CONNING THE RECORD, CONNING THE COURTS, DEFRAUDING THE PEOPLE

In the parlance of the once and forever MTV set, civil libertarians just had one of the "Best Weeks Ever". Here is the ACLU's Catherine Crump weighing in on the surprising results of President Obama's Review Board:

> Friday, the president's expressed willingness to consider ending the NSA's collection of phone records, saying, "The question we're going to have to ask is, can we accomplish the same goals that this program is intended to accomplish in ways that give the public more confidence that in fact the NSA is doing what it's supposed to be doing?"
>
> With this comment and the panel's report coming on the heels of Monday's remarkable federal court ruling that the bulk collection of telephone records is likely unconstitutional, this has been the best week in a long time for Americans' privacy rights.

That "federal court ruling" is, of course, that of Judge Richard Leon handed down a mere five days ago on Monday. Catherine is right, it has been a hell of a good week.

But lest we grow too enamored of our still vaporous success, keep in mind Judge Leon's decision, as right on the merits as it may be, and is, is still a rather adventurous and activist decision for a District level judge, and will almost certainly be pared back to some extent on appeal, even if some substantive parts of it are upheld. We shall see.

But the other cold water thrown came from Obama

himself when he gave a slippery and disingenuous press conference Friday. Here is the New York Times this morning capturing spot on the worthless lip service Barack Obama gave surveillance reform yesterday:

> By the time President Obama gave his news conference on Friday, there was really only one course to take on surveillance policy from an ethical, moral, constitutional and even political point of view. And that was to embrace the recommendations of his handpicked panel on government spying — and bills pending in Congress — to end the obvious excesses. He could have started by suspending the constitutionally questionable (and evidently pointless) collection of data on every phone call and email that Americans make.
>
> He did not do any of that.
> ….
> He kept returning to the idea that he might be willing to do more, but only to reassure the public "in light of the disclosures that have taken place."
>
> In other words, he never intended to make the changes that his panel, many lawmakers and others, including this page, have advocated to correct the flaws in the government's surveillance policy had they not been revealed by Edward Snowden's leaks.
>
> And that is why any actions that Mr. Obama may announce next month would certainly not be adequate. Congress has to rewrite the relevant passage in the Patriot Act that George W. Bush and then Mr. Obama claimed — in secret — as the justification for the data vacuuming.

Precisely. The NYT comes out and calls the dog a dog. If you read between the lines of this Ken Dilanian report at the LA Times, you get the

same preview of the nothingburger President Obama is cooking up over the holidays. As Ken more directly said in his tweet, “Obama poised to reject panel proposals on 702 and national security letters.” Yes, indeed, count on it.

Which brings us to that which begets the title of this post: I Con The Record has made a Saturday before Christmas news dump. And a rather significant one to boot. Apparently because they were too cowardly to even do it in a Friday news dump. Which is par for the course of the Obama Administration, James Clapper and the American Intel Shop. Their raison de’etre appears to be keep America uninformed, terrorized and supplicant to their power grabs. Only a big time operator like Big Bad Terror Voodoo Daddy Clapper can keep us chilluns safe!

So, the dump today is HERE in all its glory. From the PR portion of the “I Con” Tumblr post, they start off with Bush/Cheney Administration starting the “bulk” dragnet on October 4, 2001. Bet that is when it first was formalized, but the actual genesis was oh, maybe, September 12 or so. Remember, there were security daddies agitating for this long before September 11th.

Then the handcrafted Intel spin goes on to say this:

> Over time, the presidentially-authorized activities transitioned to the authority of the Foreign Intelligence Surveillance Act (“FISA”). The collection of communications content pursuant to presidential authorization ended in January 2007 when the U.S. Government transitioned the TSP to the authority of the FISA and under the orders of the Foreign Intelligence Surveillance Court (“FISC”). In August 2007, Congress enacted the Protect America Act (“PAA”) as a temporary measure. The PAA, which expired in February 2008, was replaced by the FISA Amendments Act of 2008, which was enacted in July 2008 and remains in effect. Today, content

> collection is conducted pursuant to section 702 of FISA. The metadata activities also were transitioned to orders of the FISC. The bulk collection of telephony metadata transitioned to the authority of the FISA in May 2006 and is collected pursuant to section 501 of FISA. The bulk collection of Internet metadata was transitioned to the authority of the FISA in July 2004 and was collected pursuant to section 402 of FISA. In December 2011, the U.S. Government decided to not seek reauthorization of the bulk collection of Internet metadata.
>
> After President Bush acknowledged the TSP in December 2005, two still-pending suits were filed in the Northern District of California against the United States and U.S. Government officials challenging alleged NSA activities authorized by President Bush after 9/11. In response the U.S. Government, through classified and unclassified declarations by the DNI and NSA, asserted the state secrets privilege and the DNI's authority under the National Security Act to protect intelligence sources and methods. Following the unauthorized and unlawful release of classified information about the Section 215 and Section 702 programs in June 2013, the Court directed the U.S. Government to explain the impact of declassification decisions since June 2013 on the national security issues in the case, as reflected in the U.S. Government's state secrets privilege assertion. The Court also ordered the U.S. Government to review for declassification all prior classified state secrets privilege and sources and methods declarations in the litigation, and to file redacted, unclassified versions of those documents with the Court.

This is merely an antiseptic version of the timeline of lies that has been relentlessly exposed by Marcy Wheeler right here on this blog, among other places. What is not included in the antiseptic, sandpapered spin is that the program was untethered from law completely and then "transitioned" to FISC after being exposed as such.

Oh, and lest anybody think this sudden disclosure today is out of the goodness of Clapper and Obama's hearts, it is not. As Trevor Timm of EFF notes, most all of the "I Con" releases have been made only after being forced to by relevant FOIA and other court victories and that this one in particular is mostly germinated by EFF's court order (and Vaughn index) obtained.

