1AC 3

Observation 1: Inherency 4

Thus the plan 6

Observation II: Solvency 7

Advantage 1 is the Economy 8

Advantage 2 is Surveillance 14

Case Extensions 18

Inherency Extensions 19

Surveillance Increasing 20

USA Freedom Act Doesn’t Solve 22

702 is Expanding 23

Solvency 24

FISA Reform Solves 702 25

Declassification Solves 25

Special Advocate Solves 25

Section 702 Bad 25

702 --> Loophole 25

702 X 4th Amendment 25

702 X Constitution 25

702 X Privacy 25

No Oversight 25

AT: NSA Limitations Check 25

Advantage 1 Extensions 25

702 🡪 Data Loalization 25

Surveillance 🡪 Data Localization 25

Data Localization X Growth 25

Data Localization X Trade 25

Data Localization X Tech 25

AT: Data Localization Good 25

Data Globalization 🡪 Growth 25

We Solve Data Localization 25

Debt Bad 25

Advantage 2 Extensions 25

Surveillance Bad-Democracy 25

Surveillance Bad-4th Amendment 25

Surveillance Bad-Terrorism 25

Surveillance Bad-Soft Power 25

Surveillance Bad-Social Control 25

Surveillance Bad-Laundry List 25

Surveillance Bad-Corporate Control 25

Surveillance Bad-Unpopular 25

Human Rights Impacts 25

Utah Data Center Add-On 25

2AC Utah Data Center Add-On 25

Utah Data Center is Expanding 25

Data Centers Bad-Surveillance 25

Data Centers Bad-Democracy 25

Data Centers Bad-Resources 25

Data Centers Bad-Water 25

Data Centers Bad-Privacy 25

Data Centers Bad-Economics 25

Data Centers Bad-General 25

Data Centers Bad-Cyber Security 25

Energy Use Bad 25

Global Warming Impact 25

Answers to Neg Stuff 25

AT: T-Domestic 25

AT: Terrorism DA 25

AT: TPP Ptx: 25

Case Neg 25

States CP 25

Extend: States CP Solvency 25

CP Solvency: Congress doesn’t enforce 25

Courts CP 25

AT: Cyber Terror 25

Digital Innocence Turn 25

AT: 4th Amendment 25

# 1AC

### Observation 1: Inherency

#### The recent passage of the USA Freedom Act weakened protections under section 702—it violates domestic and international human rights law, broadly expands federal surveillance powers, and threatens billions world wide.

Kayyali 14 (Nadia, JD, UC Hastings, Outreach Editor, Hastings Race and Poverty Law Journal, and Board Member, National Lawyers Guild San Francisco Bay Area, “The Way the NSA Uses Section 702 is Deeply Troubling. Here’s Why,” Electronic Frontiers Foundation Blog, May 8, https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why)

The most recent disclosure of classified NSA documents revealed that the British spy agency GCHQ sought unfettered access to NSA data collected under Section 702 of the FISA Amendments Act. Not only does this reveal that the two agencies have a far closer relationship than GCHQ would like to publicly admit, it also serves as a reminder that surveillance under Section 702 is a real problem that has barely been discussed, much less addressed, by Congress or the President.¶ In fact, the "manager’s amendment" to the USA FREEDOM Act, which passed unanimously out of the House Judiciary Committee, has weakened the minimal changes to Section 702 that USA FREEDOM originally offered. Although Representative Zoe Lofgren—who clearly understands the import of Section 702—offered several very good amendments that would have addressed these gaps, her amendments were all voted down. There’s still a chance though—as this bill moves through Congress it can be strengthened by amendments from the floor.¶ Section 702 has been used by the NSA to justify mass collection of phone calls and emails by collecting huge quantities of data directly from the physical infrastructure of communications providers. Here’s what you should know about the provision and why it needs to be addressed by Congress and the President: ¶ Most of the discussion around the NSA has focused on the phone records surveillance program. Unlike that program, collection done under Section 702 captures content of communications. This could include content in emails, instant messages, Facebook messages, web browsing history, and more. ¶ Even though it’s ostensibly used for foreign targets, Section 702 surveillance sweeps up the communications of Americans. The NSA has a twisted, and incredibly permissive, interpretation of targeting that includes communications about a target, even if the communicating parties are completely innocent. As John Oliver put it in his interview with former NSA General Keith Alexander: "No, the target is not the American people, but it seems that too often you miss the target and hit the person next to them going, 'Whoa, him!'"¶ The NSA has confirmed that it is searching Section 702 data to access American’s communications without a warrant, in what is being called the "back door search loophole." In response to questions from Senator Ron Wyden, former NSA director General Keith Alexander admitted that the NSA specifically searches Section 702 data using "U.S. person identifiers," for example email addresses associated with someone in the U.S.¶ The NSA has used Section 702 to justify programs in which the NSA can siphon off large portions of Internet traffic directly from the Internet backbone. These programs exploit the structure of the Internet, in which a significant amount of traffic from around the world flows through servers in the United States. In fact, through Section 702, the NSA has access to information stored by major Internet companies like Facebook and Google.¶ Section 702 is likely used for computer security operations. Director of National Intelligence James Clapper noted Section 702's use to obtain communications "regarding potential cyber threats" and to prevent "hostile cyber activities." Richard Ledgett, Deputy Director of NSA, noted the use of intelligence authorities to mitigate cyber attacks.¶ The FISA Court has little opportunity to review Section 702 collection. The court approves procedures for 702 collection for up to a year. This is not approval of specific targets, however; "court review [is] limited to 'procedures' for targeting and minimization rather than the actual seizure and searches." This lack of judicial oversight is far beyond the parameters of criminal justice.¶ Not only does the FISA Court provide little oversight, Congress is largely in the dark about Section 702 collection as well. NSA spying defenders say that Congress has been briefed on these programs. But other members of Congress have repeatedly noted that it is incredibly difficult to get answers from the intelligence community, and that attending classified hearings means being unable to share any information obtained at such hearings. What’s more, as Senator Barbara Mikulski stated: "'Fully briefed' doesn’t mean that we know what’s going on." Without a full picture of Section 702 surveillance, Congress simply cannot provide oversight.¶ Section 702 is not just about keeping us safe from terrorism. It’s a distressingly powerful surveillance tool. While the justification we’ve heard repeatedly is that NSA surveillance is keeping us safer, data collected under Section 702 can be shared in a variety of circumstances, such as ordinary criminal investigations. For example, the NSA has shared intelligence with the Drug Enforcement Agency that has led to prosecutions for drug crimes, all while concealing the source of the data.¶ The President has largely ignored Section 702. While the phone records surveillance program has received significant attention from President Obama, in his speeches and his most recent proposal, Section 702 remains nearly untouched.¶ The way the NSA uses Section 702 is illegal and unconstitutional—and it violates international human rights law. Unlike searches done under a search warrant authorized by a judge, Section 702 has been used by the NSA to get broad FISA court authorization for general search and seizure of huge swathes of communications. The NSA says this is OK because Section 702 targets foreign citizens. The problem is, once constitutionally protected communications of Americans are swept up, the NSA says these communications are “fair game” for its use.¶ Innocent non-Americans don't even get the limited and much abused protections the NSA promises for Americans. Under international human rights law to which the United States is a signatory, the United States must respect the rights of all persons. With so many people outside the United States keeping their data with American companies, and so much information being swept up through mass surveillance, that makes Section 702 the loophole for the NSA to violate the privacy rights of billions of Internet users worldwide.¶ The omission of Section 702 reform from the discourse around NSA surveillance is incredibly concerning, because this provision has been used to justify some of the most invasive NSA surveillance. That’s why EFF continues to push for real reform of NSA surveillance that includes an end to Section 702 collection. You can help by educating yourself and engaging your elected representatives. Print out our handy one-page explanation of Section 702. Contact your members of Congress today and tell them you want to see an end to all dragnet surveillance, not just bulk collection of phone records.

### Thus the plan

#### **The United States federal government should substantially curtail domestic surveillance by amending Section 702 of the FISA Amendment Act of 2008 to 1) extend Fourth Amendment protections to U.S.-title-held Corporations operating overseas or engaged in overseas communication and 2) requiring warrants for law enforcement queries under Section 702 for the purpose of criminal investigation of U.S. persons. Funding and enforcement will occur through normal means. We reserve the right to clarify intent.**

### Observation II: Solvency

#### The US should reform Section 702 by limiting foreign intelligence collection to counterterrorism and national security and requiring warrants for criminal investigations.

Granick 14 (Jennifer, Director of Civil Liberties at the Stanford Center for Internet and Society, “Reforming The Section 702 Dragnet (Part 1),” *Just Security,* January 30, 2014, http://justsecurity.org/6574/reforming-section-702-dragnet-1/)

Section 702 allows immense data to be collected, allows foreign rights violation, and cripples US business and democracy.¶ As Professor Christopher Sprigman and I argued in the New York Times, PRISM is designed to produce at least 51 percent confidence in a target’s “foreignness” — as John Oliver of “The Daily Show” put it, “a coin flip plus 1 percent.” We believe that the NSA intentionally designed PRISM so that it is a certainty it will regularly acquire information it is not allowed to have. Whether or not you agree with us or not that this is illegal, the fact remains that statistically the NSA is getting an immense amount of information it is not allowed to have, even under the terrifyingly broad auspices of section 702. That must be changed.¶ Another fundamental problem with section 702 is that it authorizes targeting and monitoring of average citizens of other countries for reasons that are not necessarily related to the security of the United States. Targets need only be non-U.S. persons, and communications which are not purely domestic are fair game. This disregard for other people’s privacy is a terrible idea. Not only does it violate international human rights principles, but—as Sprigman and I wrote back in June—it’s bad for American business and democracy. We can alleviate this problem through reintroducing some or all of the safeguards under traditional FISA, like limiting targets to foreign powers or agents of foreign powers, or limiting collection to facilities that the targets actually use. If we are going to continue to dragnet through foreigners’ communications with each other and with Americans, we might limit the categories of foreign intelligence information for which such a tool is used to counterterrorism and national security, and not for the mere conduct of foreign affairs or collection of economic information.¶ Good policy requires public awareness of how many Americans’ communications are swept up in section 702. We should be told that now, and the government should be obligated to do some kind of regular reporting.¶ The current proposal would allow “about” collection in terrorism contexts. But innocent people talk about terrorism all the time. We discuss and tell jokes about Osama bin Laden, we wonder about Yemen safe houses and Taliban oppression. We’ve seen no meaningful way that the government distinguishes between these healthy, private conversations, and obtaining meaningful intelligences. Until we do, we should consider completely prohibiting “about the target” collection.¶ Back door searches should require at least a Title III warrant. Outside of section 702, the government would not have access to this information concerning Americans without complying with the dictates of the Wiretap Act (or perhaps in some cases traditional FISA), and it should not be able to avoid those protections via a dragnet.¶ Similarly, we should consider under what conditions, if any, it is appropriate share communications obtained in a dragnet with the Internal Revenue Service, Drug Enforcement Agency, Alcohol, Tobacco and Firearms, or other law enforcement agencies. If and when such referrals are made, the subjects ought to be notified.¶ Minimization should at least meet the standard of traditional FISA if not better.¶ People who are incidentally or mistakenly collected on should be notified.¶ We need to make it easier to enforce surveillance limitations, for victims of violations to obtain judicial remedies, and for public courts to review the lawfulness of Executive Branch operations.¶ So far, there has been no robust investigations into the sketchy ways the NSA is implementing section 702 via PRISM and overbroad upstream collection. Nor have we had a good public debate about the dangers of section 702 and how to avoid them. Nor have we talked about the ways privacy is being decimated by the NSA’s overseas collection. Now is the time for the NSA to come clean about what it is doing. Now is the time to have those public conversations. And now is the time to think creatively about enforcing the laws we have implementing reforms to alleviate the problems we’ve learned about

### Advantage 1 is the Economy

#### First, surveillance like Section 702 costs the U.S. billions and drives investors out.

Schneier, 15 (Bruce (2015-03-02). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (p. 121-2). W. W. Norton & Company. Kindle Edition.)

Those of us who fought the crypto wars, as we call them, thought we had won them in the 1990s. What the Snowden documents have shown us is that instead of dropping the notion of getting backdoor government access, the NSA and FBI just kept doing it in secret. Now that this has become public, US companies are losing business overseas because their non-US customers don’t want their data collected by the US government. NSA surveillance is costing US companies business in three different ways: people fleeing US cloud providers, people not buying US computer and networking equipment, and people not trusting US¶ companies. When the story about the NSA’s getting user data directly from US cloud providers— the PRISM program— broke in 2013, businesses involved faced a severe public relations backlash. Almost immediately, articles appeared noting that US cloud companies were losing business and their counterparts in countries perceived as neutral, such as Switzerland, were gaining. One survey of British and Canadian companies from 2014 found that 25% of them were moving their data outside the US, even if it meant decreased performance. Another survey of companies found that NSA revelations made executives much more concerned about where their data was being stored. Estimates of how much business will be lost by US cloud providers vary. One 2013 study by the Information Technology and Innovation Foundation foresees the loss of revenue at $ 22 to $ 35 billion over three years; that’s 10% to 20% of US cloud providers’ foreign market share. The Internet analysis firm Forrester Research believes that’s low; it estimates three-year losses at $ 180 billion because some US companies will also move to foreign cloud providers. US computer and networking companies are also taking severe hits. Cisco reported 2013 fourth quarter revenue declines of 8% to 10%. AT& T also reported earnings losses, and had problems with its European expansion plans. IBM lost sales in China. So did Qualcomm. Verizon lost a large German government contract. There’s more. I have attended private meetings where large US software companies complained about significant loss of foreign sales. Cisco’s CEO John Chambers wrote to the Obama administration, saying that NSA’s hacking of US equipment “will undermine confidence in our industry and in the ability of technology companies to deliver products globally.” Chambers’s comments echo the third aspect of the competitiveness problem facing US companies in the wake of Snowden: they’re no longer trusted. The world now knows that US telcos give the NSA access to the Internet backbone and that US cloud providers give it access to user accounts. The world now knows that the NSA intercepts US-sold computer equipment in transit and surreptitiously installs monitoring hardware. The world knows that a secret court compels US companies to make themselves available for NSA eavesdropping, and then orders them to lie about it in public. Remember the Lavabit story from Chapter 5? All of this mistrust was exacerbated by the Obama administration’s repeated reassurances that only non-Americans were the focus of most of the NSA’s efforts. More than half of the revenue of many cloud companies comes from outside the US. Facebook’s Mark Zuckerberg said it best in a 2013 interview: “The government response was, ‘Oh don’t worry, we’re not spying on any Americans.’ Oh, wonderful: that’s really helpful to companies trying to serve people around the world, and that’s really going to inspire confidence in American internet companies.”

#### Second, that causes foreign investors to localize their data and pull out of U.S technology industries.

Castro 13 (Daniel, Vice President, Information Technology and Innovation Foundation “How Much Will PRISM Cost the U.S. Cloud Computing Industry?” *Information Technology and Innovation Foundation*, August 2013 http://www2.itif.org/2013-cloud-computing-costs.pdf)

The recent revelations about the extent to which the National Security Agency (NSA) and other U.S. law enforcement and national security agencies have used provisions in the Foreign Intelligence Surveillance Act (FISA) and USA PATRIOT Act to obtain electronic data from third- parties will likely have an immediate and lasting impact on the competitiveness of the U.S. cloud computing industry if foreign customers decide the risks of storing data with a U.S. company outweigh the benefits.¶ The United States has been the leader in providing cloud computing services not just domestically, but also abroad where it dominates every segment of the market. In the 2013 Informa Cloud World Global Insights survey, 71 percent of respondents (of which only 9 percent were from North America) ranked the United States as the leader in cloud computing usage and innovation.1 In this same survey, nine out of ten respondents linked cloud computing to their country’s economic competitiveness.¶ But other countries are trying to play catch-up to the United States’ early success. Of the $13.5 billion in investments that cloud computing service providers made in 2011, $5.6 billion came from companies outside North America.2 Even national governments are helping to bankroll these efforts to combat U.S. market leadership—France, for example, invested €135 million in a joint venture in cloud computing.3¶ At stake is a significant amount of revenue. As shown in figure 1, the global enterprise public cloud computing market will be a $207 billion industry by 2016.4 Europeans in particular are trying to edge out their American competitors, and they are enlisting their¶ ￼governments to help. Jean-Francois Audenard, the cloud security advisor to France Telecom, said with no small amount of nationalistic hyperbole, “It’s extremely important to have the governments of Europe take care of this issue because if all the data of enterprises were going to be under the control of the U.S., it’s not really good for the future of the European people.”5¶ ￼￼And governments have begun to respond. In a 2012 policy document titled “Unleashing the Potential of Cloud Computing in Europe,” the European Commission (EC) called for a number of steps to promote cloud computing adoption in Europe, including creating pan-European technical standards, EU-wide certification for cloud computing providers, and model contract language.7 The Europeans are quite frank about their intentions. The EC notes “this strategy is about building a new industry, and better competing against the United States in particular.”8 Gartner estimates that in Western Europe alone the cloud computing market will be $47 billion by 2015, and the EC estimates that European cloud computing providers stand to gain €80 billion in revenue by 2020.9¶ While much of this projected growth was until recently up for grabs by U.S. companies, the disclosures of the NSA’s electronic surveillance may fundamentally alter the market dynamics. Neelie Kroes, European Commissioner for Digital Affairs, stated the problem quite succinctly, “If European cloud customers cannot trust the United States government, then maybe they won't trust U.S. cloud providers either. If I am right, there are multibillion-euro consequences for American companies. If I were an American cloud provider, I would be quite frustrated with my government right now.”10¶ The impact of PRISM on U.S companies may be particularly acute because cloud computing is a rapidly growing industry. This means that cloud computing vendors not only have to retain existing customers, they must actively recruit new customers to retain¶ ￼￼market share. Global spending on cloud computing is expected to grow by as much as 100 percent between 2012 and 2016, whereas the global IT market will only grow by 3 percent.11 If U.S. companies lose market share in the short term, this will have long-term implications on their competitive advantage in this new industry.

