunications services.

USTR complains about Chinese requirements for encryption both for information systems tied to critical infrastructure.

> Starting in 2012, both bilaterally and during meetings of the WTO's Committee on Technical Barriers to Trade, the United States raised its concerns with China about framework regulations for information security in critical infrastructure known as the Multi-Level Protection Scheme (MLPS), first issued in June 2007 by the Ministry of Public Security (MPS) and the Ministry of Industry and Information Technology (MIIT). The MLPS regulations put in place guidelines to categorize information systems according to the extent of damage a breach in the system could pose to social order, public interest, and national security. The MLPS regulations also appear to require buyers to comply with certain information security technical regulations and encryption regulations that are referenced within the MLPS regulations. If China issues implementing rules for the MLPS regulations and applies the rules broadly to commercial sector networks and IT infrastructure, they could adversely affect sales by U.S. information security technology providers in China.

And for providers on its 4G network.

> At the end of 2011 and into 2012, China released a Chinese government-developed

> 4G Long-Term Evolution (LTE) encryption algorithm known as the ZUC standard. The European Telecommunication Standards Institute (ETSI) 3rd Generation Partnership Project (3GPP) had approved ZUC as a voluntary LTE encryption standard in September 2011. According to U.S. industry reports, MIIT, in concert with the State Encryption Management Bureau (SEMB), informally announced in early 2012 that only domestically developed encryption algorithms, such as ZUC, would be allowed for the network equipment and mobile devices comprising 4G TD-LTE networks in China. It also appeared that burdensome and invasive testing procedures threatening companies' sensitive intellectual property could be required.
>
> In response to U.S. industry concerns, USTR urged China not to mandate any particular encryption standard for 4G LTE telecommunications equipment, in line with its bilateral commitments and the global practice of allowing commercial telecommunications services providers to work with equipment vendors to determine which security standards to incorporate into their networks.

Finally, USTR dubs China's limits on outsider VOIP services a trade restriction.

> Restrictions on VoIP services imposed by certain countries, such as prohibiting VoIP services, requiring a VoIP provider to partner with a domestic supplier, or imposing onerous licensing requirements have the effect of restricting legitimate trade or creating a preference for local suppliers, typically former monopoly suppliers.

All of these complaints, of course, can be viewed narrowly as a trade problem. But the

underlying motivation on China's part is almost certainly about keeping the US out of its telecom networks, both to prevent spying and to sustain speech restraints behind the Great Firewall.

It's not just China about which USTR complains. It issues similar dual purpose (trade and spying) complaints against India and Colombia, among others.

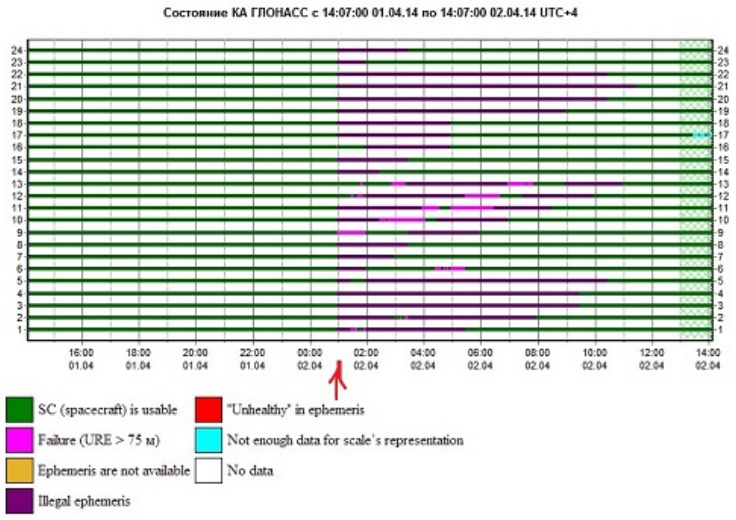
And of course, it finds European plans to require intra-EU transit limits – a plan done largely to combat US spying – a 'draconian" trade restriction.

> In particular, Deutsche Telekom AG (DTAG), Germany's biggest phone company, is publicly advocating for EU-wide statutory requirements that electronic transmissions between EU residents stay within the territory of the EU, in the name of stronger privacy protection. Specifically, DTAG has called for statutory requirements that all data generated within the EU not be unnecessarily routed outside of the EU;
>
> [snip]
>
> The United States and the EU share common interests in protecting their citizens' privacy, but the draconian approach proposed by DTAG and others appears to be a means of providing protectionist advantage to EU-based ICT suppliers.