So, with that, behold the "I Con" release of ten different declarations previously filed and extant under seal in the *Jewel* and *Shubert* cases. Much of the language in all is similar template affidavit language, which you expect from such filings if you have ever dealt with them. As for individual dissection, I will leave that for later and for discussion by all in comments.

The one common theme that I can discern from a scan of a couple of note is that there is no reason in the world minimally redacted versions such as these could not have been made public from the outset. No reason save for the conclusion that to do so would have been embarrassing to the Article II Executive Branch and would have lent credence to American citizens properly trying to exercise and protect their rights in the face of a lawless and constitutionally infirm assault by their own government. The declarations by Mike McConnell, James Clapper, Keith Alexander, Dennis Blair, Frances Fleisch and Deborah Bonanni display a level of too cute by a half duplicity that ought be grounds for sanctions.

The record has been conned. Our federal courts have been conned. All as the Snowden disclosures

have proven. And the American people have been defrauded by pompous terror mongers who value their own and institutional power over truth and honesty to those they serve. Clapper, Alexander and Obama have the temerity to call Ed Snowden a traitor? Please, look in the mirror boys.

Lastly, and again as Trevor Timm pointed out above, these are just the declarations for cases the EFF and others are still pursuing. What of the false secret declarations made in *al-Haramain v. Obama*, which the government long ago admitted were bogus? Why won't the cons behind "I Con" release those declarations? What about the frauds perpetrated in *Mohamed v. Jeppesen* that have fraudulently ingrained states secrets cons into the government arsenal?

If the government wants to come clean, here is the opportunity. Frauds have been perpetrated on our courts, in our name. We should hear about that. Unless, of course, Obama and the "I Cons" are really nothing more than simple good old fashioned cons.

[By the way, Christmas is a giving season. If you have extra cheer to spread, our friends like Cindy Cohn, Trevor Timm, Hanni Fakhoury and Kurt Opsahl et al at EFF, and Ben Wizner, Alex Abdo, Catherine Crump et al at the ACLU all do remarkable work. Share your tax deductible love with them this season if you can. They make us all better off.]

THE NSA REVIEW GROUP'S NON-DENIAL DENIAL ON ENCRYPTION

As part of a section on "Technical Measures to Increase Security and User Confidence," Recommendation 29 of the NSA Review Group is, in part, the following:

> We recommend that, regarding encryption, the US Government should:
>
> (1) fully support and not undermine efforts to create encryption standards;
>
> (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software;

Several paragraphs into this section, the Group with no tech experts asserts,

> Upon review, however, we are unaware of any vulnerability created by the US Government in generally available commercial software that puts users at risk of criminal hackers or foreign governments decrypting their data. Moreover, it appears that in the vast majority of generally used, commercially available encryption software, there is no vulnerability, or "backdoor," that makes it possible for the US Government or anyone else to achieve unauthorized access.

This appears to be based on an Appendix provided by NSA addressing the reliability of certain encryption systems. I'm not competent to assess the claims or comprehensiveness of that presentation and eagerly await some reviews of this report from the tech experts. [Update: William Ockham notes the Appendix doesn't include the standard NSA is accused of weakening.]

The very next paragraph, with bullet points, reads,

> Nonetheless, it is important to take strong steps to enhance trust in this basic underpinning of information technology. Recommendation 32 is designed to describe those steps. The central point is that trust in encryption standards, and in the

> resulting software, must be maintained. Although NSA has made clear that it has not and is not now doing the activities listed below, the US Government should make it clear that:
>
> - *NSA will not engineer vulnerabilities into the encryption algorithms that guard global commerce;*
> - *The United States will not provide competitive advantage to US firms by the provision to those corporations of industrial espionage;*
> - *NSA will not demand changes in any product by any vendor for the purpose of undermining the security or integrity of the product, or to ease NSA's clandestine collection of information by users of the product; and*
> - *NSA will not hold encrypted communication as a way to avoid retention limits.*

I consider myself a bit of an aficionado in NSA claims, and I can only think of one place where they've made even some of these claims, sort of: the obviously bogus talking points NSA sent home at Thanksgiving. That document made a similar caveated comment about industrial espionage and

assured that NSA will not demand changes by any vendor, noting it did not have the authority to do so. I pointed out some of the loopholes to those claims here.

I don't think they have said anything about engineering vulnerabilities into encryption standards; in any case, the allegation was that they inserted vulnerabilities into certain standards through persuasion, not engineering. Besides, ODNI General Counsel Robert Litt has stated explicitly (and not all that surprisingly) that cracking encryption is their job.

Finally, I don't think the NSA has ever addressed the fact that their minimization standards clearly allow them to keep encrypted communication forever. They like to lie about that one instead. To place in their mouth a claim that they won't do so to get around retention limits (particularly followed, as it is, by a recommendation for how not to do this) is thin comfort coming from an agency that considers encryption possible evidence of terrorism.

I doubt this assertion that NSA doesn't try to weaken encryption is fooling anyone. Indeed, it appears less than 30 pages after the Report states, in justifying moving Information Assurance out of NSA,

> When the offensive personnel find some way into a communications device, software system, or network, they may be reluctant to have a patch that blocks their own access.

So it's hard to treat this entire passage as anything else but the "strong step to enhance trust" they say is necessary within it.

The NSA Review Group makes worthwhile recommendations on a reorganization of NSA—the most aggressive one of which — to split the DIRNSA from the CyberCommand position — Obama already pre-empted. Moving Information Assurance

out of NSA would also create a champion for privacy, albeit a hopelessly weak one (they even state it should be moved to DHS, but Congress would never agree to do so).