#### Third, that’s really bad—data localization destroys growth: raises business costs, reduces access to services, swamps tech advances, and creates economic burdens in the trillions

Chander and Le 15 (Anupam, Dir California Intl Law Ctr and Prof of Law at UC Davis; and Uyen, Free Speech and Technology Fellow, California Intl Law Ctr, “Data Nationalism,” 64 Emory L.J. 677, L/N)

Many governments believe that by forcing companies to localize data within national borders, they will increase investment at home. Thus, data localization measures are often motivated, whether explicitly or not, by desires to promote local economic development. In fact, however, data localization raises costs for local businesses, reduces access to global services for consumers, hampers local start-ups, and interferes with the use of the latest technological advances.¶ In an Information Age, the global flow of data has become the lifeblood of economies across the world. While some in Europe have raised concerns about the transfer of data abroad, the European Commission has recognized "the critical importance of data flows notably for the transatlantic economy." n209 The Commission observes that international data transfers "form an integral part of commercial exchanges across the Atlantic including for new growing digital businesses, such as social media or cloud computing, with large amounts of data going from the EU to the US." n210 Worried about the effect of constraints on data flows on both global information sharing and economic development, the Organisation for Economic Co-operation and Development (OECD) has urged nations to avoid "barriers to the location, access and use of cross-border [\*722] data facilities and functions" when consistent with other fundamental rights, in order to "ensure cost effectiveness and other efficiencies." n211¶ The worry about the impact of data localization is widely shared in the business community as well. The value of the Internet to national economies has been widely noted. n212 Regarding Brazil's attempt to require data localization, the Information Technology Industry Council, an industry association representing more than forty major Internet companies, had argued that "in-country data storage requirements would detrimentally impact all economic activity that depends on data flows." n213 The Swedish government agency, the National Board of Trade, recently interviewed fifteen local companies of various sizes across sectors and concluded succinctly that "trade cannot happen without data being moved from one location to another." n214¶ Data localization, like most protectionist measures, leads only to small gains for a few local enterprises and workers, while causing significant harms spread across the entire economy. The domestic benefits of data localization go to the few owners and employees of data centers and the few companies servicing these centers locally. Meanwhile, the harms of data localization are widespread, felt by small, medium, and large businesses that are denied access to global services that might improve productivity. In response to Russia's recently passed localization law, the NGO Russian Association for Electronic Communications stressed the potential economic consequences, pointing to the withdrawal of global services and substantial economic losses caused by the passing of similar laws in other countries. n215 For example, besides the loss of international social media platforms, localization would make it impossible for [\*723] Russians to order airline tickets or consumer goods through online services. Localization requirements also seriously affect Russian companies like Aeroflot because the airline depends on foreign ticket-booking systems. n216¶ Critics worried, at the time, that the Brazilian data localization requirement would "deny[] Brazilian users access to great services that are provided by US and other international companies." n217 Marilia Marciel, a digital policy expert at Fundacao Getulio Vargas in Rio de Janeiro, observes, "Even Brazilian companies prefer to host their data outside of Brazil." n218 Data localization affects domestic innovation by denying entrepreneurs the ability to build on top of global services based abroad. Brasscom, the Brazilian Association of Information Technology and Communication Companies, argues that such obligations would "hurt[] the country's ability to create, innovate, create jobs and collect taxes from the proper use of the Internet." n219¶ Governments implementing in-country data mandates imagine that the various global services used in their country will now build infrastructure locally. Many services, however, will find it uneconomical and even too risky to establish local servers in certain territories. n220 Data centers are expensive, all the more so if they have the highest levels of security. One study finds Brazil to be the most expensive country in the Western hemisphere in which to build data centers. n221 Building a data center in Brazil costs $ 60.9 million on average, [\*724] while building one in Chile and the United States costs $ 51.2 million and $ 43 million, respectively. n222 Operating such a data center remains expensive because of enormous energy and other expenses - averaging $ 950,000 in Brazil, $ 710,000 in Chile, and $ 510,000 in the United States each month. n223 This cost discrepancy is mostly due to high electricity costs and heavy import taxes on the equipment needed for the center. n224 Data centers employ few workers, with energy making up three-quarters of the costs of operations. n225 According to the 2013 Data Centre Risk Index - a study of thirty countries on the risks affecting successful data center operations - Australia, Russia, China, Indonesia, India, and Brazil are among the riskiest countries for running data centers. n226¶ Not only are there significant economic costs to data localization, the potential gains are more limited than governments imagine. Data server farms are hardly significant generators of employment, populated instead by thousands of computers and few human beings. The significant initial outlay they require is largely in capital goods, the bulk of which is often imported into a country. The diesel generators, cooling systems, servers, and power supply devices tend to be imported from global suppliers. n227 Ironically, it is often American suppliers of servers and other hardware that stand to be the beneficiaries of data localization mandates. n228 One study notes, "Brazilian suppliers of components did not benefit from this [data localization requirement], since the imported products dominate the market." n229 By increasing capital purchases from abroad, data localization requirements can in fact increase merchandise trade deficits. Furthermore, large data farms are [\*725] enormous consumers of energy, n230 and thus often further burden overtaxed energy grids. They thereby harm other industries that must now compete for this energy, paying higher prices while potentially suffering limitations in supply of already scarce power.¶ Cost, as well as access to the latest innovations, drives many e-commerce enterprises in Indonesia to use foreign data centers. Daniel Tumiwa, head of the Indonesian E-Commerce Association (IdEA), states that "the cost can double easily in Indonesia." n231 Indonesia's Internet start-ups have accordingly often turned to foreign countries such as Australia, Singapore, or the United States to host their services. One report suggests that "many of the "tools' that start-up online media have relied on elsewhere are not fully available yet in Indonesia." n232 The same report also suggests that a weak local hosting infrastructure in Indonesia means that sites hosted locally experience delayed loading time. n233 Similarly, as the Vietnamese government attempts to foster entrepreneurship and innovation, n234 localization requirements effectively bar start-ups from utilizing cheap and powerful platforms abroad and potentially handicap Vietnam from "joining in the technology race." n235¶ Governments worried about transferring data abroad at the same time hope, somewhat contradictorily, to bring foreign data within their borders. Many countries seek to become leaders in providing data centers for companies operating across their regions. In 2010, Malaysia announced its Economic Transformation Program n236 to transform Malaysia into a world-class data [\*726] center hub for the Asia-Pacific region. n237 Brazil hopes to accomplish the same for Latin America, while France seeks to stimulate its economy via a "Made in France" digital industry. n238 Instead of spurring local investment, data localization can lead to the loss of investment. First, there's the retaliation effect. Would countries send data to Brazil if Brazil declares that data is unsafe if sent abroad? Brasscom notes that the Brazilian Internet industry's growth would be hampered if other countries engage in similar reactive policies, which "can stimulate the migration of datacenters based here, or at least part of them, to other countries." n239 Some in the European Union sympathize with this concern. European Commissioner for the Digital Agenda, Neelie Kroes, has expressed similar doubts, worrying about the results for European global competitiveness if each country has its own separate Internet. n240 Then there's the avoidance effect. Rio de Janeiro State University Law Professor Ronaldo Lemos, who helped write the original Marco Civil and is currently Director of the Rio Institute for Technology and Society, warns that the localization provision would have caused foreign companies to avoid the country altogether: "It could end up having the opposite effect to what is intended, and scare away companies that want to do business in Brazil." n241 Indeed, such burdensome local laws often lead companies to launch overseas, in order to try to avoid these rules entirely. Foreign companies, too, might well steer clear of the country in order to avoid entanglement with cumbersome rules. For example, Yahoo!, while very popular in Vietnam, places its servers for the [\*727] country in Singapore. n242 In these ways we see that data localization mandates can backfire entirely, leading to avoidance instead of investment.¶ Data localization requirements place burdens on domestic enterprises not faced by those operating in more liberal jurisdictions. Countries that require data to be cordoned off complicate matters for their own enterprises, which must turn to domestic services if they are to comply with the law. Such companies must also develop mechanisms to segregate the data they hold by the nationality of the data subject. The limitations may impede development of new, global services. Critics argue that South Korea's ban on the export of mapping data, for example, impedes the development of next-generation services in Korea: Technology services, such as Google Glass, driverless cars, and information programs for visually-impaired users, are unlikely to develop and grow in Korea. Laws made in the 1960s are preventing many venture enterprises from advancing to foreign markets via location/navigation services. n243¶ The harms of data localization for local businesses are not restricted to Internet enterprises or to consumers denied access to global services. As it turns out, most of the economic benefits from Internet technologies accrue to traditional businesses. A McKinsey study estimates that about seventy-five percent of the value added created by the Internet and data flow is in traditional industries, in part through increases in productivity. n244 The potential economic impact across the major sectors - healthcare, manufacturing, electricity, urban infra-structure, security, agriculture, retail, etc. - is estimated at $ 2.7 to $ 6.2 trillion per year. n245 This is particularly important for emerging economies, in which traditional industries remain predominant. The Internet raises profits as well, due to increased revenues, lower costs of goods sold, and lower administrative costs. n246 With data localization mandates, traditional businesses [\*728] will lose access to the many global services that would store or process information offshore.

#### Fourth, the plan will reverse these trends. Reforming 702 will bring hundreds of billions back to the U.S. and save the domestic technology industry

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

There is a realpolitic argument to be made here as well, which ties more directly to U.S. foreign interests. Namely, U.S. failure to [\*228] ensure privacy protections may lead to a loss in U.S. competitiveness. And economic concerns are central to U.S. national security. Consider the impact of the public release of information about NSA Section 702 surveillance on the U.S. cloud computing industry. There was an immediate, detrimental impact on the strength of the U.S. economy. Billions of dollars are now on the line because of concerns that the services provided by U.S. information technology companies are neither secure nor private. n450 The Information Technology and Innovation Foundation estimates that declining revenues of corporations that focus on cloud computing and data storage alone could reach $ 35 billion over the next three years. n451 Other commentators, such as Forrester Research analyst James Staten, have put actual losses as high as $ 180 billion by 2016, unless something is done to restore overseas' confidence in data held by U.S. companies. n452

Failure to extend privacy protections to individuals with substantial connections to the country via industry would, in this view, make it harder, not easier for the United States to assert its legitimate power and authority abroad. So, under Kennedy's reasoning, one could argue that Fourth Amendment rights should be extended to individuals economically tied to U.S. entities. This determination, however, is ultimately one of policy--not law. Deciding whether a greater national security threat is entailed in loss of competitiveness of U.S. industry, versus loss of protections extended to non-U.S. persons in the interests of privacy, is part of the weighing that must be done by the executive branch in pursuing its interests abroad. In this way, the Rehnquist opinion and [\*229] the Kennedy concurrence can be read as compatible with not extending Fourth Amendment rights to individuals lacking a legal relationship (in other words, those stemming directly from the individual's status as a member of the political community). n453

This appears to have been the crux of President Obama's effort to reassure the international community in January 2014 that the United States would not use its authority to collect trade secrets to advantage U.S. corporations. n454 In Presidential Policy Directive 28, Obama acknowledged the privacy interests held by foreign persons:

#### Fifth, empirically, tech sustains growth and staves off other economic woes.

Jorgenson 01 (Dale, Frederic Eaton Abbe Professor of Economics at Harvard University and chair of the National Research Council’s Board on Science, Technology, and Economic Policy, “U.S. Economic Growth in the Information Age”

The resurgence of the U.S. economy from 1995 to 1999 outran all but the most optimistic expectations. It is not surprising that the unusual combination of more rapid growth and slower inflation touched off a strenuous debate among economists about whether improvements in U.S. economic performance can be sustained. This debate has been intensified by the recent growth slowdown, and the focus has shifted to how best to maintain economic momentum.¶ A consensus is building that the remarkable decline in information technology (IT) prices provides the key to the surge in U.S. economic growth. The IT price decline is rooted in developments in semiconductor technology that are widely understood by technologists and economists. This technology has found its broadest applications in computing and communications equipment, but has reduced the cost and improved the performance of aircraft, automobiles, scientific instruments, and a host of other products.¶ Although prices have declined and product performance has improved in many sectors of the U.S. economy, our picture of these developments is still incomplete. The problem faced by economists is that prices are difficult to track when performance is advancing so rapidly. This year’s computer, cell phone, and design software is different from last year’s. Fortunately, statistical agencies are now focusing intensive efforts on filling in the gaps in our information.¶ Price indexes for IT that hold performance constant are necessary to separate the change in performance of IT equipment from the change in price for a given level of performance. Accurate and timely computer prices have been part of the U.S. National Income and Product Accounts (NIPA) since 1985. Software investment was added to the NIPA in 1999. Unfortunately, important information gaps remain, especially regarding price trends for investments in software and communications equipment.¶ Knowing how much the nation spends on IT is only the first step. We must also consider the dynamics of investment in IT and its impact on our national output. The national accounting framework treats IT equipment as part of the output of investment goods, and capital services from this equipment as a component of capital input. A measure of capital services is essential for capturing the effects of rapidly growing stocks of computers, communications equipment, and software on the output of the U.S. economy.¶ A substantial acceleration in the IT price decline occurred in 1995, triggered by a much sharper acceleration in the price decline of semiconductors. This can be traced to a shift in the product cycle for semiconductors in 1995 from three years to two years as the consequence of intensifying competition. Although the fall in semiconductor prices has been projected to continue for at least another decade, the recent acceleration may be temporary.¶ The investment boom of the later 1990s was not sustainable, because it depended on growth in hours worked that was substantially in excess of growth in the labor force. Nonetheless, growth prospects for the U.S. economy have improved considerably, due to enhanced productivity growth in IT production and rapid substitution of IT assets for non-IT assets in response to falling IT prices. An understanding of the role of IT is crucial to the design of policies to revive economic growth and exploit the opportunities created by our improved economic performance.

#### Sixth, that’s good, because an economic decline would cause war.

Royal 10 — Jedidiah Royal, Director of Cooperative Threat Reduction at the U.S. Department of Defense, M.Phil. Candidate at the University of New South Wales, 2010 (“Economic Integration, Economic Signalling and the Problem of Economic Crises,” *Economics of War and Peace: Economic, Legal and Political Perspectives*, Edited by Ben Goldsmith and Jurgen Brauer, Published by Emerald Group Publishing, ISBN 0857240048, p. 213-215)

Less intuitive is how periods of economic decline may increase the likelihood of external conflict. Political science literature has contributed a moderate degree of attention to the impact of economic decline and the security and defence behaviour of interdependent states. Research in this vein has been considered at systemic, dyadic and national levels. Several notable contributions follow. ¶ First, on the systemic level, Pollins (2008) advances Modelski and Thompson's (1996) work on leadership cycle theory, finding that rhythms in the global economy are associated with the rise and fall of a pre-eminent power and the often bloody transition from one pre-eminent leader to the next. As such, exogenous shocks such as economic crises could usher in a redistribution of relative power (see also Gilpin. 1981) that leads to uncertainty about power balances, increasing the risk of miscalculation (Feaver, 1995). Alternatively, even a relatively certain redistribution of power could lead to a permissive environment for conflict as a rising power may seek to challenge a declining power (Werner. 1999). Separately, Pollins (1996) also shows that global economic cycles combined with parallel leadership cycles impact the likelihood of conflict among major, medium and small powers, although he suggests that the causes and connections between global economic conditions and security conditions remain unknown.¶ Second, on a dyadic level, Copeland's (1996, 2000) theory of trade expectations suggests that 'future expectation of trade' is a significant variable in understanding economic conditions and security behaviour of states. He argues that interdependent states are likely to gain pacific benefits from trade so long as they have an optimistic view of future trade relations. However, if the expectations of future trade decline, particularly for difficult [end page 213] to replace items such as energy resources, the likelihood for conflict increases, as states will be inclined to use force to gain access to those resources. Crises could potentially be the trigger for decreased trade expectations either on its own or because it triggers protectionist moves by interdependent states.4 ¶ Third, others have considered the link between economic decline and external armed conflict at a national level. Blomberg and Hess (2002) find a strong correlation between internal conflict and external conflict, particularly during periods of economic downturn. They write,¶ The linkages between internal and external conflict and prosperity are strong and mutually reinforcing. Economic conflict tends to spawn internal conflict, which in turn returns the favour. Moreover, the presence of a recession tends to amplify the extent to which international and external conflicts self-reinforce each other. (Blomberg & Hess, 2002. p. 89) ¶ Economic decline has also been linked with an increase in the likelihood of terrorism (Blomberg, Hess, & Weerapana, 2004), which has the capacity to spill across borders and lead to external tensions. ¶ Furthermore, crises generally reduce the popularity of a sitting government. “Diversionary theory" suggests that, when facing unpopularity arising from economic decline, sitting governments have increased incentives to fabricate external military conflicts to create a 'rally around the flag' effect. Wang (1996), DeRouen (1995). and Blomberg, Hess, and Thacker (2006) find supporting evidence showing that economic decline and use of force are at least indirectly correlated. Gelpi (1997), Miller (1999), and Kisangani and Pickering (2009) suggest that the tendency towards diversionary tactics are greater for democratic states than autocratic states, due to the fact that democratic leaders are generally more susceptible to being removed from office due to lack of domestic support. DeRouen (2000) has provided evidence showing that periods of weak economic performance in the United States, and thus weak Presidential popularity, are statistically linked to an increase in the use of force. ¶ In summary, recent economic scholarship positively correlates economic integration with an increase in the frequency of economic crises, whereas political science scholarship links economic decline with external conflict at systemic, dyadic and national levels.5 This implied connection between integration, crises and armed conflict has not featured prominently in the economic-security debate and deserves more attention. ¶ This observation is not contradictory to other perspectives that link economic interdependence with a decrease in the likelihood of external conflict, such as those mentioned in the first paragraph of this chapter. [end page 214] Those studies tend to focus on dyadic interdependence instead of global interdependence and do not specifically consider the occurrence of and conditions created by economic crises. As such, the view presented here should be considered ancillary to those views.