Meanwhile, even as I was writing this, one of the EU's top Data Privacy figures, Paul Nemitz, just floated making the reverse accusation against America, that its NSA spying is a trade impediment to European businesses trying to do business in the US.

Fun stuff.

# [UPDATED] RUSSIAN GPS-ALTERNATIVE SATELLITES WENT 'ILLEGAL/FAILURE': SOLAR STORM DAMAGE OR CYBERWAR IN SPACE?




[*Update at end of article.—Rayne 6:45 pm EST*]

Between 1030 and 0400 UTC last night or early morning, most of Russia's GLONASS satellites reported "illegal" or "failure" status. As of this post, they do not appear to be back online.

GLONASS is the equivalent of GPS, an alternative global navigation satellite system (GNSS) launched and operated by Russian Aerospace Defense Forces (RADF). Apart from GPS, it is the only other GNSS with global capability.

It's possible that the outage is related to either a new M-class solar storm – the start of which was reported about 48 hours ago – or recent X-class solar flare on March 29 at

approximately 1700 UTC. The latter event caused a short-term radio blackout about one hour after the flare erupted.

But there is conjecture that GLONASS' outage is human in origin and possibly deliberate. The absence of any reported outage news regarding GPS and other active satellite systems suggests this is quite possible, given the unlikelihood that technology used in GLONASS differs dramatically from that used in other satellite systems.

At least one observer mentioned that a monitoring system tripped at 21:00 UTC – 00:00 GLONASS system time. The odds of a natural event like a solar storm tripping at exactly top of the hour are ridiculously slim, especially since radiation ejected from the new M-class storm may not reach its peak effect on earth for another 24-48 hours.


It's not clear whether the new GLONASS-M satellite launched March 24th may factor into this situation. There are no English language reports indicating the new satellite was anything but successful upon its release, making it unlikely its integration into the GLONASS network caused today's outage.

If the outage is based in human activity, the problem may have been caused by:

– an accidental disabling here on earth, though RADF most likely has redundancies to prevent such a large outage;

– deliberate tampering here on earth, though with RADF as operator this seems quite unlikely; or

– deliberate tampering in space, either through scripts sent from earth, or technology installed with inherent flaws.

The last is most likely, and of either scripts sent from earth or the flawed technology scenarios, the former is more likely to cause a widespread outage.

However, if many or all the core operating systems on board the GLONASS satellites had been updated within the last four years – after the discovery of Stuxnet in the wild – it's not impossible that both hardware and software were compromised with an infection. Nor is it impossible that the same infection was triggered into aggressive action from earth.

Which begs the question: are we in the middle of a cyberwar in space?

**UPDATE – 6:45 PM EST–**

Sources report the GLONASS satellite network was back online noon-ish Russian time (UTC+4); the outage lasted approximately 11 hours. Unnamed source(s) said the outage was due to the upload of bad ephemeris data, the information used by the satellites to locate other satellites in space. An alleged system-wide update with bad data suggests RADF has serious problems with change management, though.

There is speculation the M-class solar storm, summarized at 1452 UTC as an "X-ray Event exceeded M5," may have impacted GLONASS. However early feedback about radiation ejected by an M-class storm indicated the effects would not reach earth for 24-48 hours after the storm's eruption.

---

# THE RUPPROGE FAKE

# DRAGNET FIX, AS INTRODUCED: DOES IT INCLUDE KEITH ALEXANDER'S QUID PRO QUO?

This post is going to be a general review on the contents of the actual records collection part of the RuppRoge Fake Dragnet Fix, which starts on page 15, though I confess I'm particularly interested in what other uses — besides the phone dragnet — it will be put to.

First, note that this bill applies to "electronic communication service providers," not telecoms. In addition, it uses neither the language of Toll Records from National Security Letters nor Dialing, Addressing, Routing, or Signalling from Pen Registers. Instead, it uses "records created as a result of communications of an individual or facility." Also remember that FISC has, in the past, interpreted "facility" to mean "entire telecom switch." This language might permit a lot of things, but I suspect that one of them is another attempt to end run content collection restrictions on Internet metadata — the same problem behind the hospital confrontation and the Internet dragnet shutdown in 2009. I look forward to legal analysis on whether this successfully provides an out.