But ultimately on this and some other cybersecurity related issues (including its toothless recommendation on Zero Days that immediately follows this section), the Report serves only to pretend the US doesn't engage in weakening security as part of its offensive attacks using the Internet.

Update: Oh, as to that Appendix that doesn't include the standard everyone has been worried about? Someone's just found a fatal bug in the standard.

> An advisory published Thursday warns that a "FIPS module" of the widely used OpenSSL library contained a "fatal bug" in its implementation of Dual EC_DRBG. Credible doubts about the trustworthiness of the deterministic random bit generator surfaced almost immediately after National Security Agency (NSA) officials shepherded it through an international standards body in 2006. In September, those fears were rekindled when *The New York Times* reported the algorithm may contain an NSA-engineered backdoor that makes it easier for government spies to decode encrypted communications.
>
> The fatal Dual EC_DRBG bug resides in the FIPS Object Module v2.0, an optional OpenSSL library used to build crypto apps that are certified by the US government's Federal Information Processing Standards. When using the module's implementation of Dual EC_DRBG, the application crashes and can't be recovered. That's an amazing discovery for an application that had to undergo countless hours of testing to be certified by the government of the world's most powerful country.

60 MINUTES BETTERS THEIR BENGHAZI DEBACLE: PIRATES AHOY! AND CHINESE GLOBAL SUICIDE BOMBERS

I will have more to say about tonight's 60 Minutes debacle.

But for now, let me make three points.

First, John Miller should never work in journalism again (he's reportedly prepping to run NYPD's intelligence shop, so he may not need to). There were numerous examples in tonight's 60 Minutes piece where even a mildly curious journalist would have asked follow-up questions. But given that Miller, who has an ODNI and FBI background, knows this stuff, his failure to ask obvious follow-up questions is proof this was not at all about journalism.

Of particular note that everyone is getting snookered on: Lying Keith Alexander said that NSA only listens to the phone calls of 60 US persons. When Miller sort of asked a follow-up, Alexander seemed to reiterate that this is NSA.

Of course, FBI formally owns the wiretapping of US persons in the US. So that 60 number may only be Americans we wiretap overseas. One of those follow-up questions that might have been useful.

Then there was the NSA's effort to show us what contact chaining looks like. As a threshold matter, they had subbed out all the real phone numbers with "555-1212" type numbers. Which means the computer was altered for TV.

Then, CBS showed an NSA analyst contact chaining

off pirates.

Yes, pirates!

Aside from opening up NSA to the claim that we're now all 3 degrees of Captain Hook, the pirate operation of course means the claims of the analyst only apply to EO 12333 collection (cause pirates are almost never US persons).

That is, we should assume it is completely meaningless as a demonstration of what the US phone dragnet is about.

Then there's the scary BIOS plot.

I'll need to go back and review this, but the jist of the scary claim at the heart of the report is that the NSA caught China planning a BIOS plot to shut down the global economy.

To.

Shut.

Down.

The.

Global.

Economy.

Of course, if that happened, it'd mean a goodly percentage of China's 1.3 billion people would go hungry, which would lead to unbelievable chaos in China, which would mean the collapse of the state in China, the one thing the Chinese elite want to prevent more than anything.

But the NSA wants us to believe that this was actually going to happen.

That China was effectively going to set off a global suicide bomb. Strap on the economy in a cyber-suicide vest and … KABOOOOOOOM!

And the NSA heroically thwarted that attack.

That's what they want us to believe and some people who call themselves reporters are reporting as fact.

“WE’RE NOT GOING TO LEAVE IT TO THE GUY WHO LIES TO CONGRESS WITH IMPUNITY ANYMORE”

The regular outlets for NSA leakers are presenting details of the recommendations the NSA Review Committee has given to President Obama (Gorman, Sanger). Curiously, Siobhan Gorman suggests that because the recommendations closely following the Leahy-Sensenbrenner bill, it bodes well for passage of that bill.

> The panel’s idea “aligns very closely” with a bill offered by House Judiciary Committee Chairman James Sensenbrenner (R., Wis.) and Senate Judiciary Chairman Patrick Leahy (D., Vt.), said one person familiar with the report, suggesting it could give ammunition to congressional efforts.

From what I’ve seen so far, I’m not sure that’s actually true. Moreover, that’s not how intelligence reform generally works. Rather, usually the executive adopts changes asked by Congress, thereby dissuading Congress from actually passing those changes into enforceable law. With Jim Sensenbrenner correctly calling Dianne Feinstein’s Fake FISA Fix “a joke” and growing number of co-sponsors for Sensenbrenner’s bill, I can imagine why the Executive would want to pre-empt actual law.

Significantly, the proposed recommendations don’t end the concept of a phone dragnet; they just move administration of it elsewhere — either a third party or the telecoms — equally prone for abuse. The Review Committee apparently

didn't review efficacy of these programs.

Besides, according to David Sanger, the proposals predictably focus more on Angela Merkel's privacy than the hundreds of millions of others whose privacy the NSA compromises.

> The advisory group is also expected to recommend that senior White House officials, including the president, directly review the list of foreign leaders whose communications are routinely monitored by the N.S.A. President Obama recently apologized to Chancellor Angela Merkel of Germany for the N.S.A.'s monitoring of her calls over the past decade, promising that the actions had been halted and would not resume. But he refused to make the same promise to the leaders of Mexico and Brazil.
>
> Administration officials say the White House has already taken over supervision of that program. "We're not leaving it to Jim Clapper anymore," said one official, referring to the director of national intelligence, who appears to have been the highest official to review the programs regularly.
>
> [snip]
>
> [National Security Council spokesperson Caitlin Hayden] added that the review was especially focused on "examining whether we have the appropriate posture when it comes to heads of state; how we coordinate with our closest allies and partners; and what further guiding principles or constraints might be appropriate for our efforts."