### Advantage 2 is Surveillance

#### First, Section 702 of the FISA Authorization Act authorizes a broad expansion of surveillance technology

Butler 13 (Alan, Appelate Advocate Counsel, Electronic Privacy Information Ctr. And JD UCLA School of Law, “ARTICLE: Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance,” 48 New Eng. L. Rev. 55, L/N)

Recent debate about foreign intelligence surveillance relates to two key FISA provisions that were added and amended in the decade following the attacks of September 11, 2001. The first is the business records provision n5 which was established by Congress in the USA PATRIOT Act, Section 215. n6 [\*58] The second provision governs the targeting of non-U.S. persons reasonably believed to be outside the United States, which was added by Section 702 of the FAA. n7 Both of these provisions expanded the scope of foreign intelligence surveillance that can be conducted within the United States.¶ The FISA was enacted to impose statutory restrictions on domestic intelligence gathering. n8 It outlines the Government's authority to conduct national security investigations both inside the United States and abroad. n9 Within the parameters of the statute, certain intelligence community members are authorized to engage in "electronic surveillance" of foreign agents; n10 to conduct physical searches targeting foreign agents; n11 and to use pen/trap n12 surveillance or apply for court orders compelling the production of business records in connection with certain national security investigations. n13 The FISA did not regulate any intelligence collection abroad until it was amended in 2007 and 2008. n14¶ Most FISA surveillance is authorized by orders of the FISC, n15 a special [\*59] court created by Congress in 1978 to provide judicial oversight of electronic surveillance and other intelligence gathering activities. The FISC has jurisdiction under the FISA to authorize electronic surveillance, pen/trap surveillance, physical searches, and orders directing the production of business records. n16 The court may only issue orders for electronic surveillance and physical searches upon a showing of probable cause that the target is a "foreign power or agent of a foreign power." n17 However, the FAA broadened the scope of FISC-authorized surveillance by allowing the government to target persons "reasonably believed to be located outside [of] the United States" without establishing probable cause to show they are foreign agents. n18 In addition, under the PATRIOT Act, applications for pen register surveillance and business record orders can be used to obtain information for FBI national security investigations. n19 Under the new rules, the FISC "shall enter" orders granting such applications if the information sought is "relevant" to an ongoing investigation of international terrorism. n20¶ In addition to granting new intelligence collection authority, the FAA imposed new rules for collection abroad. n21 The FAA authorizes members of the Intelligence Community to acquire foreign intelligence by targeting persons that they reasonably believe are located outside the United States, without following the traditional FISA rules governing "electronic [\*60] surveillance" or "physical search." n22 Instead, the FISC reviews targeting and minimization procedures, adopted by the Attorney General and the Director of National Intelligence pursuant to Section 702, for compliance with the statute and the Fourth Amendment. n23 After the FISC approves the targeting and minimization requirements and reviews the government certification to ensure it "contains all the required elements," the court "shall enter" the order to the government. n24 Once the order is granted, the government can issue "directives" to "electronic communication service providers," such as telephone and Internet companies, requiring their assistance in collecting electronic communications. n25¶ The FAA amendments were the result of an effort by executive and legislative branch officials to "modernize" the FISA. n26 This modernization was justified in part by the government's belief that certain requirements for surveillance and collection unduly restricted the "speed and agility" [\*61] needed to fight post-9/11 threats. n27 In this modernization debate, the question arose whether the government should rely on internal executive branch procedures to ensure adequate oversight of intelligence gathering, or should be required to provide individualized evidence to the FISC before conducting electronic surveillance.¶ At the time the FAA was passed, the Bush administration claimed that the amendments were a necessary response to changing technology, specifically the shift from satellite to fiber optic transmission of international communications. n28 Yet, as Kris and Wilson demonstrate in their leading treatise, a review of telecommunications history shows that claim to have been greatly exaggerated. n29 Still, changing technologies used to transmit emails and one-end domestic and international wire communications presented new challenges to the application of FISA's provisions governing "electronic surveillance." n30 Email and other electronic [\*62] communications present special difficulties because many international messages are stored in, or transmitted through, facilities in the United States. n31 As a result, the government attempted to expand its surveillance authority: first with unilateral executive action, n32 then judicial authorization, n33 and finally through legislation with the PAA n34 and its successor the FAA. n35

#### Second, Section 702 authorizes programmatic surveillance-violates the 4th Amendment

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

Almost immediately after passage of the FAA, members of Congress, scholars, and others began criticizing Section 702 because [\*154] of the potential for the government to use the authorities to engage in programmatic surveillance. n144¶ In 2009 prominent national security law Professor William Banks explained, "the FAA targets do not have to be suspected of being an agent of a foreign power or, for that matter, they do not have to be suspected of terrorism or any national security offense, so long as the collection of foreign intelligence is a significant purpose of the surveillance." n145 Surveillance could be directed at a person, organization, e-mail address, or even "an entire ISP or area code." n146 He noted, "the surveillance permitted under the FAA does not require that the Government identify a particular known facility where the intercepted communications occur." n147 These provisions represented a sea change from how FISA had previously worked (albeit introducing, for the first time, statutory restrictions in an area previously governed by Executive Order). U.S. persons' communications now could be incidentally collected under the statute, on a large scale, without many of the protections in traditional FISA. n148¶ Banks presciently pointed out the most likely way in which the new authorities would be used:¶ Although details of the implementation of the program . . . are not known, a best guess is the Government uses a broad vacuum cleaner-like first stage of collection, focusing on transactional data, where wholesale interception occurs following the development and implementation of filtering criteria. Then the NSA engages in a more particularized collection of content after analyzing mined data . . . [A]ccidental or incidental acquisition of U.S. persons inside the United States [will] surely occur[], especially in light of the difficulty of ascertaining a target's location. n149¶ For Professor Banks, part of the problem was that the nature of international information flows meant that it would be impossible [\*155] to tell if an individual is located overseas or within domestic bounds. n150¶ Banks was not the only one to question the implementation of Section 702. Cases began to appear, raising facial and as applied constitutional challenges. Problems characteristic of relying on Article III courts in the context of surveillance came to the fore. In Clapper v. Amnesty International, plaintiffs alleged that Section 702 violated the targets' Fourth Amendment rights because it allowed for the acquisition of international communications absent an individualized court order supported by probable cause. n151 The Supreme Court dismissed the suit for lack of standing--that is, the absence of any concrete injury. It did not reach the merits of the Fourth Amendment claim. n152

#### Third, that erodes U.S. constitutionalism and rights guarantees-there are no checks.

Donohue continues in 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

As aforementioned, Section 702 places four limitations on acquisition, each of which is meant to restrict the amount of information that can be obtained by the government. n166 The NSA has sidestepped these statutory restrictions in three important ways: first, it has adopted procedures that allow analysts to acquire information "about" selectors (that is, communications modes used by targets) or targets, and not merely communications to or from targets (or selectors employed by targets), or information held by targets themselves. Second, it has created a presumption of non-U.S. person status: That is, if an individual is not known to be a U.S. person (and thus exempted from Section 702 and treated either under Sections 703 and 704 or under traditional FISA, depending on the location), then the NSA assumes that the individual is a non-U.S. person. Third, the NSA has failed to adopt standards that would require it to ascertain whether a target is located within domestic bounds. Instead, the agency, having looked at the available evidence, absent evidence to the contrary, assumes that the target is located outside the United States. These interpretations work together to undermine Congress's addition of Sections 703 and 704, even as they open the door to more extensive collection of domestic communications.

#### Fourth, privacy is a lynchpin to a variety of other human rights—absent a guarantee of privacy authoritarianism can flourish

Banisar and Davies 15 (David, Electronic Privacy Information Center, and Simon, Privacy International, Global Internet Liberty Campaign 15 (“PRIVACY AND HUMAN RIGHTS: An International Survey of Privacy Laws and Practice” http://gilc.org/privacy/survey/intro.html)

Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Convenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age. The publication of this report reflects the growing importance, diversity and complexity of this fundamental right.¶ This report provides details of the state of privacy in fifty countries from around the world. It outlines the constitutional and legal conditions of privacy protection, and summarizes important issues and events relating to privacy and surveillance.¶ Nearly every country in the world recognizes a right of privacy explicitly in their Constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. Most recently-written Constitutions such as South Africa's and Hungary's include specific rights to access and control one's personal information.¶ In many of the countries where privacy is not explicitly recognized in the Constitution, such as the United States, Ireland and India, the courts have found that right in other provisions. In many countries, international agreements that recognize privacy rights such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights have been adopted into law.¶ In the early 1970s, countries began adopting broad laws intended to protect individual privacy. Throughout the world, there is a general movement towards the adoption of comprehensive privacy laws that set a framework for protection. Most of these laws are based on the models introduced by the Organization for Economic Cooperation and Development and the Council of Europe.¶ In 1995, conscious both of the shortcomings of law, and the many differences in the level of protection in each of its States, the European Union passed a Europe-wide directive which will provide citizens with a wider range of protections over abuses of their data.[fn 1] The directive on the "Protection of Individuals with regard to the processing of personal data and on the free movement of such data" sets a benchmark for national law. Each EU State must pass complementary legislation by October 1998.¶ The Directive also imposes an obligation on member States to ensure that the personal information relating to European citizens is covered by law when it is exported to, and processed in, countries outside Europe. This requirement has resulted in growing pressure outside Europe for the passage of privacy laws. More than forty countries now have data protection or information privacy laws. More are in the process of being enacted.¶ ¶ Reasons for Adopting Comprehensive Laws¶ There are three major reasons for the movement towards comprehensive privacy and data protection laws. Many countries are adopting these laws for one or more reasons.¶ To remedy past injustices. Many countries, especially in Central Europe, South America and South Africa, are adopting laws to remedy privacy violations that occurred under previous authoritarian regimes.¶ To promote electronic commerce. Many countries, especially in Asia, but also Canada, have developed or are currently developing laws in an effort to promote electronic commerce. These countries recognize consumers are uneasy with their personal information being sent worldwide. Privacy laws are being introduced as part of a package of laws intended to facilitate electronic commerce by setting up uniform rules.¶ To ensure laws are consistent with Pan-European laws. Most countries in Central and Eastern Europe are adopting new laws based on the Council of Europe Convention and the European Union Data Protection Directive. Many of these countries hope to join the European Union in the near future. Countries in other regions, such as Canada, are adopting new laws to ensure that trade will not be affected by the requirements of the EU Directive.

#### Fifth, upholding constitutional principles of democracy and human rights solves global wars in the middle east.

Rosenberg et al, 6 (Yemeni National Organization for Defending Rights and Freedoms (HOOD), Brief Amicus Curiae of the Yemeni National Organization for Defending Rights and Freedoms, in Support of Petitioner Salim Ahmed Hamdan, Lawrence D. Rosenberg, Counsel of Record, in Salim Ahmed Hamdan, Petitioner, v. Donald H. Rumsfeld, et al., Respondents, n. 05-184, 2005 U.S. Briefs 194, 2006 U.S. S. Ct. Briefs LEXIS 4, January 6, 2006, LN)

On issues of democracy, human rights, and the rule of law, the United States sets the example for the rest of the world. Especially since the September 11, 2001 attacks, the United States has challenged the Middle East to follow in its footsteps--to embrace the development of democratic institutions, to respect human rights, and to adhere to the rule of law. The Arab world has responded, and progress has been made throughout much of the Middle East. But progress is difficult, especially in the post-9/11 environment. For the Middle East to continue pursuing these ideals, it is critical that the United States continue to lead the way. The September 11 attacks worked a fundamental shift in United States policy in the Middle East. Secretary of State Condoleezza Rice has acknowledged this change of direction: "For sixty years, . . . the United States[] [\*\*10] pursued stability at the expense of democracy . . . in the Middle East, and . . . achieved neither. Now we are taking a different course. We are supporting the democratic aspirations of all people. Successful societies allow room for healthy civic institutions--for political parties and labor unions and independent newspapers and broadcast media. Id. As the world's oldest, strongest, and most important democracy, the United States sets a key guidepost for other nations when it clearly enunciates and applies the principles upon which free societies necessarily are based. Arab nations pay heed to the United States' [\*\*12] example and efforts. "The Arab world holds in high esteem . . . the ambitious American dream of attaining a more just, peaceful and tolerant human society." The League of Arab States Statement on the Occasion of the 1st Anniversary of the Tragic Events of 11/9/2001 (Sept. 11, 2002), available at http://www.arableagu...98&level\_id=219 (last visited Jan. 5, 2006). King Abdullah of Jordan, for example, has acknowledged [\*6] that "the leadership of the United States is crucial in all our efforts to reach a just and lasting peace of the Middle East." President Bush, Jordanian King Discuss Iraq, Middle East (May 6, 2004), available at http://www.whitehous...20040506-9.html (last visited Jan. 5, 2006). This recognition and admiration are derived from the United States' moral and political legitimacy. Moreover, the United States has backed up its words with concrete efforts that "vividly demonstrate[] U.S. commitment to promoting democracy and respect for human rights." Freedom, democracy and human rights all go hand in hand. . . . The promotion of democracy and freedom is a cornerstone of the foreign policy of the administration. And we can already see the results . . . . Human Rights "Extremely Important" To U.S., Says Delegate to UNCHR, July 21, 2005 (statement of Goli Ameri, U.S. delegate to United [\*\*18] Nations Commission on Human Rights), available at http://usinfo.state..../21-564409.html (last visited Jan. 5, 2006). But "the experiment of human rights is still new in [Yemen]," and the difficult task still remains "to pay great and special attention to the principles of human rights, to consolidate them and surround them with the respect they deserve, to make them an ideal road to the flourishing of the democratic experiment . . . ." Yemen Human Rights Report at 8. As Yemen and other Middle East nations tackle that difficult task, it is essential to recall that "America[,] not just the nation[,] but an idea, [is] alive in the minds of people everywhere." George H.W. Bush, President, State of the Union Address. To foster continued progress on democracy, human rights, and the rule of law in the Middle East, the United States must continue to nurture and promote this "idea" that it has long represented throughout the world.

# Case Extensions

## Inherency Extensions

### Surveillance Increasing

#### The NSA mass surveillance records, stores, parses, and searches all electronic communication—and it’s increasing offline as well

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

The recent National Security Agency (NSA) data scandal has revealed what technologists have long suspected: every aspect of online life is tracked and recorded. The NSA maintains programs that cover "nearly everything a typical user does on the internet" n1 and collect "pretty much everything it can" n2 - e-mail and text messages, voice and video chats, photos and videos, file transfers, social networking information, Internet browsing histories and searches, and so on - rendering all of this data searchable by the government. n3 Pursuant to secret court orders, Americans' telephone and Internet metadata records are being proactively recorded, stored, parsed, and searched. n4 From the massive datasets derived from this data, it is possible to determine whom people talk to, where they are, what they are interested in, and even to predict what they might do next. n5 Outside of the NSA context, government monitoring has expanded through the use of third-party data and by the creation of state-run databases. Digital surveillance is increasing offline as well. For example, some police cars [\*983] now use license plate readers to create a database of driver locations. n6 New overhead camera technology permits tracking of the location and activities of everyone in an entire city for hours. n7 In the Boston bombing investigation, street cameras, cellphone recordings, and even a municipal facial recognition system were employed in pursuit of the culprits. n8

#### Social media and the observation of social media is increasing significantly

Miller 10 (Rich Miller on September 16, 2010 http://www.datacenterknowledge.com/archives/2010/09/16/facebook-50-million-a-year-on-data-centers/)

An analysis of Facebook’s spending with data center developers indicates that the company is now paying about $50 million a year to lease data center space, compared to about $20 million when we last analyzed its leases in May 2009. That jump in spending reflects increased investment in infrastructure as the social network has grown from 200 million users in mid-2009 to more than 500 million today. During that period, Facebook has added multiple data centers in two major Internet hubs: Ashburn, Virginia and Silicon Valley in California. The company has also announced plans to build a 300,000 square foot data center in Prineville, Oregon for additional expansion.

#### XKeyscore Overarching Data Collection

Shneier 15 (Bruce, “More about NSA’s XKeyscore”. Shneier on Security. July 7) https://www.schneier.com/blog/archives/2015/07/more\_about\_the\_.html

I've been reading through the 48 classified documents about the NSA's XKEYSCORE system released by the Intercept last week. From the article: The NSA's XKEYSCORE program, first revealed by The Guardian, sweeps up countless people's Internet searches, emails, documents, usernames and passwords, and other private communications. XKEYSCORE is fed a constant flow of Internet traffic from fiber optic cables that make up the backbone of the world's communication network, among other sources, for processing. As of 2008, the surveillance system boasted approximately 150 field sites in the United States, Mexico, Brazil, United Kingdom, Spain, Russia, Nigeria, Somalia, Pakistan, Japan, Australia, as well as many other countries, consisting of over 700 servers. These servers store "full-take data" at the collection sites -- meaning that they captured all of the traffic collected -- and, as of 2009, stored content for 3 to 5 days and metadata for 30 to 45 days. NSA documents indicate that tens of billions of records are stored in its database. "It is a fully distributed processing and query system that runs on machines around the world," an NSA briefing on XKEYSCORE says. "At field sites, XKEYSCORE can run on multiple computers that gives it the ability to scale in both processing power and storage." There seems to be no access controls at all restricting how analysts can use XKEYSCORE. Standing queries -- called "workflows" -- and new fingerprints have an approval process, presumably for load issues, but individual queries are not approved beforehand but may be audited after the fact. These are things which are supposed to be low latency, and you can't have an approval process for low latency analyst queries. Since a query can get at the recorded raw data, a single query is effectively a retrospective wiretap.

### USA Freedom Act Doesn’t Solve

#### USA FREEDOM Act doesn’t reform Section 702

Geiger 15 (Harley, Advocacy Director and Senior Counsel at the Center for Democracy & Technology, “Q&A on the USA FREEDOM Act of 2015,” Center for Democracy and Technology-Security and Surveillance, April 28, https://cdt.org/blog/q-a-on-the-usa-freedom-act-of-2015/)

Q2: Why is this bill worth supporting when it doesn’t address 702 backdoor searches or the DEA‘s criminal bulk collection authority?¶ A2: CDT is definitely invested in addressing these problems, and we’d certainly prefer to see the USA FREEDOM Act make far more reforms than it does. However, it is not an omnibus surveillance reform bill. The USA FREEDOM Act addresses one category of problems, mainly domestic bulk collection under the PATRIOT Act. [Note: the DEA authority is criminal and was not created in the PATRIOT Act.] Congress should view the bill through this lens too – as one step, not the final step. We believe that enacting effective reform to domestic bulk collection under the PATRIOT Act will create a more favorable environment in Congress to enact reforms in other areas – especially around the sunset for Sec. 702 in 2017.

### 702 is Expanding

#### 702 authorizes broad collection of internet data—NSA’s interpretations continue to expand reach.

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

Three points related to the volume and intrusiveness of the resulting surveillance deserve notice. First, to obtain "about" communications, because of how the Internet is constructed, the NSA must monitor large amounts of data. n180 That is, if the NSA may [\*163] collect not just e-mail to or from the target's e-mail account (badguy@ISP.com), but, in addition, other communications happening to mention badguy@ISP.com that pass through the collection point, then the NSA is monitoring a significant amount of traffic. And the agency is not just considering envelope information (for example, messages in which the selector is sending, receiving, or copied on the communication) but the actual content of messages. n181¶ Second, wholly domestic conversations may become swept up in the surveillance simply by nature of how the Internet is constructed. Everything one does online involves packets of information. Every Web site, every e-mail, every transfer of documents takes the information involved and divides it up into small bundles. Limited in size, these packets contain information about the sender's IP address, the intended receiver's IP address, something that indicates how many packets the communication has been divvied up into, and what number in the chain is represented by the packet in question. n182¶ Packet switched networks ship this information to a common destination via the most expedient route--one that may, or may not, include the other packets of information contained in the message. If a roadblock or problem arises in the network, the packets can then be re-routed, to reach their final destination. Domestic messages may thus be routed through international servers, if that is the most efficient route to the final destination.¶ What this means is that even if the NSA applies an IP filter to eliminate communications that appear to be within the United States, it may nevertheless monitor domestic conversations by nature of them being routed through foreign servers. In this manner, a student in Chicago may send an e-mail to a student in Boston [\*164] that gets routed through a server in Canada. Through no intent or design of the individual in Chicago, the message becomes international and thus subject to NSA surveillance.¶ Third, further collection of domestic conversations takes place through the NSA's intercept of what are called multi-communication transactions, or MCTs. It is important to distinguish here between a transaction and a communication. Some transactions have only single communications associated with them. These are referred to as SCTs. Other transactions contain multiple communications. If even one of the communications in an MCT falls within the NSA's surveillance, all of the communications bundled into the MCT are collected.¶ The consequence is of significant import. FISC estimated in 2011 that somewhere between 300,000 and 400,000 MCTs were being collected annually on the basis of "about" communication--where the "active user" was not the target. So hundreds of thousands of communications were being collected that did not include the target as either the sender or the recipient of the communication. n183

## Solvency

### FISA Reform Solves 702

#### FISA Reform must increase reporting, make disclosure of opinions mandatory, and create an adversarial environment in the court—legislation is key

Butler 13 (Alan, Appelate Advocate Counsel, Electronic Privacy Information Ctr. And JD UCLA School of Law, “ARTICLE: Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance,” 48 New Eng. L. Rev. 55, L/N)

In the wake of the Clapper opinion and the NSA leaks, a number of legislative proposals are being considered to reform the FISA and to improve government accountability. While a litigation solution remains possible and should be pursued, legislative reform may more fully address the need for additional oversight and transparency. Ultimately, reforms adopted should include three key components: increased public reporting, mandatory disclosure of FISC opinions, and more adversarial briefing at the FISC.¶ This article considers the recent proposals to increase transparency and oversight of foreign intelligence surveillance conducted by the U.S. Intelligence Community. First, the article will provide a brief overview of the FISA programs at issue. The article will then consider the Court's standing analysis in Clapper in light of recent disclosures, and discuss its impact on future judicial oversight of surveillance activities. Further, it will describe recent legislative proposals to amend the FISA, improve oversight mechanisms, and require public reporting regarding the privacy impact of FISA surveillance. Finally, the article will outline three key elements necessary to reform the current FISA system and propose additional transparency and oversight procedures necessary to bring surveillance in line with constitutional and legal principles.