The facility language is also troubling in association with the foreign power language of the bill (which already is a vast expansion beyond the terrorism-only targeting of the phone dragnet). Because you could have a telecom switch in contact with a suspected agent of a foreign power and still get a great deal of data, much of it on innocent people. The limitation (at b1B) to querying with "specific identifiers or selection terms' then becomes far less meaningful.

Then add two details from section h, covering the directives the government gives the providers. The government requires the data in the format they want. Section 215 required existing business records, which may have provided providers a way to be obstinate about how they delivered the data (and this may have led to the government's problems with the cell phone data). But it also says this (in the paragraph providing for compensation I wrote about here):

> The Government may provide any information, facilities, or assistance necessary to aid an electronic communications service provider in complying with a directive

Remember, one month ago, Keith Alexander said he'd be willing to trade a phone dragnet fix for what amounts to the ability to partner with industry on cybersecurity. The limits on this bill to electronic communication service providers means it's not precisely what Alexander wanted (I understand him to want that kind of broad partnership across industries). Still, the endorsement of the government basically going to camp out at a provider makes me wonder if there isn't some of that. Note, that also may answer my question about when and where NSA would conduct the pizza joint analysis, which would mean there'd still be NSA techs (or contractors) rifling through raw data, but they'd be doing it at the telecoms' location.

The First Amendment restriction appears more limited than it is in the Section 215 context, though I suspect RuppRoge simply reflects the reality of what NSA is doing now. Both say you can't investigate an American solely for First Amendment views, but RuppRoge says you can't get the information for an investigation of an American. Given that RuppRoge eliminates any requirement that this collection be tied to an investigation, it would make it very easy to query a US person selector based on First

Amendment issues in the guise of collecting information for another reason. But again, I suspect that's what the NSA is doing in practice in any case.

Note, too, that RuppRoge borrows the "significant purpose" language from FISA, meaning the government can have a domestic law enforcement goal to getting these records.

RuppRoge then lays out an elaborate certification/directive system that is (as I guessed) modeled on the FISA Amendments Act, but written to be even more Byzantine in the bill. It works the same, though: the Attorney General and the Director of National Intelligence submit broad certifications to the FISC, which reviews whether they comply with the general requirements in the bill. It can also get emergency orders (though for some reason here, as elsewhere, RuppRoge have decided to invent new words from the standard ones), though the language is less about emergency and more about timely acquisition of data. Ultimately, there is judicial review, after the fact, except that like FAA, the review is programmatic, not identifier specific. Significantly, the records the government has to keep only need to comply with selection procedures (which are the new name for targeting procedures) "at the time the directive was issued," which would seem to eliminate any need to detask over a year if you discover the target isn't actually in contact with an agent of a foreign power. Also, in the clause permitting the FISC to order data be destroyed if the directives were improper, the description talks about halting production of "records," but destruction of "information." That might be more protective (including the destruction of reports based on data) or it might not (requiring only the finished reports be destroyed). Interestingly, this section includes no language affirmatively permitting alert systems, though RuppRoge have made it clear that's what they intend with the year long certifications. In addition, those year long certifications might be used in conjunction with

a year long PRISM order to first search a provider for metadata, then immediately task on content (which would be useful in a cybersecurity context).

The bill also changed the language of minimization procedures, which they call "civil liberties and privacy protection procedures." Interestingly, the procedures differ from the standard in Section 215, including both a generalized privacy protection and one limiting receipt and dissmenation of "records associated with a specific person." These might actually be more protective than those in Section 215, or they might not, given that the identifying information (at b1D) excludes things like phone number or email which clearly identify a specific person, but get no protection (this identifying information hearkens back, at least in part, to debates about whether the dragnet minimization procedures complied with requirement for them in law on this point). In other words, it may provide people more protection, but given the NSA's claim that they can't get identify from a phone number, they likely don't consider that data to be protected at all.

I can't help believing much of this bill was written with cases like Lavabit and the presumed Credo NSL challenges in mind, as it uses language disdainful of legal challenges.

> If the judge determines that such petition consists of claims, defenses, or other legal contentions that are not warranted by existing law or consists of a frivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of the such petition and order the recipient to comply with the directive or any part of it.

This seems to completely rule out any constitutional challenge to this law from providers.  Though the bill even allows for emergency acquisition while FISC is reviewing a certification, suggesting RuppRoge don't want the FISC to make any through either. So if this bill were to pass, you can be sure it will remain in place indefinitely.