It's that James Clapper line that ought to be the tell, however: that folks within the Administration are boldly stating that James Clapper won't be able to run amok anymore.

The same James Clapper, of course, on whom the White House imposed no consequences for lying to Congressional overseers.

Which brings me to my favorite detail, from the NYT:

> One of the expected recommendations is that the White House conduct a regular review of those collection activities, the way covert action by the C.I.A. is reviewed annually.

Obama suggested last week he serves in no more than an advisory role for the Deep State, someone who can propose changes, but not someone who can order them. That an advisory committee has to tell the President that the NSA operates with less oversight than the CIA whose covert operations have systematically exceeded the claimed authority granted by the President says something.

I do fear this Review will pre-empt some of the most important legislative fixes.

But I also hope we'll finally see heightened distance between the Deep State and the Executive that is overdue for reining it in.

SHELDON WHITEHOUSE: WE CAN'T UNILATERALLY DISARM, EVEN TO KEEP AMERICA COMPETITIVE

I have to say, the Senate Judiciary Committee hearing on the dragnet was a bust.

Pat Leahy was fired up — and even blew off a

Keith Alexander attempt to liken the Internet to a library with stories of the library card he got when he was 4. While generally favoring the dragnet, Chuck Grassley at least asked decent questions. But because of a conflict with a briefing on the Iran deal, Al Franken was the only other Senator to show up for the first panel. And the government witnesses — Keith Alexander, Robert Litt, and James Cole — focused on the phone dragnet disclosed over 6 months ago, rather than newer disclosures like back door searches and the Internet dragnet, which moved overseas. Litt even suggested — in response to a question from Leahy — that they might still be able to conduct the dragnet if they could bamboozle the FISA Court on relevance, again (see Spencer on that). As a result, no one discussed the systemic legal abuses of the Internet dragnet or NSA's seeming attempt to evade oversight and data sharing limits by moving their dragnet overseas.

Things went downhill when Leahy left for the Iran briefing and Sheldon Whitehouse presided over the second panel, with the Computer & Communications Industry Association's Edward Black, CATO's Julian Sanchez, and Georgetown professor (and former DOJ official) Carrie Cordero. Sanchez hit some key points on the why Internet metadata is not actually like phone pen registers. Cordero acknowledged that metadata was very powerful but then asserted that the metadata of the phone-based relationships of every American was not.

And Black tried to make the case that the spying is killing America.

Or, more specifically, his industry's little but significant corner of America, the Internet. While only some of this was in his opening statement, Black made the case that the Internet plays a critical role in America's competitiveness.

> While these are critical issues, it is important that the Committee also concern itself with the fact that the

> behavior of the NSA, combined with the global environment in which this summer's revelations were released, may well pose an existential threat to the Internet as we know it today, and, consequently, to many vital U.S. interests, including the U.S. economy.
>
> [snip]
>
> The U.S. government has even taken notice. A recent comprehensive re- port from the U.S. International Trade Commission (ITC) noted, "digital trade continues to grow both in the U.S. economy and globally" and that a "further increase in digital trade is probable, with the U.S. in the lead." In fact, the re- port also shows, U.S. digital exports have exceeded imports and that surplus has continually widened since 2007.
>
> [snip]
>
> As a result, the economic security risks posed by NSA surveillance, and the international political reaction to it, should not be subjugated to traditional national security arguments, as our global competitiveness is essential to long-term American security. It is no accident that the o□fficial National Security Strategy of the United States includes increasing exports as a major component of our national defense strategy.

Then he laid out all the ways that NSA's spying has damaged that vital part of the American economy: by damaging trust, especially among non-American users not granted to the protections Americans purportedly get, and by raising suspicion of encryption.

Black then talked about the importance of the Internet to soft power. He spoke about this generally, but also focused on the way that NSA

spying was threatening America's dominant position in Internet governance, which (for better and worse, IMO) has made the Internet the medium of exchange it is.

> The U.S. government position of supporting the multi-stakeholder model of Internet governance has been compromised. We have heard increased calls for the ITU or the United Nations in general to seize Internet governance functions from organizations that are perceived to be too closely associated with the U.S. government, such as the Internet Corporation for Assigned Names and Numbers (ICANN).

And he pointed to proposals to alter the architecture of the Internet to minimize the preferential access the US currently has.

Let's be honest, Black is a lobbyist, and he's pitching his industry best as he can. I get that. Yet even still, he's not admitting that these governance and architecture issues really don't provide neutrality — though US stewardship may be the least-worst option, it provides the US a big advantage.

What Black hinted at (but couldn't say without freaking out foreign users even more) is that our stewardship of the Internet is not just one of the few bright spots in our economy, but also a keystone to our power internationally. And it gives us huge spying advantages (not everyone trying to erode our control of the Internet's international governance is being cynical — Edward Snowden has made it clear we have abused our position).

Which is why Whitehouse's response was so disingenuous. He badgered Black, interrupting him consistently. He asked him to compare our spying with that of totalitarian governments, which Black responded was an unfair comparison. And Whitehouse didn't let Black point out that American advantages actually do mean we spy more

than others, because we can.

Basically, Whitehouse suggested that, in the era of Big Data, if we didn't do as much spying as we could — and to hell with what it did to our preferential position on the Internet — it would amount to unilaterally disarming in the face of Chinese and Russian challenges.

> If we were to pass law that prevented us from operating in Big Data, would be unilaterally disarming.

Whitehouse followed this hubris up with several questions that Sanchez might have gladly answered but Black might have had less leeway to answer, such as whether a court had ever found these programs to be unconstitutional. (The answer is yes, John Bates found upstream collection to be unconstitutional, he found the Internet dragnet as conducted for 5 years to be illegal wiretapping, and in the Yahoo litigation in 2007, Yahoo never learned what the minimization procedures were, and therefore never had the opportunity to make the case.) Black suggested, correctly, I think, that Whitehouse's position meant we were just in an arms race to be the Biggest Brother.