#### Comprehensive FISA reform must enable transparency and oversight to uphold the rule of law—reporting, disclosure, and briefing are key.

Butler 13 (Alan, Appelate Advocate Counsel, Electronic Privacy Information Ctr. And JD UCLA School of Law, “ARTICLE: Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance,” 48 New Eng. L. Rev. 55, L/N)

The Supreme Court's decision in Clapper will limit judicial oversight of FISA surveillance in the future. In light of the new standing limitation and recent disclosures about FBI and NSA surveillance programs, it is necessary to reform the current FISA structure to enable greater transparency and oversight, and to improve judicial review. There are also a number of proposals to reduce or eliminate surveillance authorities previously granted under the Patriot Act or the FAA, n174 but this section will focus on the reforms necessary to improve the current public oversight process.

Federal courts will continue to review challenges to current surveillance activities, and recent disclosures have reinvigorated many of these challenges. n175 But, regardless of the outcomes of particular cases, the public needs access to more information about FISA processes, including the presence and effectiveness of any privacy and civil liberties protections. There are fundamental questions about the legal scope of foreign intelligence surveillance under the FISA and under the Constitution. n176 The rule of law requires that these questions be answerable, but the Supreme Court's decision in Clapper highlights how difficult it is to obtain such review in the current system. Many of the proposals submitted in Congress would aid this process, but FISA reform must be comprehensive and have three key components: (1) additional public reporting on the scope of FISA surveillance; (2) mandatory public disclosure of FISC decisions; and (3) [\*83] adversarial briefing in the FISC. n177

### Declassification Solves

#### Current reporting requirements are inadequate—declassification of domestic surveillance is key to privacy.

Butler 13 (Alan, Appelate Advocate Counsel, Electronic Privacy Information Ctr. And JD UCLA School of Law, “ARTICLE: Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance,” 48 New Eng. L. Rev. 55, L/N)

The information provided in the Attorney General's annual FISA letter, as required by statute, n178 is inadequate to inform the public about the scope and effectiveness of foreign intelligence surveillance programs. The need for additional public reporting has been recognized since shortly after the passage of the USA PATRIOT Act. For example, the American Bar Association urged Congress in 2003 to conduct regular oversight and to create an annual public report on FISA investigations similar to the annual wiretap report prepared by the Administrative Office of the United States Courts. n179 A comprehensive statistical report is necessary to ensure that FISA authorities are used effectively and efficiently, and to ensure that the system adequately protects the privacy of U.S. persons.¶ In contrast with the annual FISA letter - which only includes the number of "orders and extensions either granted, modified, or denied" for electronic surveillance and production of business records or tangible things - the Wiretap Report provides essential details about the execution and efficiency of law enforcement surveillance. n180 The wiretap reports include a detailed overview of the cost, duration, and effectiveness of investigative surveillance. They also provide a statistical breakdown of law enforcement activities based on the type of crime investigated n181 and the types of communications intercepted. n182 This data provides a basis to evaluate the effectiveness of wiretap authority, to measure its cost, and to understand the impact of surveillance on innocent individuals. These detailed public reports ensure that law enforcement resources are used appropriately and efficiently while protecting important privacy interests.¶ The information contained in the current annual Attorney General [\*84] FISA letters is incomplete and unhelpful. The annual FISA letter contains no information about pen/trap surveillance or the use of FAA-authorized directives. n183 According to the current Presiding Judge of the FISC, the annual FISA letter does not even contain enough detail to accurately reflect the application and review process before the court. n184 When asked directly by Senator Wyden to estimate the impact of the FAA on U.S. persons, Director of National Intelligence ("DNI") James R. Clapper responded that "a meaningful and accurate unclassified response ... is not possible." n185 Instead, the DNI provided a classified response and indicated that there are regular internal executive branch compliance assessments and classified Congressional briefings to ensure oversight. n186 But none of these assessments or reports have been made public, and as a result public debate about the controversial scope of surveillance under Section 215 and Section 702 has been stifled.¶ Legislators have proposed a number of reforms that would include additional public reporting about FISA activities. Many of the reform bills introduced in the 113th Congress require additional reports by the Attorney General or Inspectors General of the Department of Justice or other Intelligence Community components. n187 Other bills provide for [\*85] additional statistical reports regarding FISA collection, including numbers of previously unreported orders and estimates of the impact on U.S. persons. n188 However, not all of these reports are required to be unclassified or otherwise made public. n189 So far none of the proposals would require reports as detailed as the annual Wiretap Reports. In part, this is because national security investigations do not have the same metrics as criminal investigations (charges, convictions, etc.). But some of the proposals do [\*86] require an analysis by the inspectors general or the attorney general of the use and effectiveness of FISA authorities. n190¶ One question raised in both Clapper and recent congressional debates is the impact of FAA-authorized surveillance on the private communications of U.S. persons. Any revised public reporting standard must address this important issue and provide declassified details about the impact, the privacy protections in place, and any violations of the privacy rules. Without these details, the public will be unable to adequately assess the efficacy of the program and the sufficiency of government privacy protections. Unlike previous reauthorization cycles, the expiring FISA provisions should be closely scrutinized when their current sunsets expire in 2015 and 2017. n191

#### Failure to declassify decisions undermines checks and balances and disables democratic oversight

Butler 13 (Alan, Appelate Advocate Counsel, Electronic Privacy Information Ctr. And JD UCLA School of Law, “ARTICLE: Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance,” 48 New Eng. L. Rev. 55, L/N)

The failure to publish FISC opinions over the last ten years is the root of the current loss of public confidence in the Administration's use of foreign intelligence authorities. n192 The court's legal analysis and conclusions, as opposed to the operational details of surveillance activities, are part of the law that cannot properly develop without public oversight. Promulgation of the law is a central requirement of democracy; the failure to promulgate results in a "failure to make law." n193 Both the FISC and the [\*87] Attorney General bear the responsibility to promote public understanding of the FISA process and what it encompasses. This is especially true where the court attempts to strike some balance between national security and civil liberties concerns. n194 Secret law undermines our system of checks and balances by disabling the democratic oversight by which the public governs its government. n195¶ A number of current proposals would increase transparency and facilitate public oversight of FISA authorities. n196 Most of these proposals require that the Attorney General submit declassified versions, or summaries, of significant FISC opinions that are already submitted to the Intelligence Committees in classified form under 50 U.S.C. ß 1871(c). Senator Blumenthal's proposal is significantly broader because it would require disclosure of any decision with a "significant construction or interpretation of law." n197 It would also provide for an adversarial party at the FISC, the Special Advocate, and would require disclosure of any FISC opinion appealed by the Advocate and any FISCR opinion issued on appeal. n198 It would also empower the Special Advocate to petition the FISC or the Foreign Intelligence Surveillance Court of Review ("FISCR") for release of any document, which the court can order even over the objection of the Attorney General. n199¶ The FISC has recently made clear that its rules do not prohibit the [\*88] Government's disclosure of prior opinions, n200 but it has so far been reluctant to publish more than a handful. n201 After the NSA leaks during the summer of 2013, several FISC opinions were released by the Director of National Intelligence. n202 The problem is that no current rule or law requires either the FISC or the Attorney General to publish significant FISC opinions, and until such a rule exists both will be hesitant to take responsibility for redacting properly classified details to facilitate public dissemination. Even top administration officials have acknowledged that we have an overclassification problem, n203 and clearly there is more work to do to make legal interpretations and authorities public. The current proposals represent a strong step in the right direction because they include mandatory declassification of FISC legal interpretations (or summaries thereof) and set clear timelines for publication release by the Attorney General. The USA FREEDOM Act and Senator Blumenthal's bill would go even further by providing for a petition from the Special Advocate directly to the FISC or FISCR for release of court documents. n204

### Special Advocate Solves

#### Appointing a special advocate is key to court precedence, 4th amendment issues, and privacy protection—the UK proves it would work

Butler 13 (Alan, Appelate Advocate Counsel, Electronic Privacy Information Ctr. And JD UCLA School of Law, “ARTICLE: Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance,” 48 New Eng. L. Rev. 55, L/N)

The recent revelations about the extent and nature of FISA surveillance have highlighted the important and unreviewed body of constitutional and statutory law being developed by the FISC. n205 Unlike other ex parte proceedings, the FISC reviews of applications submitted under Section 702 require extensive analysis and create precedent for the court. n206 But this [\*89] lawmaking process only works when the judges hear both sides of the argument. In addition, the Fourth Amendment issues and technical details of surveillance tactics are very complex, and FISC judges cannot adequately evaluate the various interests without in-depth briefing on both sides. Any FISC reform should address this problem by providing for a "Special Advocate" to the court, who would operate with a security clearance and argue in opposition to the Department of Justice on important legal questions regarding FISA and the Constitution.¶ The FISC is developing complex legal interpretations under a provision of the FAA that requires the FISC to find that the "targeting and minimization procedures" adopted by the Government are "consistent with ... the fourth amendment to the Constitution ... ." n207 But these decisions are necessarily complex and difficult to make in the abstract context of a Section 702 application because Fourth Amendment analysis is necessarily fact-based. n208 In the American judicial system, facts are developed through an adversarial process. n209 The government has an interest in arguing in favor of the surveillance applications that it submits to the FISC; a Department of Justice lawyer's role is not to present the judges with reasons why the application might be denied or modified. There is currently no advocate on the other side of these complex and novel issues judged by the FISC. And while recipients of FISA-authorized surveillance orders and directives can file challenges under certain circumstances, n210 they cannot review the classified opinions or government briefs and do not have the necessary opportunity or incentive to develop fact-based constitutional arguments.¶ The difficulty in having an adversarial process at the FISC is that the materials presented by the government are highly classified. However, [\*90] classified proceedings have become more prevalent over the past ten years in the United States n211 as well as in the United Kingdom. n212 The use of specially appointed, security-cleared attorneys to challenge government legal arguments in national security cases has been in place for more than a decade in the United Kingdom. n213 The use of such a "Special Advocate" would be appropriate in the FISA context where FISC judges are asked to make novel and significant legal determinations regarding important constitutional rights. Two former FISC judges, n214 and other prominent legal scholars, n215 have proposed adding such an adversarial position to ensure that legal developments at the FISC do not suffer from unbalanced advocacy. n216

A security cleared special advocate would promote transparency and uphold constitutional balance—key to checking expansive government surveillance.

Butler 13 (Alan, Appelate Advocate Counsel, Electronic Privacy Information Ctr. And JD UCLA School of Law, “ARTICLE: Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance,” 48 New Eng. L. Rev. 55, L/N)

Senator Blumenthal then introduced a comprehensive proposal co-sponsored by fifteen other Senators, n217 which would create an Office of the [\*91] Special Advocate as an independent establishment within the executive branch. n218 That proposal has since been incorporated into the USA FREEDOM Act. n219 This citizen's advocate would argue against expansive government interpretations of national security authorities while also increasing transparency and facilitating more robust public reporting. Under the Blumenthal proposal, the Special Advocate would review all FISA applications and filings and have the authority to appeal or otherwise challenge rulings of the FISC. n220 The Special Advocate would also have the authority to request declassification and publication of FISC opinions and documents, or trigger mandatory disclosure whenever he or she files an appeal. n221 Additionally, the Special Advocate would be responsible for filing a report with Congress every year, evaluating the effectiveness of the FISA process and suggesting any necessary legislative changes. n222¶ The Special Advocate would promote transparency and reporting while providing a much-needed balance to the constitutional and statutory arguments made before the FISC.

## Section 702 Bad

### 702 --> Loophole

#### Section 702 creates a legal loophole that allows broad collection of data without the protections of FISA—allows virtually unlimited collection of private communication data.

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

Almost immediately after passage of the FAA, members of Congress, scholars, and others began criticizing Section 702 because [\*154] of the potential for the government to use the authorities to engage in programmatic surveillance. n144¶ In 2009 prominent national security law Professor William Banks explained, "the FAA targets do not have to be suspected of being an agent of a foreign power or, for that matter, they do not have to be suspected of terrorism or any national security offense, so long as the collection of foreign intelligence is a significant purpose of the surveillance." n145 Surveillance could be directed at a person, organization, e-mail address, or even "an entire ISP or area code." n146 He noted, "the surveillance permitted under the FAA does not require that the Government identify a particular known facility where the intercepted communications occur." n147 These provisions represented a sea change from how FISA had previously worked (albeit introducing, for the first time, statutory restrictions in an area previously governed by Executive Order). U.S. persons' communications now could be incidentally collected under the statute, on a large scale, without many of the protections in traditional FISA. n148¶ Banks presciently pointed out the most likely way in which the new authorities would be used:¶ ¶ Although details of the implementation of the program . . . are not known, a best guess is the Government uses a broad vacuum cleaner-like first stage of collection, focusing on transactional data, where wholesale interception occurs following the development and implementation of filtering criteria. Then the NSA engages in a more particularized collection of content after analyzing mined data . . . [A]ccidental or incidental acquisition of U.S. persons inside the United States [will] surely occur[], especially in light of the difficulty of ascertaining a target's location. n149¶ For Professor Banks, part of the problem was that the nature of international information flows meant that it would be impossible [\*155] to tell if an individual is located overseas or within domestic bounds. n150¶ Banks was not the only one to question the implementation of Section 702. Cases began to appear, raising facial and as applied constitutional challenges. Problems characteristic of relying on Article III courts in the context of surveillance came to the fore. In Clapper v. Amnesty International, plaintiffs alleged that Section 702 violated the targets' Fourth Amendment rights because it allowed for the acquisition of international communications absent an individualized court order supported by probable cause. n151 The Supreme Court dismissed the suit for lack of standing--that is, the absence of any concrete injury. It did not reach the merits of the Fourth Amendment claim. n152¶ The FAA was set to expire at the end of 2012. By early February, James Clapper, the Director of National Intelligence, and Attorney General Eric Holder had informed Congressional leaders that reauthorization of the FAA was "the top legislative priority of the national Intelligence Community." n153 The Administration credited the FAA with the production of "significant intelligence that is vital to protect the nation against international terrorism [\*156] and other threats." n154 Offering classified briefings and attaching an unclassified annex, Clapper and Holder wrote, "We are always considering whether there are changes that could be made to improve the law in a manner consistent with the privacy and civil liberties interests of Americans." n155 But their "first priority" was "reauthorization of these authorities in their current form." n156¶ The NSA's inability to provide the number of American citizens' communications intercepted under the act became a matter of public debate. In May 2012 Senators Ron Wyden and Mark Udall raised concerns about what they referred to as a "back door" in the statute. n157 In June 2012 SSCI noted numerous senators' concern about the IC's inability to provide an estimate of the number of individuals whose communications had been intercepted. n158 Attention was further drawn to the lack of information about whether the NSA had attempted to search Americans' communications without a warrant. n159 By the end of July 2012, more than a dozen senators had joined a letter to Director of National Intelligence James R. Clapper, expressing alarm "that the intelligence community has stated that 'it is not reasonably possible to identify the number of people located inside the United [\*157] States whose communications may have been reviewed' under the FAA.'" n160

#### Section 702 allows broad and unintentional collection of communications data—and it’s receiving little public criticism

Granick 14 (Jennifer, Director of Civil Liberties at the Stanford Center for Internet and Society, “Reforming The Section 702 Dragnet (Part 1),” *Just Security,* January 30, 2014, http://justsecurity.org/6574/reforming-section-702-dragnet-1/)

So far, less attention has been paid to the legality—and wisdom—of mass surveillance under section 702 of the FISA Amendments Act (FAA), codified at 50 USC 1881a. Section 702 is the statutory authority for the PRISM program, which involves warrantless collection of communications contents via targeting non-U.S. individuals or entities reasonably believed to be located abroad. The USA Freedom Act would strengthen and impose additional restrictions on section 702 surveillance, but would not end the dragnet. Meanwhile, a report from the New America Foundation recently took a serious look at the efficacy of 702 in counterterrorism. Researchers concluded that section 702 is less valuable than people may have assumed, finding that section 702 collection played a role in only 4.4 percent of examined terrorism cases. In a few months, PCLOB plans to issue a report on section 702 collection.¶ So it’s a great time to take a serious look at reforming section 702. This post is the first in a series where I’ll explain the law, PRISM, and the ways in which intelligence agencies are using and abusing this collection authority. In the end, I’ll make a series of recommendations for how we might begin to reform 702.¶ LEGAL BACKGROUND¶ Section 702 authorizes warrantless acquisition of communications—including Americans’ communications—if at least one party to the message is overseas, and the target—that is the person or entity about which the government wants information—is a non-U.S. person.¶ When intelligence officials accurately describe the law, they do not say this. Rather, they say that the law allows them to target non-US persons reasonably believed to be abroad in order to collect foreign intelligence information. That’s true, but it encourages the false belief that only non-citizens are affected by section 702 collection. Before the Snowden disclosures, government surveillance lawyers like myself were in an ongoing “yes you do—no we don’t” argument with the intelligence agencies about what section 702 authorized. People who knew better used careful language to imply the legal tool had nothing to do with Americans and that if Americans were affected, it was only rarely. Thanks to Snowden, we are no longer pretending the Emperor has on clothes.¶ So let’s be clear:¶ While section 702 requires a non-US entity be the target of surveillance, anyone who communicates with agents of the target, or has foreign intelligence information about the target, may be monitored. In sum, under this law, the government:¶ MAY warrantlessly acquire Americans’ foreign to foreign or one-end US communications to, from or about the target; and¶ MAY warrantlessly acquire Americans’ domestic communications, so long as the acquisition was unintentional.