---

# NSA BIDS TO EXPAND SPYING IN GUISE OF "FIXING" PHONE DRAGNET

Dutch Ruppersberger has provided Siobhan Gorman with details of his plan to "fix" the dragnet — including repeating the laughable claim that the "dragnet" (which she again doesn't distinguish as solely the Section 215 data that makes up a small part of the larger dragnet) doesn't include cell data.

Only, predictably, it's not a "fix" of the phone dragnet at all, except insofar as NSA appears to be bidding to use it to do all the things they want to do with domestic dragnets but haven't been able to do legally. Rather, it appears to be an attempt to outsource to telecoms some of the things the NSA hasn't been able to do legally since 2009.

For example, there's the alert system that Reggie Walton shut down in 2009.

As I reported back in February, the NSA reportedly has never succeeded in replacing that alert system, either for technical or legal reasons or both.

> NSA reportedly can't get its automated chaining program to work. In the motion

> to amend, footnote 12 — which modifies part of some entirely redacted paragraphs describing its new automated alert approved back in 2012 — reads:
>
> > The Court understands that to date NSA has not implemented, and for the duration of this authorization will not as a technical matter be in a position to implement, the automated query process authorized by prior orders of this Court for analytical purposes. Accordingly, this amendment to the Primary Order authorizes the use of this automated query process for development and testing purposes only. No query results from such testing shall be made available for analytic purposes. Use of this automated query process for analytical purposes requires further order of this Court.
>
> PCLOB describes this automated alert this way.
>
> > In 2012, the FISA court approved a new and automated method of performing queries, one that is associated with a new infrastructure implemented by the NSA to process its calling records.68 The essence of this new process is that, instead of waiting for individual analysts to perform manual queries of particular selection terms that have been RAS approved, the NSA's database periodically performs queries on all RAS-approved seed terms, up to three hops away from the approved seeds. The database places the results of these queries

> > together in a repository called the “corporate store.”
>
> It has been 15 months since FISC approved this alert, but NSA still can’t get it working.
>
> I suspect this is the root of the stories claiming NSA can only access 30% of US phone records.

As described by WSJ, this automated system will be built into the orders NSA provides telecoms; once a selector has been provided to the telecoms, they will keep automatically alerting on it.

> Under the new bill, a phone company would search its databases for a phone number under an individual “directive” it would receive from the government. It would send the NSA a list of numbers called from that phone number, and possibly lists of phone numbers those numbers had called. **A directive also could order a phone company to search its database for such calls as future records come in**. [my emphasis]

This would, presumably, mean NSA still ends up with a corporate store, a collection of people against whom the NSA has absolutely not a shred of non-contact evidence, against whom they can use all their analytical toys, including searching of content.

Note, too, that this program uses the word “directive,” not query. Directive comes from the PRISM program, where the NSA gives providers generalized descriptions and from there have broad leeway to add new selectors. Until I hear differently, I’ll assume the same is true here: that this actually involves less individualized review before engaging in 2 degrees of Osama bin Laden.

The legislation seems ripe for inclusion of querying of Internet data (another area where the NSA could never do what it wanted to legally after 2009), given that it ties this program to "banning" (US collection of, but Gorman doesn't say that either, maintaining her consistency in totally ignoring that EO 12333 collection makes up the greater part of bulk programs) Internet bulk data collection.

> The bill from Intelligence Committee Chairman Mike Rogers (R., Mich.) and his Democratic counterpart, Rep. C.A. "Dutch" Ruppersberger (D., Md.), would ban so-called bulk collection of phone, email and **Internet** records by the government, according to congressional aides familiar with the negotiations. [my emphasis]

Call me crazy, but I'm betting there's a way they'll spin this to add in Internet chaining with this "fix."

Note, too, Gorman makes no mention of location data, in spite of having tied that to her claims that NSA only collects 20% of data. Particularly given that AT&T's Hemisphere program provides location data, we should assume this program could too, which would present a very broad expansion on the status quo.

And finally, note that neither the passage I quoted above on directives to providers, nor this passage specifies what kind of investigations this would be tied to (though they are honest that they want to do away with the fig leaf of this being tied to investigations at all).

> The House intelligence committee bill doesn't require a request be part of an ongoing investigation, Mr. Ruppersberger said, because intelligence probes aim to uncover what should be investigated, not what already is under investigation.