I get it. Whitehouse is one of those who believe — like Keith Alexander (whose firing Whitehouse has bizarrely not demanded, given his stated concerns about the failure to protect our data during Alexander's tenure) that the Chinese are plundering the US like a colony.

Not only does this stance seem to evince no awareness of how America used data theft to build itself as a country (and how America's hardline IP stance will kill people, making America more enemies). But it ignores the role of the Internet in jobs and competition and trade in ideas and goods.

Sheldon Whitehouse, from a state suffering economically almost as much as Michigan, seems anxious to piss away what competitive advantages non-defense America has to conduct spying that

hasn't really produced results (and has made our networks less secure as a result – precisely the problem Whitehouse claims to be so concerned about). That's an ugly kind of American hubris that doesn't serve this country, even if you adopt the most jingoistic nationalism imaginable.

He should know better than this. But in today's hearing, he seemed intent on silencing the Internet industry so he didn't learn better.

Update: Fixed the Black quotation.

Update: Jack Goldsmith pushes back against the American double standards on spying and stealing here.

WHEN SUSAN RICE IS RIGHT, SHE'S RIGHT!

From the No Kidding Files, courtesy of Jason Leopold, comes this gem from vaunted National Security Advisor Susan Rice:

> "Let's be honest: at times we do business with govts that do not respect the rights we hold most dear"

Well, hello there Susan, I couldn't agree more. Especially on days when I see things like this from the ~~Glenn Greenwald and Pierre Omidyar Snowden file monopoly~~ err, Barton Gellman at the Washington Post:

> The National Security Agency is

> gathering nearly 5 billion records a day on the whereabouts of cellphones around the world, according to top-secret documents and interviews with U.S. intelligence officials, enabling the agency to track the movements of individuals — and map their relationships — in ways that would have been previously unimaginable.
> ….
> The number of Americans whose locations are tracked as part of the NSA's collection of data overseas is impossible to determine from the Snowden documents alone, and senior intelligence officials declined to offer an estimate. "It's awkward for us to try to provide any specific numbers," one intelligence official said in a telephone interview. An NSA spokeswoman who took part in the call cut in to say the agency has no way to calculate such a figure.

It is thoroughly loathsome that Americans must do business with a government that does this, and insane that it is their own government.

It is "awkward" to determine how many innocent Americans are rolled up in the latest out of control security state dragnet the United States government is running globally. Actually, that is not awkward, it is damning and telling. Therefore the American citizenry must not know, at any cost.

Susan Rice is quite right, we are forced to "do business" with a government that does "not respect the rights we hold most dear"

[Here is the full text of the Susan Rice speech today that the above quote was taken from. It is a great speech, or would be if the morals of the United States under Barack Obama matched the lofty rhetoric]

INFORMATION MONOPOLY DEFINES THE DEEP STATE

The last decade witnessed the rise of deep state – an entity not clearly delineated that ultimately controls the military-industrial complex, establishing its own operational policy and practice outside the view of the public in order to maintain its control.

Citizens believe that the state is what they see, the evidence of their government at work. It's the physical presence of their elected representatives, the functions of the executive office, the infrastructure that supports both the electoral process and the resulting machinery serving the public at the other end of the sausage factory of democracy. We the people put fodder in, we get altered fodder out – it looks like a democracy.

But deep state is not readily visible; it's not elected, it persists beyond any elected official's term of office. While a case could be made for other origins, it appears to be born of intelligence and security efforts organized under the Eisenhower administration in response to new global conditions after World War II. Its function may originally have been to sustain the United States of America through any threat or catastrophe, to insure the country's continued existence.

Yet the deep state and its aims may no longer be

in sync with the United States as the people believe their country to be – a democratic society. The democratically elected government does not appear to have control over its security apparatus. This machinery answers instead to the unseen deep state and serves its goals.

As citizens we believe the Department of State and the Department of Defense along with all their subset functions exist to conduct peaceful relations with other nation-states while protecting our own nation-state in the process. Activities like espionage for discrete intelligence gathering are as important as diplomatic negotiations to these ends. The legitimate use of military force is in the monopolistic control of both Departments of State and Defense, defining the existence of a state according to philosopher Max Weber.

The existing security apparatus, though, does not appear to function in this fashion. It refuses to answer questions put to it by our elected representatives when it doesn't lie to them outright. It manages and manipulates the conditions under which it operates through implicit threats. The legitimacy of the military force it yields is questionable because it cannot be restrained by the country's democratic processes and may subvert control over military functions.

Further, it appears to answer to some other entity altogether. Why does the security apparatus pursue the collection of all information, in spite of such activities disrupting the ability of both State and Defense Departments to operate effectively? Why does it take both individuals' and businesses' communications while breaching their systems, in direct contravention to the Constitution's Fourth Amendment prohibition against illegal search and seizure?

What we have seen instead is a new facet of deep state manifest as a corollary to Weber's definition of state.

According to Weber, an entity is *“a ‘state’ if and insofar as its administrative staff successfully upholds a claim on the ‘monopoly of the legitimate use of physical force’ in the enforcement of its order.”*

Deep state as we currently understand it, however, appears to claim a different monopoly. It is not content with tightly focused actionable intelligence. It seeks collection and control of all information. Whether this effort is legitimate or not does not concern it as it is outside the definition of the state; existing outside any state entity and oversight by the Constitution, the Bill of Rights, any subsequent law, the deep state is extralegal, beyond legitimacy.

It is not merely extralegal but illegitimate, though, when it works in contravention to the stated goals of the state. It becomes a parasite sucking away citizens’ resources without adding value in return to the state.