#### MCTs allow the acquisition of bulk communication data—250 million communications per year are collected under 702

Granick 14 (Jennifer, Director of Civil Liberties at the Stanford Center for Internet and Society, “Reforming The Section 702 Dragnet (Part 1),” *Just Security,* January 30, 2014, http://justsecurity.org/6574/reforming-section-702-dragnet-1/)

Capturing Americans’ one-end-foreign communications is part and parcel of section 702. So, how many American messages does the NSA collect under this legal authority? According to a newly declassified 2011 FISA court opinion by Judge John Bates, the NSA obtained approximately 250 million communications under section 702 that year. Most of those messages, 91%, came from service providers like Google, Yahoo! and Microsoft, via PRISM. The remainder are vacuumed off the fiber optic backbone of the Internet—upstream collection.¶ When conducting upstream collection, NSA’s systems don’t always pull single messages; rather, they regularly capture what the agency, with characteristic opacity, refers to as “Internet transactions.” An “Internet transaction” may be comprised of a single message – an “SCT”, in NSA-speak. But Internet transactions often contain multiple messages – the agency refers to this bundle of messages as an “MCT”. If only one message in an MCT is responsive to the NSA’s targeting terms, the NSA devices nonetheless pull the entire package of messages into the NSA databases. Further, MCTs can contain messages that have nothing to do with foreigners or foreign intelligence. NSA’s internal auditing, done at Judge Bates’ version of gunpoint, put the number of improperly collected wholly domestic American messages at approximately 56,000 that year.

### 702 X 4th Amendment

#### The Snowden revelations that exposed PRISM have created a constitutional crisis on Fourth Amendment grounds—Section 702 of the FAA falls outside the reasonableness component and tramples constitutional provisions of privacy

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

On June 6, 2013, the Washington Post and the Guardian captured public attention by reporting that the intelligence community was collecting large amounts of information about U.S. citizens. n1 The National Security Agency (NSA) and Federal Bureau of Investigation (FBI) were "tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio, video, photographs, e-mails, documents and connection logs that enable analysts to track a person's movements and contacts over time." n2¶ In conjunction with the articles, the press published a series of PowerPoint slides attributed to the NSA, describing a program called "PRISM" (also known by its SIGAD, US-984XN). n3 The title [\*120] slide referred to it as the most used NSA SIGAD. n4 The documents explained that PRISM draws from Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple--some of the largest e-mail, social network, and communications providers--making the type of information that could be obtained substantial: email, video and voice chat, videos, photos, stored data, VoIP, file transfers, video conferencing, notifications of target activity (for example, logins), social networking details, and special requests. n5 The slides noted that the program started in September 2007, with just one partner (Microsoft), gradually expanding to the most recent company (Apple, added October 2012), and that the total cost of the program was $ 20 million per year. n6 As of 2011, most of the more than 250 million Internet communications obtained each year by the NSA under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act derived from PRISM. n7¶ A follow-up article two days later printed another slide depicting both PRISM and "upstream" collection of communications on fiber cables and infrastructure ("[c]ollection directly from the servers of . . . U.S. Service Providers.") n8 Upstream interception allowed the NSA to acquire Internet communications "as they [\*121] transit the 'internet backbone' facilities." n9 The NSA could collect all traffic crossing Internet cables--not just information targeted at specific Internet Protocol (IP) addresses or telephone number. The potential yield was substantial: in the first six months of 2011, the NSA acquired more than 13.25 million Internet transactions through its upstream collection. n10 The slide urged analysts to use both PRISM and upstream collection to obtain information. n11¶ Within days of the releases, the intelligence community acknowledged the existence of the programs. n12 In August 2013 the Director of National Intelligence, James Clapper, offered further confirmation, noting that PRISM had been in operation since Congress had passed the 2008 FISA Amendments Act. n13 He declassified eight documents, n14 and by the end of the month, he had announced that the intelligence community would release the total [\*122] number of Section 702 orders issued, and targets thereby affected, on an annual basis. n15¶ Although much of the information about PRISM and upstream collection remains classified, what has been made public suggests that these programs push statutory language to its limit, even as they raise critical Fourth Amendment concerns. n16 Accordingly, this Article proceeds in three Parts: the evolution of Section 702, a statutory analysis of PRISM and upstream collection, and the attendant constitutional concerns.¶ The Article begins by considering the origins of the current programs and the relevant authorities--particularly the transfer of part of the President's Surveillance Program, instituted just after September 11, to the 1978 Foreign Intelligence Surveillance Act (FISA). It outlines the contours of the 2007 Protect America Act, before its replacement in 2008 by the FISA Amendments Act (FAA). n17 The first Part ends with a brief discussion of the current [\*123] state of foreign intelligence collection under Executive Order 12,333, outside either FISA or the FAA.¶ The Article next turns to statutory issues related to targeting, post-targeting analysis, and the retention and dissemination of information. It argues that the NSA has sidestepped FAA restrictions by adopting procedures that allow analysts to acquire information not just to or from, but also "about" targets. In its foreignness determination the agency assumes, absent evidence to the contrary, that the target is a non-U.S. person located outside domestic bounds. And weak standards mark the foreign intelligence purpose determination. Together, these elements allow for the broad collection of U.S. persons' international communications, even as they open the door to the interception of domestic communications. In regard to post-targeting analysis, the Article draws attention to the intelligence community's use of U.S. person information to query data obtained under Section 702, effectively bypassing protections Congress introduced to prevent reverse targeting. The Article further notes in relation to retention and dissemination that increasing consumer and industrial reliance on cryptography means that the NSA's retention of encrypted data may soon become the exception that swallows the rule.¶ In its constitutional analysis, the Article finds certain practices instituted under Section 702 to fall outside acceptable Fourth Amendment bounds. Although lower courts had begun to recognize a domestic foreign intelligence exception to the warrant clause, in 1978 Congress introduced FISA to be the sole means via which domestic foreign intelligence electronic intercepts could be undertaken. Consistent with separation of powers doctrine, this shift carried constitutional meaning. Internationally, practice and precedent prior to the FAA turned on a foreign intelligence exception. But in 2008 Congress altered the status quo, introducing individualized judicial review into the process. Like FISA, the FAA carried constitutional import.¶ [\*124] If that were the end of the story, one could argue that the incidental collection of U.S. persons' information, as well as the interception of domestic conversations ought to be regarded in Justice Jackson's third category under Youngstown Sheet & Tube Co. v. Sawyer. n18 Renewal in 2012, however, points in the opposite direction. The NSA's actions, for purposes of the warrant clause, appear to be constitutionally sufficient insofar as foreign intelligence gathering to or from non-U.S. persons is concerned. The tipping point comes with regard to criminal prosecution. Absent a foreign intelligence purpose, there is no exception to the warrant requirement for the query of U.S. persons' international or domestic communications.¶ Although a warrant is not required for foreign intelligence collection overseas, the interception of communications under Section 702 must still comport with the reasonableness requirements of the Fourth Amendment. A totality of the circumstances test, in which the significant governmental interest in national security is weighed against the potential intrusion into U.S. persons' privacy, applies. The incidental collection of large quantities of U.S. persons' international communications, the scanning of content for information "about" non-U.S. person targets, and the interception of non-relevant and entirely domestic communications in multi-communication transactions, as well as the query of data using U.S. person identifiers, fall outside the reasonableness component of the Fourth Amendment.

#### The Snowden revelations that exposed PRISM have created a constitutional crisis on Fourth Amendment grounds—Section 702 of the FAA falls outside the reasonableness component and tramples constitutional provisions of privacy

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

On June 6, 2013, the Washington Post and the Guardian captured public attention by reporting that the intelligence community was collecting large amounts of information about U.S. citizens. n1 The National Security Agency (NSA) and Federal Bureau of Investigation (FBI) were "tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio, video, photographs, e-mails, documents and connection logs that enable analysts to track a person's movements and contacts over time." n2¶ In conjunction with the articles, the press published a series of PowerPoint slides attributed to the NSA, describing a program called "PRISM" (also known by its SIGAD, US-984XN). n3 The title [\*120] slide referred to it as the most used NSA SIGAD. n4 The documents explained that PRISM draws from Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple--some of the largest e-mail, social network, and communications providers--making the type of information that could be obtained substantial: email, video and voice chat, videos, photos, stored data, VoIP, file transfers, video conferencing, notifications of target activity (for example, logins), social networking details, and special requests. n5 The slides noted that the program started in September 2007, with just one partner (Microsoft), gradually expanding to the most recent company (Apple, added October 2012), and that the total cost of the program was $ 20 million per year. n6 As of 2011, most of the more than 250 million Internet communications obtained each year by the NSA under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act derived from PRISM. n7¶ A follow-up article two days later printed another slide depicting both PRISM and "upstream" collection of communications on fiber cables and infrastructure ("[c]ollection directly from the servers of . . . U.S. Service Providers.") n8 Upstream interception allowed the NSA to acquire Internet communications "as they [\*121] transit the 'internet backbone' facilities." n9 The NSA could collect all traffic crossing Internet cables--not just information targeted at specific Internet Protocol (IP) addresses or telephone number. The potential yield was substantial: in the first six months of 2011, the NSA acquired more than 13.25 million Internet transactions through its upstream collection. n10 The slide urged analysts to use both PRISM and upstream collection to obtain information. n11¶ Within days of the releases, the intelligence community acknowledged the existence of the programs. n12 In August 2013 the Director of National Intelligence, James Clapper, offered further confirmation, noting that PRISM had been in operation since Congress had passed the 2008 FISA Amendments Act. n13 He declassified eight documents, n14 and by the end of the month, he had announced that the intelligence community would release the total [\*122] number of Section 702 orders issued, and targets thereby affected, on an annual basis. n15¶ Although much of the information about PRISM and upstream collection remains classified, what has been made public suggests that these programs push statutory language to its limit, even as they raise critical Fourth Amendment concerns. n16 Accordingly, this Article proceeds in three Parts: the evolution of Section 702, a statutory analysis of PRISM and upstream collection, and the attendant constitutional concerns.¶ The Article begins by considering the origins of the current programs and the relevant authorities--particularly the transfer of part of the President's Surveillance Program, instituted just after September 11, to the 1978 Foreign Intelligence Surveillance Act (FISA). It outlines the contours of the 2007 Protect America Act, before its replacement in 2008 by the FISA Amendments Act (FAA). n17 The first Part ends with a brief discussion of the current [\*123] state of foreign intelligence collection under Executive Order 12,333, outside either FISA or the FAA.¶ The Article next turns to statutory issues related to targeting, post-targeting analysis, and the retention and dissemination of information. It argues that the NSA has sidestepped FAA restrictions by adopting procedures that allow analysts to acquire information not just to or from, but also "about" targets. In its foreignness determination the agency assumes, absent evidence to the contrary, that the target is a non-U.S. person located outside domestic bounds. And weak standards mark the foreign intelligence purpose determination. Together, these elements allow for the broad collection of U.S. persons' international communications, even as they open the door to the interception of domestic communications. In regard to post-targeting analysis, the Article draws attention to the intelligence community's use of U.S. person information to query data obtained under Section 702, effectively bypassing protections Congress introduced to prevent reverse targeting. The Article further notes in relation to retention and dissemination that increasing consumer and industrial reliance on cryptography means that the NSA's retention of encrypted data may soon become the exception that swallows the rule.¶ In its constitutional analysis, the Article finds certain practices instituted under Section 702 to fall outside acceptable Fourth Amendment bounds. Although lower courts had begun to recognize a domestic foreign intelligence exception to the warrant clause, in 1978 Congress introduced FISA to be the sole means via which domestic foreign intelligence electronic intercepts could be undertaken. Consistent with separation of powers doctrine, this shift carried constitutional meaning. Internationally, practice and precedent prior to the FAA turned on a foreign intelligence exception. But in 2008 Congress altered the status quo, introducing individualized judicial review into the process. Like FISA, the FAA carried constitutional import.¶ [\*124] If that were the end of the story, one could argue that the incidental collection of U.S. persons' information, as well as the interception of domestic conversations ought to be regarded in Justice Jackson's third category under Youngstown Sheet & Tube Co. v. Sawyer. n18 Renewal in 2012, however, points in the opposite direction. The NSA's actions, for purposes of the warrant clause, appear to be constitutionally sufficient insofar as foreign intelligence gathering to or from non-U.S. persons is concerned. The tipping point comes with regard to criminal prosecution. Absent a foreign intelligence purpose, there is no exception to the warrant requirement for the query of U.S. persons' international or domestic communications.¶ Although a warrant is not required for foreign intelligence collection overseas, the interception of communications under Section 702 must still comport with the reasonableness requirements of the Fourth Amendment. A totality of the circumstances test, in which the significant governmental interest in national security is weighed against the potential intrusion into U.S. persons' privacy, applies. The incidental collection of large quantities of U.S. persons' international communications, the scanning of content for information "about" non-U.S. person targets, and the interception of non-relevant and entirely domestic communications in multi-communication transactions, as well as the query of data using U.S. person identifiers, fall outside the reasonableness component of the Fourth Amendment.

#### Section 702 permits untargeted surveillance, opens citizens to the web of government intrusion, and allows blanket 4th amendment violations for the foreseeable future

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

The bill actually permits the government to perform mass untargeted surveillance of any and all conversations believed to be coming into and out of the United States without any individualized finding and without a requirement that wrongdoing is believed to be involved at all.¶ It arguably is not limited just to terrorism. It could be any foreign intelligence, which would include diplomacy and anything else. n232¶ Representative Jackie Speier's statement proved prescient:¶ It is fundamentally untrue to say that Americans will not be placed under surveillance . . . . The truth is, any American will subject their phone and e-mail conversations to the broad government surveillance web simply by calling a son or daughter studying abroad, sending an email to a foreign [\*178] relative, even calling an American company whose customer service center is located overseas. n233¶ Speier, a California Democrat, continued: "The bottom line is, this FISA bill permits the collection of Americans' emails and phone calls if they are communicating with someone outside of the U.S." n234 Representative Rush Holt (D-NJ), a member of HPSCI, opposed the bill on similar grounds: "It permits massive warrantless surveillance in the absence of any standard for defining how communications of innocent Americans will be protected; a fishing expedition approach to intelligence collection that we know will not make Americans more safe." n235 Representative Dennis Kucinich (D-OH) opposed the legislation for the same reason: "There's no requirement for the government to seek a warrant for any intercepted communication that includes a U.S. citizen, as long as the program in general is directed towards foreign targets." n236 Kucinich added:¶ Under this bill, violations of Fourth Amendment rights and blanket wiretaps will be permissible for the next 4 years. Massive and untargeted collection of communications will continue . . . .¶ Furthermore, it allows the type of surveillance to be applied to all communications entering and exiting the United States. These blanket wiretaps make it impossible to know whose calls are being intercepted by the National Security Agency. n237¶ These statements stood in sharp contrast to the legislators who supported the bill, all of whom discounted the amount and extent of incidental information thereby obtained, pointing particularly to the minimization procedures as a way to rectify any privacy interests thereby implicated.

#### Under 702, the NSA can retain encrypted communications indefinitely which raises a host of constitutional questions. It’s a 4th Amendment Thing.

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

One of the most concerning issues that arises in regard to the retention and dissemination of data obtained under Section 702 is that the NSA may indefinitely retain encrypted communications. In light of increasing public and private use of encryption, the exception may soon swallow the rule, resulting in fewer protections for individual and consumer privacy. In addition, the NSA's minimization procedures allow for incidental information to be kept, analyzed, and distributed if found relevant to the authorized purpose of the acquisition under one of two conditions: first, as containing foreign intelligence information, and, second, as containing evidence of a crime. n322 The former is anchored in traditional FISA and critical for U.S. national security. The latter is similarly consistent with traditional FISA; however, lacking the same procedural protections that attend searches under Titles I and II of the statute, use of information obtained under Section 702 for criminal prosecution raises important constitutional questions.¶ 1. Retention of Encrypted Communications¶ For domestic communications, the NSA retains information that contains technical data base information and data necessary to assess communications security vulnerabilities. n323 The minimization procedures explain that in the context of cryptanalytics, "maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning." n324 Unlike unencrypted communications, which are retained for five years from the date of the certification authorizing the collection (unless the NSA decides otherwise), encrypted communications may be retained for "any period of time during which encrypted material is subject to, or of use in, cryptanalysis." n325¶ [\*200] For foreign communications of or concerning U.S. persons, the NSA retains encrypted material "for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement." n326 There is no limit on the amount of time that encrypted information may be kept, as long as it continues to be subject to, or of use in, cryptanalysis. n327¶ The logic behind the default is that the government should not be forced to purge data merely because it does not hold the key or has been unable to break the code. Considering the likelihood that bad actors may try to use encryption to hide the contents of their communications, the intelligence community does not want to put itself at a disadvantage.¶ The problem is that it is not just bad actors who encipher messages. U.S. citizens and private industry are increasingly using encryption to try to protect their materials and communications. Windows, for instance, has an Encrypting File System that can be used to store information in an encrypted format. Systems like Pretty Good Privacy (PGP) can be set up and installed using a Firefox plugin, making it easy to encrypt e-mail. In March 2014, Google announced that it is now using https encrypted communications whenever users log in to Gmail, regardless of which Internet connection they are using. n328 Nicolas Lidzborski, Gmail's Security Engineering Lead explained:¶ Today's change means that no one can listen in on your messages as they go back and forth between you and Gmail's servers--no matter if you're using public WiFi or logging in from your computer, phone or tablet. In addition, every single email message you send or receive--100% of them--is encrypted while moving internally. This ensures that your messages are safe not only when they move between [\*201] you and Gmail's servers, but also as they move between Google's data centers--something we made a top priority after last summer's revelations. n329¶ The irony of Google's actions in light of the NSA's retention policies is hard to miss: in part because the NSA was intercepting Gmail and reading it (at which point the agency was required under minimization procedures to eliminate irrelevant information), the company now encrypts all communications, with the result that the NSA can still collect Gmail, but it can now keep it indefinitely, simply because it is encrypted at the front end. Assuming that the NSA has the tools to decrypt the communications, it is unclear how this provides greater protections for U.S. persons' privacy. Nevertheless, in light of Google's new policy, and calls from consumers for other companies to follow suit, n330 it seems that this practice may become standard.¶ Not only are we seeing greater individual use of encryption, but companies generally are also looking for ways to ensure the security of their data. The cost of enabling hardware encryption capabilities is falling: from $ 100 in 2009, by 2012, the cost of enabling hardware encryption capabilities to hard disk drives had plummeted to $ 15. n331 Simultaneously, a series of data breaches and their enormous cost to companies (quite apart from questions related to international consumer confidence in U.S. companies post-June 2013), encouraged industry to make greater use of encryption. n332 According to a recent market research report, the ? [\*202] hardware encryption market is expected to reach some $ 166.67 billion by 2018, growing at an incredible CAGR of 62.17% from 2013 to 2018. n333 These trends call attention to the NSA's back-end retention policies with regard to encrypted materials.¶ 2. Use of Section 702 Data in Criminal Prosecution¶ NSA's minimization procedures place a duty on the NSA to turn over any information regarding the commission of a crime to law enforcement agencies, if the NSA would like to retain the information. n334 In light of front-end considerations (the inclusion of information "about" selectors/targets and the assumption of non-U.S. person and overseas status), U.S. persons' international and, at times, domestic communications can be monitored, collected, and used against them in a court of law, without law enforcement ever satisfying Title III requirements. Neither individualized suspicion nor insertion of a neutral, third-party magistrate characterizes Section 702 collection. U.S. persons may not themselves be in direct contact with any of the approved targets under Section 702. And query of databases using U.S. person identifiers may further implicate U.S. persons in criminal activity--even acts unrelated to national security. But no individualized judicial process is required. Courts have in the past found applications under traditional FISA sufficient. n335 But Section 702 includes none of these protections, giving rise to both statutory bypass and Fourth Amendment concerns.