Again, the word "directive" in the PRISM context also provides the government the ability to secretly pass new areas of queries — having expanded at least from counterterrorism to counterproliferation and cybersecurity uses. So absent some very restrictive language, I would assume that's what would happen here: NSA would pass it in the name of terrorism, but then use it primarily for cybersecurity and counterintelligence, which the NSA considers bigger threats these days.

And that last suspicion? That's precisely what Keith Alexander said he planned to do with this "fix," presumably during the period when he was crafting this "fix" with NSA's local Congressman: throw civil libertarians a sop but getting instead an expansion of his cybersecurity authorities.

Update: Here's Spencer on HPSCI, confirming it's as shitty as I expected.

And here's Charlie Savage on Obama's alternative.

It would:

- Keep Section 215 in place, though perhaps with limits on whether it can be used in this narrow application
- Enact the same alert-based system and feed into the corporate store, just as the HPSCI proposal would
- Include judicial review like they have now (presumably including automatic approval for FISA targets)

Obama's is far better than HPSCI (though this seems to be part of a bad cop-good cop plan, and the devil remains in the details). But there are still some very serious concerns.

# HOW THE NSA DEALS WITH A THREAT TO ITS BACKBONE HEGEMONY

I have talked before about the importance of US' dominant role in global telecom infrastructure in our hegemonic position.

> US hegemony rests on a lot of things: the dollar exchange, our superlative military, our ideological lip service to democracy and human rights.
>
> But for the moment, it also rests on the globalized communication system in which we have a huge competitive advantage. That is, one reason we are the world's hegemon is because the rest of the world communicates through us — literally, in terms of telecommunications infrastructure, linguistically, in English, and in terms of telecommunications governance.

Which is why these stories (NYT, Spiegel's short version, to be followed by a longer one Monday) about NSA's targeting of Huawei are so interesting. Der Spiegel lays out the threat Huawei poses to US hegemony.

> "We currently have good access and so much data that we don't know what to do with it," states one internal document. As justification for targeting the company, an NSA document claims that "many of our targets communicate over Huawei produced products, we want to make sure that we know how to exploit these products." The agency also states concern that "Huawei's widespread infrastructure will provide the PRC (People's Republic of China) with SIGINT

> capabilities." SIGINT is agency jargon for signals intelligence. The documents do not state whether the agency found information indicating that to be the case.
>
> The operation was **conducted with the involvement of the White House intelligence coordinator** and the FBI. One document states that the threat posed by Huawei is "unique".
>
> The agency also stated in a document that "the intelligence community structures are not suited for handling issues that combine economic, counterintelligence, military influence and telecommunications infrastructure from one entity."
>
> **Fears of Chinese Influence on the Net**
>
> **The agency notes that understanding how the firm operates will pay dividends in the future.** In the past, the network infrastructure business has been dominated by Western firms, but the Chinese are working to make American and Western firms "less relevant". That Chinese push is beginning to open up technology standards that were long determined by US companies, and China is controlling an increasing amount of the flow of information on the net. [my emphasis]

And the NSA document the NYT included makes this threat clear.

> There is also concern that Huawei's widespread infrastructure will provide the PRC with SIGINT capabilities and enable them to perform denial of service type attacks.

Now, for what it's worth, the NYT story feels like a limited hangout — an attempt to pre-empt

what Spiegel will say on Monday, and also include a bunch of details on NSA spying on legitimate Chinese targets so the chattering class can talk about how Snowden is a tool of Chinese and Russian spies. (Note, the NYT story relies on interviews with a "half dozen" current and former officials for much of the information on legitimate Chinese targets here, a point noted by approximately none of the people complaining.)

But the articles make it clear that 3 years after they started this targeted program, SHOTGIANT, and at least a year after they gained access to the emails of Huawei's CEO and Chair, NSA still had no evidence that Huawei is just a tool of the People's Liberation Army, as the US government had been claiming before and since. Perhaps they've found evidence in the interim, but they hadn't as recently as 2010.

Nevertheless the NSA still managed to steal Huawei's source code. Not just so it could more easily spy on people who exclusively use Huawei's networks. But also, it seems clear, in an attempt to prevent Huawei from winning even more business away from Cisco.

I suspect we'll learn far more on Monday. But for now, we know that even the White House got involved in an operation targeting a company that threatens our hegemony on telecom backbones.