Based on all the documentation we have seen both before Snowden and after Snowden, deep state has systematically planned, developed, and implemented information collection systems. What looked like one-off wiretaps here and there has become a digital hydra. One head is lopped off as it is revealed in court or by leaks, and a multitude of others emerge to take its place, more virulent than the avatar it augments.

Room 641A in San Francisco seems like a minor annoyance compared to the likelihood that entire transoceanic cables have been spliced and mirrored, the communications in the pipeline duplicated and stored.

The information gathering does not serve the direct interests of the state, in order for the state to wield its legitimate force. The Boston bombing is a perfect example of terrorism that should have been identified and revealed to the state in adequate time to protect the public — yet the state could not and did not respond due to its blindness to information which would have

revealed the plot’s existence.

Information gathering serves purposes that do not benefit the public but businesses. The materials gathered by spying on Brazilian government officials did not help the American people but a very narrow range of business interests, specifically the petroleum industry. This calls into question not only the legitimacy of the deep state’s information gathering, but the clients or masters to whom deep state answers. Who or what benefits from this kind of information?

The deep state influences the accrual and control of information in other spheres, through coercive fear, gestated uncertainty, and manipulated doubt. Lawmakers and members of the executive office act in ways that are unpredictable, ridiculous, obscure, and ultimately to the benefit of the deep state’s growing grasp and control of information; their efforts are impacted by misleading testimony, incomplete records, and redacted reports when they are not acting out of fear of being compromised by the security apparatus itself.

Former VP Dick Cheney’s fight to protect the information he allegedly gathered for Energy Task Force represents the point at which the deep state intersected with the Executive Office, using the executive office’s powers to build a firewall behind which it could obtain authority and resources, and legal precedent through which it could act with impunity. As long as deep state functions are carried out as a necessary part of the executive’s deliberation, it feels protected and empowered to carry out its aims.

The executive office further assures deep state’s continued information monopoly by appointing to the judiciary those who tend to side with the state on First- and Fourth Amendment-related cases.

In the pursuit and prosecution of Aaron Swartz for tapping into and sharing publicly-funded

research inside the pay-walled garden JSTOR, we see the executive acting to protect inadequately defined intellectual property interests. It is unclear to the public who benefited from the prosecution, but Swartz and the public did not gain access to the intellectual properties they had paid for through tax dollars supporting public universities' research or public grants that directly funded research. Activists who may have considered liberating the publicly-funded research are surely reluctant to pursue this at risk of being hounded to death as Swartz was.

MPAA's and RIAA's combined efforts to limit flow of intellectual property through manipulation of lawmakers and the executive office ensures that the entertainment industry is protected, while offering the deep state an excuse to trawl through information moving between and within states. It is in the interest of deep state's monopolistic aims for MPAA and RIAA to press for even more control of copyrighted materials.

And now without adequate open discussion among elected representatives, the Trans-Pacific Partnership may expand the reach of the American component of deep state – assuming that the entity is no longer united with a single government – intended to assure the free flow of information across the widest stretch of the earth, from the fastest growing economies. This is not merely the manifestation of the knowledge economy or the information superhighway; the control and trade of information is the source of power.

At some point individuals as well as what remains of the state they have elected need to address the rights of information creators. The open source community maxim, Information Wants To Be Free, should be examined and considered more carefully; as deep state continues its march toward monopolistic control of information without the consent of information creators, what does "free" really mean?

STUXNET AND THE POISONS THAT OPEN YOUR EYES

Playwright August Strindberg wrote, "*…There are poisons that blind you, and poisons that open your eyes.*"

We've been blinded for decades by complacency and stupidity, as well as our trust. Most Americans still naively believe that our government acts responsibly and effectively as a whole (though not necessarily its individual parts).

By effectively, I mean Americans believed their government would not deliberately launch a military attack that could affect civilians – including Americans – as collateral damage. Such a toll would be minimized substantively. Yesterday's celebration related to the P5+1 interim agreement regarding Iran's nuclear development program will lull most Americans into deeper complacency. The existing system worked, right?

But U.S. cyber warfare to date proves otherwise. The government has chosen to deliberately poison the digital waters so that all are contaminated, far beyond the intended initial target.

There's very little chance of escaping the poison, either. The ubiquity of U.S. standards in hardware and software technology has ensured this. The entire framework – the stack of computing and communications from network to

user applications – has been affected.

- Network: Communications pathways have been tapped, either to obtain specific content, or obtain a mirror copy of all content traveling through it. It matters not whether telecom network, or internal enterprise networks.

- Security Layer: Gatekeeping encryption has been undermined by backdoors and weakened standards, as well as security certificates offering handshake validation between systems.

- Operating Systems: Backdoors have been obtained, knowingly or unknowingly on the part of OS developers, using vulnerabilities and design flaws. Not even Linux can be trusted at this point (Linux progenitor Linus Torvalds has not been smart enough to offer a dead man's switch notification.)

- User Applications: Malware has embedded itself in applications, knowingly or unknowingly on the part of app developers.

End-to-end, top-to-bottom and back again, everything digital has been touched in one layer of the framework or another, under the guise of defending us against terrorism and cyber warfare.

Further, the government watchdogs entrusted to prevent or repair damage have become part and parcel of the problem, in such a way that they cannot effectively be seen to defend the public's interests, whether those of individual citizens or corporations. The National Institute of Standards and Technology has overseen the establishment and implementation of weak encryption standards for example; it has also taken testimony [PDF] from computing and communications framework hardware and software providers, in essence hearing where the continued weak spots will be for future compromise.

The fox is watching the hen house, in other

words, asking for testimony pointing out the weakest patches installed on the hen house door.

The dispersion of cyber poison was restricted only in the most cursory fashion.