### 702 X Constitution

#### Section 702 falls outside constitutional limitations

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

As a matter of the interception of international communications, the Supreme Court has held that the Fourth Amendment does not apply to non-U.S. persons, who do not have a strong attachment to the United States. n342 The government is not required to obtain a warrant prior to conducting searches of such individuals outside domestic bounds. Prior to the 2008 FAA, neither was the government required to obtain a warrant, or anything even approximating a warrant, for the surveillance of U.S. persons overseas.¶ Sections 703 and 704 of the FAA altered the status quo, requiring the government to go to a court to obtain an individualized order, prior to targeting a U.S. person overseas. This shift carried constitutional meaning. Congress itself was intensely aware that in passing the FAA, it was invoking its authority under separation of powers doctrine, to limit the scope of executive action when it came to gathering foreign intelligence.¶ One could argue that programmatic collection (leading to the incidental collection of significant amounts of U.S. persons' communications), TFA, and the monitoring of unrelated communications embedded in MCTs run contrary to Congressional [\*205] intent under Sections 703 and 704. That is, if Congress intended U.S. persons to have a higher level of protection by inserting a neutral judicial magistrate to issue an individualized order (based on some level of suspicion of wrongdoing) for electronic surveillance, then the collection of significant amounts of U.S. persons' communications without these safeguards acts as an end-run around the protections. Under Youngstown, this would mean that the executive branch's actions should be considered at the lowest ebb.¶ The problem with this argument is that even if it might have been true in 2008, certainly by the time of the renewal debates, there was enough information available to Congress about how the executive branch was using the provisions. The decision to continue the powers at that point brought the executive branch's actions, at least insofar as the warrant clause is concerned, to the highest tier of Jackson's concurrence.¶ The Court's deference, however, extends only insofar as a warrant is required for the collection of foreign intelligence. n343 It does not extend to the querying of information for law enforcement purposes, for the simple reason that, at that point, foreign affairs are no longer relevant. Queries occur well within the realm of criminal law, where the Court has long insisted on a warrant, outside of limited exceptions. Nor do foreign affairs considerations reach the reasonableness component of the Fourth Amendment.¶ For the former, the failure of the executive to obtain prior judicial authorization, upon a showing of particularity, falls outside constitutional constraints.¶ For the latter, the test is one of the totality of the circumstances. The significant governmental interest in national security must be weighed against the potential intrusion into U.S. persons' privacy. The whole picture matters, including programmatic collection (resulting in the monitoring and collection of significant amounts of U.S. persons' communications), the scanning of content for information "about" selector s/targets, and the interception of non-relevant communications as part of MCTs. Equally important are [\*206] the protections built into the system at the back-end, to limit the acquisition, use, dissemination, and retention of U.S. persons' communications. In light of this analysis, the manner in which Section 702 has been implemented falls outside constitutional boundaries.

### 702 X Privacy

#### Section 702 gives the NSA virtually unlimited access to private communication data--erodes internet privacy.

Granick 14 (Jennifer, Director of Civil Liberties at the Stanford Center for Internet and Society, “Reforming The Section 702 Dragnet (Part 1),” *Just Security,* January 30, 2014, http://justsecurity.org/6574/reforming-section-702-dragnet-1/)

Americans’ communications with targets overseas are subject to warrantless interception. Once those communications are collected, current rules allow the NSA to search the trove for U.S. person identifiers, which Senator Ron Wyden has referred to as the “back door searches loophole”.¶ The non-U.S. targets include regular people, not just those who are agents of foreign powers. While analysts provide their foreign intelligence purpose when selecting the target, the rationale is just one short sentence.¶ By untethering surveillance from facilities that the target uses, the FAA greatly increased the opportunity for the NSA to collect information about rather than just to or from the target. As an example, if I monitor a network for “Jennifer Granick” and Jennifer Granick uses that network, I’ll get her communications, and maybe some messages about her. If I can monitor facilities “Jennifer Granick” doesn’t use, even accurate selectors will pull messages about her.¶ That last one might sound ok if the target is a known terrorist. But the definition of foreign intelligence is far broader than that, and includes information related to (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States. So, section 702 allows collection of what we might say about NSA targets like al Qaeda—or even Iran, France, Wikileaks, Petrobras, the Institute of Physics at the Hebrew University of Jerusalem, UNICEF, Medicines du Monde, or any other entity that helps the U.S. government “understand economic systems and policies, and monitor anomalous economic activities”. The government has absolutely no legitimate business listening in on anyone’s conversations about these matters.¶ [By the way, I support public disclosure of the identities of these controversial NSA targets. Knowing who the NSA thinks is legitimate to spy on gives us a much clearer idea of the topics they believe justify spying on Americans—under 702 or otherwise—as well.]¶ In fact, section 702 endangers U.S. person privacy far beyond that of any other surveillance authorization.¶ Any number of individuals may be intentionally targeted as a result of a single FAA authorization and need not be specifically identified. Therefore, more Americans are likely to be monitored since an undefined and evolving list of individuals may be believed to be agents of approved targets, and those individuals may talk with Americans;¶ No wrongdoing required on the part of the target, who need not even be an agent of a foreign power as under traditional FISA;¶ Intelligence agents may monitor any facility, even if there is no connection to the target. This vastly expands the opportunities for “about” collection of communications between wholly innocent and uninvolved people;¶ Minimization obligations under the FAA are far weaker than even those under traditional FISA because the FISA court has less authority to authorize, implement and oversee compliance with the rules;¶ Under section 702, there is no judicial review of the government’s justification for the surveillance or identification of targets;¶ The government makes no notification to individuals incidentally or mistakenly monitored; and¶ It is very difficult to learn about, or to impose consequences, for violating the FAA.

### No Oversight

#### Under 702, FISA court judges address broad constitutional questions with no public scrutiny—zero oversight

Butler 13 (Alan, Appelate Advocate Counsel, Electronic Privacy Information Ctr. And JD UCLA School of Law, “ARTICLE: Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance,” 48 New Eng. L. Rev. 55, L/N)

As new details have emerged about the FBI and NSA's domestic intelligence-gathering practices, it has become clear that the current system does not provide enough transparency to ensure public oversight and trust. n42 There are three main problems with the current system: the development of a secret body of constitutional and statutory law by the FISC, structural limitations on judicial review of FISA surveillance, and rules inhibiting Congress' ability to facilitate public oversight. As a result, important questions about the scope and nature of surveillance remain unanswered, and in many cases, there is not even enough information to know which questions to ask.¶ Over the last decade, the FISC began developing a secret body of law governing FISA surveillance and addressing important constitutional and statutory issues that should be made public. n43 This shift occurred after the Government began to expand foreign intelligence surveillance beyond the [\*64] scope of individualized FISA warrants. n44 With the enactment of the FAA, Congress introduced a new role for the FISC: approval of government surveillance programs based on general targeting and minimization procedures. n45 Under Section 702 of the FAA, the FISC judge reviewing the government application and procedures must determine whether the targeting and minimization procedures are "consistent with the requirements of [the statute] and with the Fourth Amendment." n46 As a result, the FISC now regularly assesses "broad constitutional questions" and establishes "important judicial precedents, with almost no public scrutiny." n47 The secrecy of these important opinions is a flaw in the system and prevents public oversight of developing national security law.¶ Congress plays an important role in the intelligence oversight process as well, but its oversight of FISA activity authorized under Section 702 and Section 215 is severely limited by procedural rules imposed by the Department of Justice ("DOJ") and inadequate public reporting. The law requires that the Attorney General keep the Senate Select Committee on Intelligence, n48 the House Permanent Select Committee on Intelligence, n49 and the Senate Judiciary Committee "fully informed" concerning the Government's use of FISA. n50 However, reports sent from the DOJ to the [\*65] House and Senate Intelligence Committees impose strict rules on the dissemination of the government's legal interpretation of these programs. n51 For example, the detailed reports on the use of Section 215 were only available in Intelligence Committee offices for a "limited time period," no photocopies or notes could be taken out of the room, and only certain congressional staff members were allowed to attend. n52 Similar rules likely apply to the Attorney General's reports on significant FISA legal interpretations n53 and the use of Section 702 authorities. n54 Public reports regarding the extent of FISA surveillance activity give a bare minimum of information, including only the number of applications for electronic surveillance, the number granted, modified, or denied, n55 and the same information regarding requests for orders compelling production of business records. n56 Unlike the Wiretap Reports issued by the Administrative Office of the U.S. Courts, which provide a comprehensive overview of the cost, duration, and effectiveness of surveillance in criminal investigations, n57 the FISA reports do not provide sufficient detail. n58 As a result, Members of Congress and the public do not have the information [\*66] they need to evaluate the efficacy and legality of these programs. n59¶ The problem of secret law is exacerbated by the limited judicial review of important constitutional and statutory issues related to modern FISA surveillance. As one former FISA judge recently noted, the role of judges is not to make policy, it is to "review policy determinations for compliance with statutory law" - but such review must be done in the context "of [the] adversarial process." n60 The FISA does not currently provide for adversarial hearings in the FISC, even when presented with complex and novel issues. n61 And unlike warrants and other ex parte orders issued in criminal cases, judicial review of FISA activity is not guaranteed in criminal prosecutions or other subsequent proceedings. n62 Even when the government provides notice of the use of FISA-derived evidence in criminal cases, it has not specified whether such surveillance was accomplished pursuant to Section 702 authorized directives. n63 As a result, the traditional means of obtaining judicial review of the ultimate [\*67] constitutional question regarding modern FISA surveillance is unavailable. The Supreme Court has also made it more difficult to assert a constitutional challenge in a civil case based on Section 702 activities. n64

### AT: NSA Limitations Check

#### NSA sidesteps Section 702 limitations in three ways

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

[\*158] A. Targeting¶ As aforementioned, Section 702 places four limitations on acquisition, each of which is meant to restrict the amount of information that can be obtained by the government. n166 The NSA has sidestepped these statutory restrictions in three important ways: first, it has adopted procedures that allow analysts to acquire information "about" selectors (that is, communications modes used by targets) or targets, and not merely communications to or from targets (or selectors employed by targets), or information held by targets themselves. Second, it has created a presumption of non-U.S. person status: That is, if an individual is not known to be a U.S. person (and thus exempted from Section 702 and treated either under Sections 703 and 704 or under traditional FISA, depending on the location), then the NSA assumes that the individual is a non-U.S. person. Third, the NSA has failed to adopt standards that would require it to ascertain whether a target is located within domestic bounds. Instead, the agency, having looked at the available evidence, absent evidence to the contrary, assumes that the target is located outside the United States. These interpretations work together to undermine Congress's addition of Sections 703 and 704, even as they open the door to more extensive collection of domestic communications.¶ In 2008 Congress anticipated that U.S. person information would inadvertently be collected under Section 702. This is in part why it included minimization procedures, as well as limits on what could be collected. Most Members, however, do not appear to have contemplated broad, programmatic collection that would undermine protections introduced in Sections 702 and 703. n167 Those who did articulate this possibility voted against the bill.¶ [\*159] Even if Congress did not initially appreciate the potential for programmatic collection, however, certainly by 2012 the intelligence community had made enough information available to Congress for Members to make an informed decision. This does not mean that all Members were fully informed. But to the extent that Members selected not to access the material or to take a public stand on the matter, particularly in light of the legislature's reading of its authorities with regard to classification, fault lies with Congress.¶ The Foreign Intelligence Surveillance Court failed to step into the gap. In 2011, FISC realized the implications of the NSA's interpretation of to, from or about (TFA) collection. However, in light of the seriousness of the NSA's aim (protecting national security), and the limitations imposed by the types of technologies being used, the Court read the statute in a manner that found the targeting procedures to be consistent with the statute.¶ To the extent that NSA's TFA and assumptions regarding the target's foreignness undermine the law as it is written, the legislature failed to perform effective oversight. Congress similarly neglected to uphold the limit placed on the intelligence community to not knowingly collect domestic conversations. Instead, it relied on FISC to do so--a task that the Court failed to do. In a classified environment, when so much information is cloaked from public view, it becomes even more important for the government to ensure that the authorities as they are publicly presented are consistent with the manner in which they are being exercised.

## Advantage 1 Extensions

### 702 🡪 Data Loalization

#### Section 702 guts US business competiveness—causes foreign investors to pull out of US firms and forces many to opt for data localization

Eoyang and Bishai 15 (Mieke and Chrissy, Restoring Trust between U.S. Companies and Their Government on Surveillance Issues March 19, 2015 http://www.thirdway.org/report/restoring-trust-between-us-companies-and-their-government-on-surveillance-issues)

Allegations of intrusive U.S. government electronic surveillance activities have raised international outcry and created antagonism between U.S. technology companies and the government. Without a bold and enduring reform, American companies will continue to suffer a competitive disadvantage from perceptions of U.S. government intrusion into their data. We propose bringing electronic surveillance collection from U.S. companies into an existing statutory framework in order to reassure international customers and to respect the rights of U.S. companies operating abroad.¶ The Problem¶ In the wake of the Snowden revelations, people around the world have become uneasy about the security of their communications that flow through the servers of American companies.1 They now fear—not without reason—that the NSA has broad access to a wide range of their data that may not have any direct relevance to the core foreign policy or security concerns of the United States.2¶ Snowden has also alleged that the NSA accessed American companies’ data without their knowledge.3 American technology companies reacted with outrage to media reports that, unbeknownst to them, the U.S. government had intruded onto their networks overseas and spoofed their web pages or products.4 These stories suggested that the government created and snuck through back doors to take the data rather than come through well-established front doors.5¶ Beyond the broad implications for civil liberties and diplomacy, these fears led to two immediate consequences for the industry: First, many U.S. companies shifted to an adversarial relationship with their own government. They moved to secure and encrypt their data to protect the privacy rights of their customers.6 They are pushing for reform.7 They are building state-of-the-art data centers in Europe and staffing their high-paying jobs with Europeans, not Americans.8 They are challenging the government in court.9¶ Second, international customers of U.S. technology and communications companies began taking their business elsewhere. Brazil decided against a $4.5 billion Boeing deal and cancelled Microsoft contracts.10 Germany dropped Verizon in favor of Deutsche Telekom.11 Both of these examples suggest that if even friendly governments can go to the expense and trouble of dropping American companies, foreign individual and corporate customers could certainly decide to switch their data providers for greater privacy protection. Simply put, the reputational harm had a direct impact on American companies’ competitiveness—some estimate that it has cost U.S. tech firms $180 billion thus far.12¶ Defenders of the programs may argue that the Snowden allegations are overblown or that foreign companies are just using the revelations for their own protectionist purposes. But it doesn’t matter if the allegations are actually true because the global public believes them to be true, and they are therefore real in their consequences.¶ In many ways, the Snowden revelations have created a sense of betrayal among American companies. Some had been providing information to the NSA through existing legislative means – either under Section 215 of the USA Patriot Act,13 or under Section 702 of the FISA Amendments Act (FAA).14 It was unsettling to read stories that, outside of this statutorily compelled cooperation, the government had been getting access to huge amounts of their data in other unauthorized ways. As one tech employee said, “the back door makes a mockery of the front door.”

#### Section 702 hurts US tech competitiveness

Eoyang and Bishai 15 (Mieke and Chrissy, Restoring Trust between U.S. Companies and Their Government on Surveillance Issues March 19, 2015 http://www.thirdway.org/report/restoring-trust-between-us-companies-and-their-government-on-surveillance-issues)

For collection occurring under both 215 and 702, the companies would have been served with an order compelling production of their data. But outside the U.S., Executive Order 12333,15 the long-standing guidance for foreign intelligence activities, would govern the kind of collection that has caused international outrage.¶ E.O. 12333, signed by President Reagan, set the ground rules and authorization for foreign intelligence collection when the nation’s primary security threat was the Soviet Union. At that time, traditional intelligence activities would have been focused on other nation-states—identifying their spies, trying to recruit spies for the U.S., and trying to steal other countries’ secrets while protecting our own. But the growth of terrorist groups’ capabilities, and particularly the 9/11 attacks, helped dissolve the separation between traditional overseas espionage and counter-terrorism.¶ As the nation was grappling with new threats posed by terrorism, people around the world were sharing more and more of their information online and using mostly American companies to do so. Yet the legal framework that had once recognized privacy rights was ill-suited to the Internet Age. The Intelligence Community’s traditional position that constitutional rights like the Fourth Amendment’s privacy protections didn’t apply to non-Americans outside the U.S. might have been clear when travelling and communicating internationally were more difficult. But today’s free-flowing movement of people and data means that the “nationality” of an individual’s communications is far less obvious.16¶ While extending constitutional or privacy protections to foreigners abroad is a tricky legal proposition, for many their data is being held by entities that are entitled to the due process and privacy protections of the U.S. Constitution: American companies. Our tech firms often act as custodians of other people’s data, and as such don’t have the same heightened privacy interests as the targets of that data. But accessing the companies’ data without even giving notice to the owner of the servers raises serious constitutional questions.¶ As a politician once famously noted, “corporations are people too.”17 As a legal (if not political) matter, he was right—these American tech companies are “U.S. Persons,” and they therefore should know when the government seeks to access the data they possess. The companies should be entitled to notice, especially since they can be compelled to cooperate with law enforcement requests to hand over user data. Those protections should hold true regardless of whether the user data sought by the U.S. government is that of Americans or non-Americans.

#### 702 is bad news—it undermines US democracy, guts foreign investment in the US, sparks data localization, and undermines cybersecurity.