---

# IN NOMINATION HEARING, DIRNSA NOMINEE MIKE ROGERS CONTINUES JAMES

# CLAPPER AND KEITH ALEXANDER'S OBFUSCATION ABOUT BACK DOOR SEARCHES

Yesterday, the Senate Armed Services Committee held a hearing for Vice Admiral Mike Rogers to serve as head of Cyber Command (see this story from Spencer about how Rogers' confirmation as Cyber Command chief serves as proxy for his role as Director of National Security Agency because the latter does not require Senate approval).

Many of the questions were about Cyber Command (which was, after all, the topic of the hearing), but a few Senators asked questions about the dragnet that affects us all.

In one of those exchanges — with Mark Udall — Rogers made it clear that he intends to continue to hide the answers to very basic questions about how NSA conducts warrantless surveillance of Americans, such as whether the NSA conducts back door searches on American people.

> Udall: If I might, in looking ahead, I want to turn to the 702 program and ask a policy question about the authorities under Section 702 that's written into the FISA Amendments Act. The Committee asked your understanding of the legal rationale for NASA [sic] to search through data acquired under Section 702 using US person identifiers without probable cause. You replied the NASA—the NSA's court approved procedures only permit searches of this lawfully acquired data using US person identifiers for valid foreign intelligence purposes and under the oversight of the Justice Department and the DNI. The statute's written to anticipate the incidental collection of Americans' communications in the course

> of collecting the communications of foreigners reasonably believed to be located overseas. But the focus of that collection is clearly intended to be foreigners' communications, not Americans. But declassified court documents show that in 2011 the NSA sought and obtained the authority to go through communications collected under Section 702 and conduct warrantless searches for the communications of specific Americans. Now, my question is simple. **Have any of those searches been conducted?**
>
> Rogers: I apologize Sir, **I'm not in a position to answer that as the nominee.**
>
> Udall: You—yes.
>
> Rogers: But if you would like me to come back to you in the future if confirmed to be able to specifically address that question I will be glad to do so, Sir.
>
> Udall: Let me follow up on that. You may recall that Director Clapper was asked this question in a hearing earlier this year and he didn't believe that an open forum was the appropriate setting in which to discuss these issues. The problem that I have, Senator Wyden's had, and others is that we've tried in various ways to get an unclassified answer – simple answer, yes or no – to the question. We want to have an answer because it relates – the answer does – to Americans' privacy. **Can you commit to answering the question before the Committee votes on your nomination?**
>
> Rogers: Sir, I believe that one of my challenges as the Director, if confirmed, is how do we engage the American people – and by extension their representatives – in a dialogue in which they have a level of comfort as to what we are doing and why. That is no

> insignificant challenge for those of us with an intelligence background, to be honest. But I believe that one of the takeaways from the situation over the last few months has been as an intelligence professional, as a senior intelligence leader, I have to be capable of communicating in a way that we are doing and why to the greatest extent possible. That perhaps the compromise is, **if it comes to the how we do things, and the specifics, those are perhaps best addressed in classified sessions,** but that one of my challenges is I have to be able to speak in broad terms in a way that most people can understand. And I look forward to that challenge.
>
> Udall: I'm going to continue asking that question and I look forward to working with you to rebuild the confidence. [my emphasis]

The answer to the question Rogers refused to answer is clearly yes. We know that's true because the answer is always yes when Wyden, and now Udall, ask such questions.

But we also know the answer is yes because declassified parts of last August's Semiannual Section 702 Compliance Report state clearly that oversight teams have reviewed the use of this provision, which means there's something to review.

> As reported in the last semiannual assessment, NSA minimization procedures now permit NSA to query its databases containing telephony and non-upstream electronic communications using United States person identifiers in a manner designed to find foreign intelligence information. Similarly, CIA's minimization procedures have been modified to make explicit that CIA may also query its databases using United

> States person identifiers to yield foreign intelligence information. As discussed above in the descriptions of the joint oversight team's efforts at each agency, **the joint oversight team conducts reviews of each agency's use of its ability to query using United States person identifiers.** To date, this review has not identified any incidents of noncompliance with respect to the use of United States person identifiers; as discussed in Section 4, the agencies' internal oversight programs have, however, identified isolated instances in which Section 702 queries were inadvertently conducted using United States person identifiers. [my emphasis]

It even obliquely suggests there have been "inadvertent" violations, though this seems to entail back door searches on US person identifiers without realizing they were US person identifiers, not violations of the procedures for using back door searches on identifiers known to be US person identifiers.