- Stuxnet's key target appears to have been Iran's Natanz nuclear facility, aiming at its SCADA equipment, but it spread far beyond and into the private sector as disclosed by Chevron. The only protection against it is the specificity of its end target, rendering the rest of the malware injected but inert. It's still out there.

- Duqu, a "sibling" cyber weapon, was intended for widespread distribution, its aims two-fold. It delivered attack payload capability, but it also delivered espionage capability.

- Ditto for Flame, yet another "sibling" cyber weapon, likewise intended for widespread distribution, with attack payload and espionage capability.

There could be more than these, waiting yet to be discovered.

In the case of both Duqu and Flame, there is a command-and-control network of servers still in operation, still communicating with instances of these two malware cyber weapons. The servers' locations are global – yet another indicator of the planners'/developers' intention that these weapons be dispersed widely.

Poison everything, everywhere.

But our eyes are open now. We can see the poisoners fingerprints on the work they've done, and the work they intend to do.

After their poison effectively damaged the viability of Natanz uranium refinement program, they will claim victory with the Iranian agreement on nuclear proliferation – yet at what long term price? Not unlike the early treatments for syphilis requiring the patient's exposure to mercury, those who stood by as therapists and

visitors must have been exposed on a limited basis to the chemical neurotoxin, collaterally damaged.

Likewise, Stuxnet's collateral damage remains, a toxic cure waiting to realize maximum potency on targets which were not the primary focus of Stuxnet's first and second deployments.

Code lies waiting for a patch or update to refresh it, ready to be relaunched for aims that may not serve the original planners. Holes remain open, serving as doors for some other entity's purposes — perhaps another nation-state's hostile attack, perhaps a criminal smash-and-grab, or a massive extortion attempt.

Not to mention the loss of trust among global partners whose civilian technology has been put at risk at scale undetermined, for a period of time unclear.

Or worse: whoever ordered, planned, and wrote the Stuxnet family of cyber warfare weapons wanted assurance that any other attempts to subvert their will could be dealt with in the same fashion that Stuxnet damaged Iran. There is no trust, just hegemonic cyber power. There is only a technological poison waiting for the day when its manufacturer decides to re-arm the toxic payload — a cyber weapon held to the heads of every nation-state, every corporation, every individual who relies on the existing, compromised computing and communications framework.

If Iran was successfully cowed by systematic damage to its nuclear development program and more, how easily will other nation-states be pressured into compliance with but a bit of fresh cyber poison? Will the next deployment be restrained as the second wave of Stuxnet, or will it be as ruthless as Stuxnet's earlier evil twin was intended to be?

Open your eyes.

NSA DENIES THEIR EXISTING DOMESTIC CYBERDEFENSIVE EFFORTS, AGAIN

James Risen and Laura Poitras have teamed up to analyze a 4-year plan the NSA wrote in 2012, in the wake of being told its collection of some US person content in the US was illegal. I'll discuss the document itself in more depth later. But for the moment I want to look at the denials anonymous senior intelligence officials (SIOs) gave Risen and Poitras about their domestic cyberdefensive efforts.

As a reminder, since before 2008, the government has been collecting bulk Internet data from switches located in the US by searching on selectors in the content. Some of that collection searches on identifiers of people (for example, searching for people sharing Anwar al-Awlaki's email in the body of a message). But the collection also searches on other identifiers not tied to people. This collection almost certainly includes code, in an effort to find malware and other signs of cyberattacks.

We know that's true, in part, because the Leahy-Sensenbrenner bill not only restricts that bulk domestic collection to actually targeted people, but also because it limits such collection only to terrorism and counterproliferation, thereby silently prohibiting its use for cybersecurity. The bill gives NSA 6 months to stop doing these two things — collecting non-person selectors and doing so for cybersecurity — so it's clear such collection is currently going on.

So in 2012, just months after John Bates told NSA that when it collected domestic communications using such searches, it was

violating the Constitution (the NSA contemplated appealing that decision), the NSA said (among other things),

> The interpretation and guidelines for applying our authorities, and in some cases the authorities themselves, have not kept pace with the complexity of the technology and target environments, or the operational expectations levied on NSA's mission.

The document then laid out a plan to expand its involvement in cybersecurity, citing such goals as,

> Integrate the SIGINT system into a national network of sensors which interactively sense, respond, and alert one another at machine speed

Cyberdefense and offense are not the only goals mapped out in this document. Much of it is geared towards cryptanalysis, which is crucial for many targets. But it only mentions "non-state actors" once (and does not mention terrorists specifically at all) amid a much heavier focus on cyberattacks and after a description of power moving from West to East (that is, to China).

Which is why the SIO denials to Risen and Poitras ring so hollow.

When asked what authorities haven't kept up with their programs, the SIOs cite the roamer problem (and flat out lie about the current state of the law).

> Senior intelligence officials, responding to questions about the document, said that the N.S.A. believed that legal impediments limited its ability to conduct surveillance of terrorism suspects inside the United States. Despite an overhaul of national security law in 2008, the officials

> said, if a terrorism suspect who is under surveillance overseas enters the United States, the agency has to stop monitoring him until it obtains a warrant from the Foreign Intelligence Surveillance Court.

Remember, first of all, that NSA's own internal documents (from 2012, in fact) claim this problem stems from the number of Chinese targets traveling to the US, not terrorists. Moreover, NSA can already continue surveilling targets when they come in the US, but has to get emergency authorization to do so. This new bid for authority must stem from NSA not tracking these targets closely enough to realize they're in the US for 72 hours, and not wanting to involve the FISC for a time. But the NSA does not currently have to stop monitoring them until they get a warrant — that claim is simply false.

But clearly, the roamer problem is not the most pressing issue at hand (which Keith Alexander admits, on the record, with more captive NYT journalists). It's cybersecurity. And yet, the SIOs issuing obviously false denials to Risen and Poitras deny even that, as in this response to a question about the "sensors" comment above.