Kehl, 14 (Danielle, policy analyst at New America's Open Technology Institute, “How the NSA Hurts Our Economy, Cybersecurity, and Foreign Policy” *Slate*, July 31, http://www.slate.com/blogs/future\_tense/2014/07/31/usa\_freedom\_act\_update\_how\_the\_nsa\_hurts\_our\_economy\_cybersecurity\_and\_foreign.html)

As Congress prepares for the August recess, Sen. Patrick Leahy has just introduced a new version of the USA FREEDOM Act, which aims to curb the NSA’s bulk collection and surveillance powers. Calls for immediate, serious reforms are growing louder by the day as new evidence continues to emerge about how much NSA surveillance is costing us—in terms of both the economy and our cybersecurity.¶ Intelligence and Obama administration officials have vigorously defended the NSA programs over the past year. But they have offered little hard evidence to prove the value of mass surveillance and other far-reaching NSA activity. Both the President’s Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board (PCLOB) issued extensive reports that call into question whether the benefits of the NSA’s bulk collection program carried out under Section 215 of the USA PATRIOT Act are enough to justify the tradeoffs. The PCLOB gave a more favorable outlook in the recent report on surveillance authorized under Section 702 of the FISA Amendments Act—but those findings were almost immediately called into question by a Washington Post story that revealed that nine out of 10 Internet users swept up by Section 702 surveillance are not legally targeted foreigners. And these reports don’t even begin to grapple with effects of the extensive collection taking place outside of the country under Executive Order 12333.¶ Meanwhile, evidence of the costs continues to pile up. This week, two new reports were published that demonstrate how surveillance reform is needed to protect fundamental rights here in the U.S. An in-depth study conducted by the American Civil Liberties Union and Human Rights Watch documents how mass surveillance undermines press freedom, the right to legal counsel, and other essential elements of a healthy democracy. And a separate report from New America’s Open Technology Institute examines how the NSA’s programs are bad for the U.S. economy, American foreign policy, and the security of the Internet as a whole. (Full disclosure: I am the primary author of the second paper; Future Tense is a partnership of Slate, New America, and Arizona State University.)¶ It’s easy to get caught up in the simplistic debate that often dominates the surveillance conversation: that this is about balancing national security and individual privacy. But the binary argument over security vs. privacy ignores the other negative impacts of NSA surveillance on our national interests. The U.S. cloud computing industry—a fast-growing and American-dominated market—could lose anywhere from $22 billion to $180 billion in the next few years as companies lose customers abroad and here at home. U.S. tech companies are facing declines in overseas sales due to the backlash, while foreign governments are blaming the NSA for decisions to drop American companies from huge contracts, as we’ve witnessed with Boeing in Brazil and Verizon in Germany.¶ Beyond the dollars and cents, the Snowden disclosures have accelerated data localization and data protection proposals from foreign governments that are looking for greater national control over their citizens’ info. These proposals could create significant economic and technological hurdles for American businesses: It’s both more expensive and more difficult to house servers in specific countries in order to comply with data localization laws. What’s more, mandatory data localization policies can have a negative impact on Internet freedom and the protection of human rights in countries that do not have strong local protections against surveillance. In fact, the Snowden disclosures could broadly undermine the entire U.S. Internet Freedom agenda, which was a key component of American foreign policy under Secretary of State Hillary Clinton.¶ Lastly, there’s growing evidence that certain NSA surveillance techniques are actually bad for cybersecurity. As the Institute of Electrical and Electronics Engineers recently explained: “The United States might have compromised both security and privacy in a failed attempt to improve security.”¶ We’ve learned in the past year that the NSA has been deliberately weakening the security of the Internet, including commercial products that we rely on every day, in order to improve its own spying capabilities. The agency has apparently tried everything from secretly undermining essential encryption tools and standards to inserting backdoors into widely used computer hardware and software products, stockpiling vulnerabilities in commercial software, and building a vast network of spyware inserted onto computers and routers around the world. A former U.S. ambassador to the U.N. Human Rights Council, Eileen Donahoe, wrote a forceful article back in March about how the NSA’s actions threaten our national security.¶ When you weigh these costs against the questionable benefits of the programs, the need to rein in the NSA and restore international confidence in the U.S. becomes obvious. The USA FREEDOM Act is “historic” not because it would solve all of our problems, but rather because it would be a much-needed first step in the long road to recovery from the effects of widespread NSA surveillance.¶ Future Tense is a partnership of Slate, New America, and Arizona State University.

### Surveillance 🡪 Data Localization

#### US Surveillance is modeled globally—becomes a justification for internet localization abroad.

Schneier, 15 (Bruce (2015-03-02). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (p. 106-7). W. W. Norton & Company. Kindle Edition.)

In 2010, then secretary of state Hillary Clinton gave a speech declaring Internet freedom a major US foreign policy goal. To this end, the US State Department funds and supports a variety of programs worldwide, working to counter censorship, promote encryption, and enable anonymity, all designed “to ensure that any child, born anywhere in the world, has access to the global Internet as an open platform on which to innovate, learn, organize, and express herself free from undue interference or censorship.” This agenda has been torpedoed by the awkward realization that the US and other democratic governments conducted the same types of surveillance they have criticized in more repressive countries. Those repressive countries are seizing on the opportunity, pointing to US surveillance as a justification for their own more draconian Internet policies: more surveillance, more censorship, and a more isolationist Internet that gives individual countries more control over what their citizens see and say. For example, one of the defenses the government of Egypt offered for its plans to monitor social media was that “the US listens in to phone calls, and supervises anyone who could threaten its national security.” Indians are worried that their government will cite the US’s actions to justify surveillance in that country. Both China and Russia publicly called out US hypocrisy. This affects Internet freedom worldwide. Historically, Internet governance— what little there was— was largely left to the United States, because everyone more or less believed that we were working for the security of the Internet instead of against it. But now that the US has lost much of its credibility, Internet governance is in turmoil. Many of the regulatory bodies that influence the Internet are trying to figure out what sort of leadership model to adopt. Older international standards organizations like the International Telecommunications Union are trying to increase their influence in Internet governance and develop a more nationalist set of rules. This is the cyber sovereignty movement, and it threatens to fundamentally fragment the Internet. It’s not new, but it has been given an enormous boost from the revelations of NSA spying. Countries like Russia, China, and Saudi Arabia are pushing for much more autonomous control over the portions of the Internet within their borders. That, in short, would be a disaster. The Internet is fundamentally a global platform. While countries continue to censor and control, today people in repressive regimes can still read information from and exchange ideas with the rest of the world. Internet freedom is a human rights issue, and one that the US should support. Facebook’s Mark Zuckerberg publicly took the Obama administrationto task on this, writing, “The US government should be the champion for the Internet, not a threat.” He’s right.

#### Surveillance causes data localization—Snowden leaks prove

Chander and Le 15 (Anupam, Dir California Intl Law Ctr and Prof of Law at UC Davis; and Uyen, Free Speech and Technology Fellow, California Intl Law Ctr, “Data Nationalism,” 64 Emory L.J. 677, L/N)

Beginning on June 5, 2013, the British newspaper The Guardian shocked the world with revelations that the U.S. National Security Agency (NSA) had been secretly intercepting personal data of individuals and dignitaries domestically and abroad. n169 Through internal records released by Edward Snowden, a technical specialist working for the NSA, the NSA was accused of monitoring more than thirty-five world leaders n170 and intercepting communications from more than 50,000 computer systems worldwide. n171 Anger at disclosures of U.S. surveillance abroad has led some countries to respond by attempting to keep data from leaving their shores, lest it fall into U.S. or other foreign governmental hands. For example, India's former Deputy National Security Advisor, Nehchal Sandhu, reportedly sought ways to route domestic Internet traffic via servers within the country, arguing that "such an arrangement would limit the capacity of foreign elements to scrutinize intra-India traffic." n172 The BRICS nations (Brazil, Russia, India, China, and South Africa) are seeking to establish an international network of cables that would create "a network free of US eavesdropping." n173 But does data localization in [\*715] fact stave off foreign surveillance? There are significant reasons to be skeptical of this claim.

#### Security measures in liberal states leads to data localization and authoritarianism abroad—creates a precedent for coercion and control

Chander and Le 15 (Anupam, Dir California Intl Law Ctr and Prof of Law at UC Davis; and Uyen, Free Speech and Technology Fellow, California Intl Law Ctr, “Data Nationalism,” 64 Emory L.J. 677, L/N)

Information control is central to the survival of authoritarian regimes. Such regimes require the suppression of adverse information in order to maintain their semblance of authority. This is because "even authoritarian governments allege a public mandate to govern and assert that the government is acting in the best interests of the people." n280 Information that disturbs the claim of a popular mandate and a beneficent government is thus to be eliminated at all costs. Opposition newspapers or television is routinely targeted, with licenses revoked or printing presses confiscated. The Internet has made this process of information control far more difficult by giving many dissidents the ability to use services based outside the country to share information. The Internet has made it harder, though not impossible, for authoritarian regimes to suppress their citizens from both sharing and learning information. n281 Data localization will erode that liberty-enhancing feature of the Internet.¶ The end result of data localization is to bring information increasingly under the control of the local authorities, regardless of whether that was originally intended. The dangers inherent in this are plain. Take the following cases. The official motivation for the Iranian Internet, as set forth by Iran's [\*736] head of economic affairs Ali Aghamohammadi, was to create an Internet that is "a genuinely halal network, aimed at Muslims on an ethical and moral level," which is also safe from cyberattacks (like Stuxnet) and dangers posed by using foreign networks. n282 However, human rights activists believe that "based on [the country's] track record, obscenity is just a mask to cover the government's real desire: to stifle dissent and prevent international communication." n283 An Iranian journalist agreed, "this is a ploy by the regime," which will "only allow[] [Iranians] to visit permitted websites." n284 More recently, even Iran's Culture Minister Ali Janati acknowledged this underlying motivation: "We cannot restrict the advance of [such technology] under the pretext of protecting Islamic values." n285¶ Well aware of this possibility, Internet companies have sought at times to place their servers outside the country in order to avoid the information held therein being used to target dissidents. Consider one example: when it began offering services in Vietnam, Yahoo! made the decision to use servers outside the country, perhaps to avoid becoming complicit in that country's surveillance regime. n286 This provides important context for the new Vietnamese decree mandating local accessibility of data. While the head of the Ministry of Information's Online Information Section defends Decree 72 as "misunderstood" and consistent with "human rights commitments," n287 the Committee to Protect Journalists worries that this decree will require "both local and foreign companies that provide Internet services ... to reveal the identities of users who violate numerous vague prohibitions against certain speech in Vietnamese law." n288 As Phil Robertson of Human Rights Watch argues, "This is a law that has been established for selective persecution. This [\*737] is a law that will be used against certain people who have become a thorn in the side of the authorities in Hanoi." n289¶ Data localization efforts in liberal societies thus offer cover for more pernicious efforts by authoritarian states. When Brazil's government proposed a data localization mandate, a civil society organization focused on cultural policies compared the measure to the goals of China and Iran:¶ [SEE FIGURE IN ORIGNIAL]¶ Translated, this reads as follows: "Understand this: storing data in-country is the Internet dream of China, Iran, and other totalitarian countries, but it is IMPOSSIBLE #MarcoCivil." n290¶ Thus, perhaps the most pernicious and long-lasting effect of data localization regulations is the template and precedent they offer to continue and enlarge such controls. When liberal nations decry efforts to control information by authoritarian regimes, the authoritarian states will cite our own efforts to bring data within national control. If liberal states can cite security, privacy, law enforcement, and social economic reasons to justify data controls, so can authoritarian states. Of course, the Snowden revelations of widespread U.S. surveillance will themselves justify surveillance efforts by other states. For example, Russia has begun to use NSA surveillance to justify increasing control over companies such as Facebook and Google. n291 Such rules have led critics to worry about increasing surveillance powers of the Russian state. n292 Critics caution, "In the future, Russia may even succeed in splintering the web, [\*738] breaking off from the global Internet a Russian intranet that's easier for it to control." n293 Even though officials describe such rules as being antiterrorist, others see a more sinister motive. The editor of Agentura.ru, Andrei Soldatov, believes that Zheleznyak's proposal is motivated by the government's desire to control internal dissent. n294 Ivan Begtin, the director of the group Information Culture, echoes this, arguing that Zheleznyak's surveillance power "will be yet another tool for controlling the Internet." n295 Begtin warns, "In fact, we are moving very fast down the Chinese path." n296¶ Finally, creating a poor precedent for more authoritarian countries to emulate is not the only impact on liberty of data localization by liberal states. Even liberal states have used surveillance to undermine the civil rights of their citizens and residents. n297 The proposal for a German "Internetz" has drawn worries that national routing would require deep packet inspection, raising fears of extensive surveillance. n298 The newspaper Frankfurter Allgemeine argues that not only would a state-sanctioned network provide "no help against spying," it would lead to "a centralization of surveillance capabilities" for German spy agencies. n299 India's proposed localization measures in combination with the various surveillance systems in play - including Aadhaar, CMS, National Intelligence Grid (Natgrid), and Netra - have raised concerns for human rights, including freedom of expression. n300

#### Surveillance causes data localization—Brazil proves

Etzioni 15 (Amitai, Prof of Sociology at George Washington University, “Do Tech Companies Owe It to the Public to Cooperate With Surveillance?” *The Atlantic*, MAR 9, 2015, http://www.theatlantic.com/politics/archive/2015/03/tech-companies-owe-it-to-the-public-to-cooperate-with-surveillance/387094/)

The Snowden revelations greatly troubled the corporations involved for more reasons than one. Some nations, like Brazil, considered setting up their own versions of the Internet to protect their citizens from American snooping—a move that would harm the business of companies such as Google and Facebook that greatly benefit from the unified World Wide Web. (Google is used by 1.17 billion people worldwide, while 1.35 billion use Facebook.) These same corporations also feared that Americans would stop using their services if they felt that their privacy was compromised. Many of their CEOs hold the libertarian view that that government regulations are a costly burden and that the government that governs least governs best. And they still seem to hold on to the vision that cyberspace is a new world that can govern itself.

### Data Localization X Growth

#### Data localization kills economic growth and job creation

Business Roundtable 2012 (The Business Roundtable (BRT) is a group of chief executive officers of major U.S. corporations formed to promote pro-business public policy, “Promoting Smart Economic Growth through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements,” July 2012, http://businessroundtable.org/sites/default/files/legacy/uploads/studies-reports/downloads/Global\_IT\_Policy\_Paper\_final.pdf)

This paper builds on the BRT plan by closely examining one critical and actionable aspect of global information technology (IT) policy: the growing international risk of government-imposed limits on cross-border data services through local data server requirements. This trend is bad for U.S. technology and commerce and, in turn, bad for economic growth and job creation. This paper recommends concrete actions that the U.S. government and BRT companies can take to oppose these requirements wherever they arise.¶ For decades, the United States has led the world in advocating policies that open markets and reduce regulatory barriers to commerce. Such policies are all the more important today given the integration of networked technologies into global business models and the positive impact these business models have on the creation of U.S. jobs and economic growth. Globally networked technologies, such as the Internet, cloud computing, virtual private networks and mobile commerce, are critical to modern business. These cross-border network technologies have created the most profound platform for worldwide commerce in history.¶ BRT and our members are concerned about a dangerous trend we are experiencing as we conduct business around the world. Governments are beginning to erect new counterproductive, overreaching regulatory barriers to services that rely on cross-border, information-driven business models. We want to raise awareness of the potential damage these policies could cause, and we encourage business and government to work together to implement policies to mitigate such risks.¶ BRT is focusing first on the emerging trend of local data server requirements, i.e., requirements to mandate server infrastructure within the borders of a country, rather than allowing businesses to use servers located in other countries. Such policies are disruptive and an unnecessary drain on resources. They can fragment the unified, economically efficient and technologically flexible nature of global networks such as the Internet. We want to work with the U.S. government to identify these threats and to advance practices that minimize the barriers to open markets here at home and work with other governments to adopt the best practices embodied in the E.U.- U.S. Trade Principles for Information and Communication Technology Services.1￼￼￼￼

#### Data localization guts economic growth

Business Roundtable 2012 (The Business Roundtable (BRT) is a group of chief executive officers of major U.S. corporations formed to promote pro-business public policy, “Promoting Smart Economic Growth through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements,” July 2012, http://businessroundtable.org/sites/default/files/legacy/uploads/studies-reports/downloads/Global\_IT\_Policy\_Paper\_final.pdf)

Local data server requirements hurt economic productivity¶ and dramatically undercut the efficiencies and scalability made possible by cloud computing and networked technologies.¶Local data server requirements hurt economic productivity and dramatically undercut the efficiencies and scalability made possible by cloud computing and networked technologies. The disruption caused by such requirements can undercut the ability to conduct business with a country and shut out any business that does not have an existing large, local presence. At times, these measures serve to protect local interests at the expense of international competition. Such restrictions may make it more difficult to integrate even large countries into the global supply chain and may stifle the deployment of cutting-edge innovative services to the detriment of consumers.¶ The negative impact of local data server requirements on productivity, efficiency and scalability manifests itself in higher operating costs for business. To comply with restrictive policies, businesses may endure increased capital costs — for example, the purchasing of additional servers. The policies further burden businesses because capital expenditures such as server purchases require new operational spending on software licenses, additional employees and additional hardware.

#### Data localization stifles economic growth and makes recover from the current financial crisis impossible

Business Roundtable 2012 (The Business Roundtable (BRT) is a group of chief executive officers of major U.S. corporations formed to promote pro-business public policy, “Promoting Smart Economic Growth through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements,” July 2012, http://businessroundtable.org/sites/default/files/legacy/uploads/studies-reports/downloads/Global\_IT\_Policy\_Paper\_final.pdf)

Local data server requirements have negative consequences for countries’ economic growth.¶ Companies from more closed markets will have an unearned advantage in profiting from the coming services and infrastructure boom if the governments of more open markets do not press for standards against barriers such as local server data requirements.¶ When governments impose blanket restrictions on trade such as local data server requirements, they fight the battle for economic growth with one hand tied behind their backs. The service economy accounts for nearly 70 percent of both world economic output and world employment, and yet these barriers restrict¶ the potential of businesses to deliver increased productivity¶ and growth at a time of a crucial, fragile economic recovery in much of the developed world. When trade barriers disrupt the free flow of lawful information, they can result in a slowing of technological innovation and prevent companies from offering certain products and services, consequently dampening economic growth.¶ These restrictions on services trade also have a negative impact on growth specifically in developing countries. Services trade is a conduit for leapfrogging the traditional path of economic development (the “agriculture¶ to manufacturing to services” model). In the 21st century, nations have the potential to advance directly into services at an internationally competitive level, due to the scalability and efficiency of IT platforms such as the Internet and other global networks. But barriers such as local data server requirements limit these prospects.¶ We are concerned that the disruptions that local data server requirements and other services trade barriers bring to global economic growth are set to increase. Experts expect a coming boom in services and infrastructure spending as the world moves beyond the financial crisis. However, barriers to services trade will diminish the potential for growth. Additionally, because services trade policies differ across countries, some countries’ potential for growth will be affected more negatively. The United States and the European Union are mostly open, while several of the developing nations are not. Companies from more closed markets will have an unearned advantage in profiting from the coming services and infrastructure boom if the governments of more open markets do not press for standards against barriers such as local server data requirements.