Still, it is an unclassified fact that NSA uses these back door searches.

Yet the nominee to head the NSA refuses to answer a question on whether or not NSA uses these back door searches.

And it's not just in response to this very basic question that Rogers channeled the dishonest approach of James Clapper and Keith Alexander.

As Udall alluded, at the end of a long series of questions about Cyber Command, the committee asked a series of questions about back door searches and other dragnet issues. They asked (see pages 42-43):

- Whether NSA can conduct back door searches on data acquired under EO 12333 and if so under what legal

rationale

- Whether NSA can conduct back door searches on data acquired pursuant to traditional FISA and if so under what legal rationale
- What the legal rationale is for back door searches on data acquired under FISA Amendments Act
- What the legal rationale is for searches on the Section 215 query results in the "corporate store"

I believe every single one of Rogers' answers — save perhaps the question on traditional FISA — involves some level of obfuscation. (See this post for further background on what NSA's Raj De and ODNI's Robert Litt have admitted about back door searches.)

Consider his answer on searches of the "corporate store" as one example.

> **What is your understanding of the legal rationale for searching through the "Corporate Store" of metadata acquired under section 215 using U.S. Persons identifiers for foreign intelligence purposes?**
>
> The section 215 program is specifically authorized by orders issued by the Foreign Intelligence Surveillance Court pursuant to relevant statutory requirements. (Note: the legality of the program has been reviewed and approved by more than a dozen FISC judges on over 35 occasions since 2006.) As further required by statute, the program is also governed by minimization procedures adopted by the Attorney General an d approved by the FISC. Those orders, and

> the accompanying minimization procedures, require that searches of data under the program may only be performed when there is a Reasonable Articulable Suspicion that the identifier to be queried is associated with a terrorist organization specified in the Court's order.

Remember, not only do declassified Primary Orders make it clear NSA doesn't need Reasonable Articulable Suspicion to search the corporate store, but PCLOB has explained the possible breadth of "corporate store" searches plainly.

> According to the FISA court's orders, records that have been moved into the corporate store may be searched by authorized personnel "for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms."71 Analysts therefore can query the records in the corporate store with terms that are not reasonably suspected of association with terrorism. They also are permitted to analyze records in the corporate store through means other than individual contact-chaining queries that begin with a single selection term: because the records in the corporate store all stem from RAS-approved queries, the agency is allowed to apply other analytic methods and techniques to the query results.72 For instance, such calling records may be integrated with data acquired under other authorities for further analysis. The FISA court's orders expressly state that the NSA may apply "the full range" of signals intelligence analytic tradecraft to the calling records that are responsive to a query, which includes every record in the corporate store.73

There is no debate over whether NSA can conduct

back door searches in the "corporate store" because both FISC and PCLOB say they can.

Which is probably why SASC did not ask **whether** this was possible — it is an unclassified fact that it is — but rather what the legal rationale for doing so is.

And Rogers chose to answer this way:

1. By asserting that the phone dragnet must comply with statutory requirements
2. By repeating tired boilerplate about how many judges have approved this program (ignoring that almost all of these approvals came before FISC wrote its first legal opinion on the program)
3. By pointing to AG-approved minimization procedures (note—it's not actually clear that NSA's — as distinct from FBI's — dragnet specific procedures are AG-approved, though the more general USSID 18 ones are)
4. By claiming FISA orders and minimization procedures "require that searches of data under the program may only be performed when there is a Reasonable Articulable Suspicion that the identifier to be queried is associated with a terrorist organization"

The last part of this answer is either downright ignorant (though I find that unlikely given how closely nominee responses get vetted) or plainly non-responsive. The question was not about queries of the dragnet itself – the "collection store" of all the data. The question was about the "corporate store" – the database of query results based off those RAS approved identifiers. And, as I said, there is no dispute that searches of the corporate store do not require RAS approval. In fact, the FISC orders Rogers points to say as much explicitly.

And yet the man Obama has picked to replace Keith Alexander, who has so badly discredited the Agency with his parade of lies, refused to answer that question directly. Much less explain the legal rationale used to conduct RAS-free searches on phone query results showing 3rd degree connections to someone who might have ties to terrorist groups, which is what the question was.

Which, I suppose, tells us all we need to know about whether anyone plans to improve the credibility or transparency of the NSA.