> Senior intelligence officials said that the system of sensors is designed to protect the computer networks of the Defense Department, and that the N.S.A. does not use data collected from Americans for the system.

The government currently has sensors at DOD and is negotiating to deploy them on critical infrastructure, but it wants sensors more broadly. And, as noted, it already partners with the telecoms to filter data searching for malicious code. Their programs already exceed their claims here, but they're still going to claim to the contrary nevertheless.

Most of the rest of the claims these SIOs made —

most denying that it collects or intends to collect data from within the US – ring equally hollow; many can be disproven with public documents. But that all makes sense. Because, whatever the targets, the document itself reveals a determination to increase the bulk collection and sorting approach. especially in the US.

Chalk this up to another example of NSA lying most unconvincingly when it tries to deny its illegal domestic wiretapping.

LAVABIT AND THE DEFINITION OF US GOVERNMENT HUBRIS

Well, you know, if you do not WANT the United States Government sniffing in your and your family's underwear, it is YOUR fault. Silly American citizens with your outdated stupid piece of paper you call the Constitution.

Really, get out if you are a citizen, or an American communication provider, that actually respects American citizen's rights. These trivialities the American ethos was founded on are "no longer operative" in the minds of the surveillance officers who claim to live to protect us.

Do not even think about trying to protect your private communications with something so anti-American as privacy enabling encryption like Lavabit which only weakly, at best, even deigned to supply.

Any encryption that is capable of protecting an American citizen's private communication (or even participating in the TOR network) is essentially inherently criminal and cause for potentially being designated a "selector", if

not target, of any number of searches, whether domestically controlled by the one sided ex-parte FISA Court, or hidden under Executive Order 12333, or done under foreign collection status and deemed “incidental”. Lavabit’s Ladar Levinson knows.

Which brings us to where we are today. Let Josh Gerstein set the stage:

> A former e-mail provider for National Security Agency leaker Edward Snowden, Lavabit LLC, filed a legal brief Thursday detailing the firm’s offers to provide information about what appear to have been Snowden’s communications as part of a last-ditch offer that prosecutors rejected as inadequate.
>
> The disagreement detailed in a brief filed Thursday with the U.S. Court of Appeals for the Fourth Circuit resulted in Lavabit turning over its encryption keys to the federal government and then shutting down the firm’s secure e-mail service altogether after viewing it as unacceptably tainted by the FBI’s possession of the keys.

I have a different take on the key language from Lavabit’s argument in their appellate brief though, here is mine:

> First, the government is bereft of any statutory authority to command the production of Lavabit’s private keys. The Pen Register Statute requires only that a company provide the government with technical assistance in the installation of a pen- trap device; providing encryption keys does not aid in the device’s installation at all, but rather in its use. Moreover, providing private keys is not “unobtrusive,” as the statute requires, and results in interference with Lavabit’s services, which the statute forbids. Nor does the

> Stored Communications Act authorize the government to seize a company's private keys. It permits seizure of the contents of an electronic communication (which private keys are not), or information pertaining to a subscriber (which private keys are also, by definition, not). And at any rate it does not authorize the government to impose undue burdens on the innocent target business, which the government's course of conduct here surely did.
>
> Second, the Fourth Amendment independently prohibited what the government did here. The Fourth Amendment requires a warrant to be founded on probable cause that a search will uncover fruits, instrumentalities, or evidence of a crime. But Lavabit's private keys are none of those things: they are lawful to possess and use, they were known only to Lavabit and never used by the company to commit a crime, and they do not prove that any crime occurred. In addition, the government's proposal to examine the correspondence of all of Lavabit's customers as it searched for information about its target was both beyond the scope of the probable cause it demonstrated and inconsistent with the Fourth Amendment's particularity requirement, and it completely undermines Lavabit's lawful business model. General rummaging through all of an innocent business' communications with all of its customers is at the very core of what the Fourth Amendment prohibits.

The legal niceties of Lavabit's arguments are thus:

> The Pen Register Statute does not come close. An anodyne mandate to provide information needed merely for the "unobtrusive installation" of a device

> will not do. If there is any doubt, this Court should construe the statute in light of the serious constitutional concerns discussed below, to give effect to the "principle of constitutional avoidance" that requires this Court to avoid constructions of statutes that raise colorable constitutional difficulties. Norfolk S. Ry. Co. v. City of Alexandria, 608 F.3d 150, 156–57 (4th Cir. 2010).

And, later in the pleading:

> By those lights, this is a very easy case. Lavabit's private keys are not connected with criminal activity in the slightest—the government has never accused Lavabit of being a co-conspirator, for example. The target of the government's investigation never had access to those private keys. Nor did anyone, in fact, other than Lavabit. Given that Lavabit is not suspected or accused of any crime, it is quite impossible for information known only to Lavabit to be evidence that a crime has occurred. The government will not introduce Lavabit's private keys in its case against its target, and it will not use Lavabit's private keys to impeach its target at trial. Lavabit's private keys are not the fruit of any crime, and no one has ever used them to commit any crime. Under those circumstances, absent any connection between the private keys and a crime, the "conclusion[] necessary to the issuance of the warrant" was totally absent. Zurcher, 436 U.S., at 557 n.6 (quoting, with approval, Comment, 28 U. Chi. L. Rev. 664, 687 (1961)).

What this boils down to is, essentially, the government thinks the keys to Lavabit's encryption for their customers belong not just

to Lavabit, and their respective customers, but to the United States government itself.

Your private information cannot be private in the face of the United States Government. Not just Edward Snowden, but anybody, and everybody, is theirs if they want it. That is the definition of bullshit.

[Okay, big thanks to Darth, who generously agreed to let us use the killer Strangelovian graphic above. Please follow Darth on Twitter]