### Data Localization X Trade

#### Data localization undermines privacy and security, poses a mortal threat to international trade and increases costs and burdens

Chander and Le 15 (Anupam, Dir California Intl Law Ctr and Prof of Law at UC Davis; and Uyen, Free Speech and Technology Fellow, California Intl Law Ctr, “Data Nationalism,” 64 Emory L.J. 677, L/N)

The era of a global Internet may be passing. Governments across the world are putting up barriers to the free flow of information across borders. Driven by concerns over privacy, security, surveillance, and law enforcement, governments are erecting borders in cyberspace, breaking apart the World Wide Web. The first generation of Internet border controls sought to keep information out of a country - from Nazi paraphernalia to copyright infringing material. n1 The new generation of Internet border controls seeks not to keep information out but rather to keep data in. Where the first generation was relatively narrow in the information excluded, the new generation seeks to keep all data about individuals within a country.¶ Efforts to keep data within national borders have gained traction in the wake of revelations of widespread electronic spying by United States intelligence agencies. n2 Governments across the world, indignant at the recent disclosures, have cited foreign surveillance as an argument to prevent data from leaving their borders, allegedly into foreign hands. n3 As the argument [\*680] goes, placing data in other nations jeopardizes the security and privacy of such information. We define "data localization" measures as those that specifically encumber the transfer of data across national borders. These measures take a wide variety of forms - including rules preventing information from being sent outside the country, rules requiring prior consent of the data subject before information is transmitted across national borders, rules requiring copies of information to be stored domestically, and even a tax on the export of data. We argue here that data localization will backfire and that it in fact undermines privacy and security, while still leaving data vulnerable to foreign surveillance. Even more importantly, data localization increases the ability of governments to surveil and even oppress their own populations.¶ Imagine an Internet where data must stop at national borders, examined to see whether it is allowed to leave the country and possibly taxed when it does. While this may sound fanciful, this is precisely the impact of various measures undertaken or planned by many nations to curtail the flow of data outside their borders. Countries around the world are in the process of creating Checkpoint Charlies - not just for highly secret national security data but for ordinary data about citizens. The very nature of the World Wide Web is at stake. We will show how countries across the world have implemented or have planned dramatic steps to curtail the flow of information outside their borders. By creating national barriers to data, data localization measures break up the World Wide Web, which was designed to share information across the globe. n4 The Internet is a global network based on a protocol for interconnecting computers without regard for national borders. Information is routed across this network through decisions made autonomously and automatically at local routers, which choose paths based largely on efficiency, unaware of political borders. n5 Thus, the services built on the Internet, from email to the World [\*681] Wide Web, pay little heed to national borders. Services such as cloud computing exemplify this, making the physical locations for the storage and processing of their data largely invisible to users. Data localization would dramatically alter this fundamental architecture of the Internet.¶ Such a change poses a mortal threat to the new kind of international trade made possible by the Internet - information services such as those supplied by Bangalore or Silicon Valley. n6 Barriers of distance or immigration restrictions had long kept such services confined within national borders. But the new services of the Electronic Silk Road often depend on processing information about the user, information that crosses borders from the user's country to the service provider's country. Data localization would thus require the information service provider to build out a physical, local infrastructure in every jurisdiction in which it operates, increasing costs and other burdens enormously for both providers and consumers and rendering many of such global services impossible.

### Data Localization X Tech

#### Data localization kills tech innovation

Chander and Le 15 (Anupam, Dir California Intl Law Ctr and Prof of Law at UC Davis; and Uyen, Free Speech and Technology Fellow, California Intl Law Ctr, “Data Nationalism,” 64 Emory L.J. 677, L/N)

Data localization requirements also interfere with the most important trends in computing today. They limit access to the disruptive technologies of the future, such as cloud computing, the "Internet of Things," and data-driven innovations (especially those relying on "big data"). Data localization sacrifices the innovations made possible by building on top of global Internet platforms based on cloud computing. This is particularly important for entrepreneurs operating in emerging economies that might lack the infrastructure already developed elsewhere. And it places great impediments to the development of both the Internet of Things and big data analytics, requiring costly separation of data by political boundaries and often denying the possibility of aggregating data across borders. We discuss the impacts on these trends below.¶ Cloud Computing. Data localization requirements will often prevent access to global cloud computing services. As we have indicated, while governments assume that global services will simply erect local data server farms, such hopes are likely to prove unwarranted. Thus, local companies will be denied access to the many companies that might help them scale up, or to go global. n247 Many companies around the world are built on top of existing global services. Highly successful companies with Indian origins such as Slideshare and Zoho relied on global services such as Amazon Web Services and Google Apps. n248 A Slideshare employee cites the scalability made possible by the use of Amazon's cloud services, noting, "Sometimes I need 100 servers, sometimes I only need 10." n249 A company like Zoho can use Google Apps, while at the same time competing with Google in higher value-added services. n250 [\*729] Accessing such global services thus allows a small company to maintain a global presence without having to deploy the vast infrastructure that would be necessary to scale as needed.

#### Data localization kills competition, innovation, and productivity

Chander and Le 15 (Anupam, Dir California Intl Law Ctr and Prof of Law at UC Davis; and Uyen, Free Speech and Technology Fellow, California Intl Law Ctr, “Data Nationalism,” 64 Emory L.J. 677, L/N)

Data Driven Innovation (Big Data). Many analysts believe that data-driven innovations will be a key basis of competition, innovation, and productivity in the years to come, though many note the importance of protecting privacy in the process of assembling ever-larger databases. n258 McKinsey even reclassifies data as a new kind of factor of production for the Information Age. n259 Data localization threatens big data in at least two ways. First, by limiting data aggregation by country, it increases costs and adds complexity to the collection and maintenance of data. Second, data localization requirements can reduce the size of potential data sets, eroding the informational value that can be gained by cross-jurisdictional studies. Large-scale, global experiments technically possible through big data analytics, especially on the web, may have to give way to narrower, localized studies. Perhaps anonymization will suffice to comport with data localization laws and thus still permit cross-border data flow, but this will depend on the specifics of the law.

### AT: Data Localization Good

#### There’s just no benefit to data localization—it doesn’t help law enforcement track criminals

Chander and Le 15 (Anupam, Dir California Intl Law Ctr and Prof of Law at UC Davis; and Uyen, Free Speech and Technology Fellow, California Intl Law Ctr, “Data Nationalism,” 64 Emory L.J. 677, L/N)

[\*732] After a draft of this paper was made available online, we learned that the United States government has, on occasion, exercised its authority to review foreign investments into United States telecommunications infrastructure to require data localization from some of the telecommunications companies. n266 The obligations seem to have arisen as part of the informal "Team Telecom" review of such investments. Team Telecom consists in representatives from the Departments of Justice, Defense, and Homeland Security, as well as the Federal Bureau of Investigation. n267 The inconsistent and varying nature of these obligations - sometimes requiring only prior notice for the use of a foreign service and other times requiring data storage in the United States - suggests that the law enforcement needs are exaggerated. There is no reason to suspect that a criminal is more likely to use one telecommunications provider over another.¶ Equally important, it seems unlikely that data localization will prove an effective means to ensure that data about their residents is available to law enforcement personnel when they want it. Moreover, other alternatives are reasonably available to assist law enforcement access to data - alternatives that are both less trade restrictive and more speech-friendly than data localization.¶ Data localization will not necessarily provide law enforcement better access to a criminal's data trail because localization requirements are extremely hard to enforce. They might simply end up driving potential wrongdoers abroad to less compliant and more secretive services. Indeed, the most law-abiding companies will follow costly data localization rules, while others will simply ignore them, comforted by the knowledge that such laws are difficult to enforce. Any success with gaining information from these companies will likely prove temporary, as, over time, potential scofflaws will become aware of the monitoring and turn to services that intentionally skirt the law. The services avoiding the law will likely be foreign ones, lacking any [\*733] personnel or assets on the ground against which to enforce any sanction. Thus, understood dynamically, the data localization requirement will only hamper local and law-abiding enterprises, while driving some citizens abroad.

#### There’s no uniqueness to your law enforcement turn—most countries have the authority to compel corporations to share data

Chander and Le 15 (Anupam, Dir California Intl Law Ctr and Prof of Law at UC Davis; and Uyen, Free Speech and Technology Fellow, California Intl Law Ctr, “Data Nationalism,” 64 Emory L.J. 677, L/N)

Law enforcement is, without doubt, a laudable goal, so long as the laws themselves do not violate universal human rights. Many governments already have authority under their domestic laws to compel a company operating in their jurisdictions to share data of their nationals held by that company abroad. A recent study of ten countries concluded that the government already had the right to access data held extraterritorially in the cloud in every jurisdiction examined. n268 Although the process varied, "every single country ... vests authority in the government to require a Cloud service provider to disclose customer data in certain situations, and in most instances this authority enables the government to access data physically stored outside the country's borders." n269¶ Even if companies refuse to comply with such orders, or if the local subsidiary lacks the authority to compel its foreign counterpart to share personal data, governments can resort to information-sharing agreements. For example, the Convention on Cybercrime, which has been ratified by forty-four countries including the United States, France, and Germany, n270 obliges Member States to adopt and enforce laws against cybercrimes and to provide "mutual assistance" to each other in enforcing cyberoffenses. n271 Many states have entered into specific Mutual Legal Assistance Treaties (MLATs) with foreign nations. These treaties establish a process that protects the rights of [\*734] individuals yet gives governments access to data held in foreign jurisdictions. Currently, the United States has MLATs in force with fifty-six countries. n272 The United States also entered into a Mutual Legal Assistance Agreement (MLAA) with China and Taiwan. n273 All the countries discussed in the country studies above, with the exception of Indonesia, Kazakhstan, and Vietnam, have MLAT arrangements in force with the United States. Generally, MLATs "specify which types of requested assistance must be provided, and which may be refused." n274 Requests for assistance may be refused typically when the execution of such request would be prejudicial to the state's security or public interest; the request relates to a political offense; there is an absence of reasonable grounds; the request does not conform to the MLAT's provisions; or the request is incompatible with the requested state's law. n275 The explanatory notes to the MLAT between the United States and the European Union observe that a request for data shall only be denied on data protection grounds in "exceptional cases." n276 At the same time, there are procedural requirements to help ensure that the information gathering is supporting a proper governmental investigation. For example, Article 17 of the U.S.-Germany MLAT provides that the government requesting assistance must do [\*735] so in writing and must specify the evidence or information sought, authorities involved, applicable criminal law provisions, etc. n277

### Data Globalization 🡪 Growth

#### Data globalization creates new markets, promotes business development, bolsters small business, lowers costs, and creates econ growth.

Business Roundtable 2012 (The Business Roundtable (BRT) is a group of chief executive officers of major U.S. corporations formed to promote pro-business public policy, “Promoting Smart Economic Growth through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements,” July 2012, http://businessroundtable.org/sites/default/files/legacy/uploads/studies-reports/downloads/Global\_IT\_Policy\_Paper\_final.pdf)

III.Threats Posed by Local Data Server Requirements to the Benefits of Global Operating Models¶ The advent of cross-border networked technologies, such as cloud computing and mobile commerce, has enabled a new age of global efficiency.¶ Network-based technological developments have enabled companies to virtualize their data storage and processing facilities and scale them as needed to service global markets, without replicating the infrastructure in every market where they have a supplier or customer. These scalable systems lower capital risk, expedite transaction processing, facilitate innovation, and make it easier to bring services to new markets quickly and efficiently. Such systems do not foreclose local investments. In fact, by integrating countries into a seamless global network and expediting the provision of services to global markets, networked operations can spur the development of local businesses that consume such services and enhance consumer welfare.¶ Open markets and globally networked technologies are critical to the success of U.S. businesses of all sizes and across economic sectors.¶ Even in the current global economic environment, U.S. business excels due to its ability to harness the efficiency gains made possible by network-based technologies such as cloud computing and centralized processing centers. Network-based technologies are critically important to businesses as diverse as electronic retailers, search engines, financial services, insurance, logistics and transportation, social networks, energy suppliers and utilities, web hosting providers, registrars, and technology infrastructure and service providers that rely on the Internet and other global telecom networks. Universities, research institutions, hospitals and other organizations also rely on unified technology platforms.¶ Networked technologies are also essential to small businesses, nonprofits and entrepreneurs. Thanks to the Internet and advances in technology, small companies, nongovernmental organizations and individuals can customize and rapidly scale their services at a lower cost and collaborate globally. Improved access to networked technologies also creates new opportunities for entrepreneurs and innovators to design applications and to extend their reach to new international customers.¶ But the very future of these globally networked technologies and the efficiency- based cross-border services business models they support are at risk.¶ These beneficial technologies will not thrive if unwarranted regulatory barriers impede them. Unfortunately, a growing number of countries are adopting or considering such barriers. One example is the requirement to locate data servers locally. Local data server requirements mandate that businesses use in-country servers and storage facilities to host all data that flow into and out of that country. In the most extreme examples, the requirements prohibit storage of data concerning a country’s nationals on any server outside the country.

### We Solve Data Localization

#### US leadership is key to rolling back data localization

Business Roundtable 2012 (The Business Roundtable (BRT) is a group of chief executive officers of major U.S. corporations formed to promote pro-business public policy, “Promoting Smart Economic Growth through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements,” July 2012, http://businessroundtable.org/sites/default/files/legacy/uploads/studies-reports/downloads/Global\_IT\_Policy\_Paper\_final.pdf)

Sustained and credible U.S. leadership and multilateral collaboration are necessary to protect against blanket local data server requirements. BRT recognizes the good work of the United States and other key trading partners in negotiating well-crafted policies that address the integrated nature of today’s global economy. We want to work with the U.S. government to promote further acceptance and implementation of these principles.¶ The E.U.-U.S. Trade Principles for Information and Communication Technology Services and the OECD Principles for Internet Policy-Making provide a solid foundation for advocating against local data server requirements. In relevant part, they state:¶ The E.U.-U.S. Trade Principles for Information and Communication Technology Services — “Local Infrastructure”: Governments should not require ICT service suppliers to use local infrastructure, or establish a local presence, as a condition of supplying services.¶ The OECD Principles for Internet Policy-Making — “Promoting and Enabling the Cross-Border Delivery of Services”: Suppliers should have the ability to supply services over the Internet on a cross- border and technologically neutral basis in a manner that promotes interoperability of services and technologies, where appropriate. Users should have the ability to access and generate lawful content and run applications of their choice. To ensure cost effectiveness and other efficiencies, other barriers to the location, access and use of cross-border data facilities and functions should be minimized, providing that appropriate data protection and security measures are implemented in a manner consistent with the relevant OECD Guidelines and reflecting the necessary balance among all fundamental rights, freedoms and principles.¶ BRT and the U.S. government can work together to implement these policy principles and assess disruptive market and policy trends. As an initial step to doing so, we have chosen to focus on the very real operating impacts that come from a growth in local data server requirements. At the same time, we realize that to be fully successful with other countries, the United States must lead by example and must have a best-practice and consistent position on these matters.¶ A clearly articulated U.S. position on the appropriate way to minimize barriers to data server location will allow the United States to advance its position that the unimpeded, free flow of cross-border data is of fundamental importance to the economic competitiveness of U.S. business, as well as business communities and societies around the world.

### Debt Bad

#### We are about to hit the debt limit

Department of treasury 3/17/2015 (http://www.treasury.gov/initiatives/Pages/debtlimit.aspx)

The debt limit is the total amount of money that the United States government is authorized to borrow to meet its existing legal obligations, including Social Security and Medicare benefits, military salaries, interest on the national debt, tax refunds, and other payments. The debt limit does not authorize new spending commitments. It simply allows the government to finance existing legal obligations that Congresses and presidents of both parties have made in the past. Failing to increase the debt limit would have catastrophic economic consequences. It would cause the government to default on its legal obligations – an unprecedented event in American history. That would precipitate another financial crisis and threaten the jobs and savings of everyday Americans – putting the United States right back in a deep economic hole, just as the country is recovering from the recent recession. Congress has always acted when called upon to raise the debt limit. Since 1960, Congress has acted 78 separate times to permanently raise, temporarily extend, or revise the definition of the debt limit – 49 times under Republican presidents and 29 times under Democratic presidents. In the coming weeks, Congress must act to increase the debt limit. Congressional leaders in both parties have recognized that this is necessary. Recently, however, a number of myths about this issue have begun to surface.

#### Hitting the debt limit would be catastrophic

Berman 13 (Matt is an assistant managing editor at National Journal. Before joining National Journal, he managed social media on the communications team at the Carnegie Endowment for International Peace. October 7, 2013 http://www.nationaljournal.com/domesticpolicy/americans-don-t-get-how-bad-hitting-the-debt-ceiling-would-be-20131007)

No one knows exactly what will happen if the United States passes the deadline for raising the debt limit on Oct. 17. That includes the Treasury Department, which calls a possible breach economically "catastrophic." But that characterization is not stopping 39 percent of Americans from thinking that there's nothing major to fear. That fact alone should be terrifying. A new poll from Pew shows that, while 47 percent of Americans think raising the debt ceiling is "absolutely essential to avoid crisis," 54 percent of Republicans, 28 percent of Democrats, and 38 percent of independents think the U.S. can go past the deadline "without major problems." Just 36 percent of Republicans think raising the limit is crucial. The 39 percent of Americans who think exceeding the deadline would be no big deal are likely very, very wrong. For now, the Treasury has set the deadline at Oct. 17. After that point, the government will just have $30 billion cash-on-hand to meet its obligations. By Nov. 1, those obligations would include $18 billion in Medicare payments, $25 billion in Social Security payments, and $12 billion in military payments. Failing to make those payments alone sounds really, really bad. But this wouldn't just impact the people reliant on government money. Failure by the world's largest borrower to pay its debt -- unprecedented in modern history -- will devastate stock markets from Brazil to Zurich, halt a $5 trillion lending mechanism for investors who rely on Treasuries, blow up borrowing costs for billions of people and companies, ravage the dollar, and throw the U.S. and world economies into a recession that probably would become a depression. Among the dozens of money managers, economists, bankers, traders, and former government officials interviewed for this story, few view a U.S. default as anything but a financial apocalypse. Another way of looking at the impact on the global economy, as they put it, is as an immediate economic crisis that's, at a minimum, way larger than anything faced in the fall of 2008. But as long as a sizable number of Americans—and a majority of Republicans—view default as something less than toxic, the possibility of default remains.

## Advantage 2 Extensions

### Surveillance Bad-Democracy

#### Surveillance trades off with freedom and democracy—it alters the relationship between citizen and government by creating a panoptic environment of control

Schneier, 15 (Bruce (2015-03-02). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (p. 95-7). W. W. Norton & Company. Kindle Edition.)

Surveillance has a potentially enormous chilling effect on society. US Supreme Court Justice Sonia Stomayor recognized this in herconcurring opinion in a 2012 case about the FBI’s installing a GPS tracker in someone’s car. Her comments were much broader: “Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring— by making available at a relatively low cost such a substantial quantity of intimate information about any person whom the Government, in its unfettered discretion, chooses to track— may ‘alter the relationship between citizen and government in a way that is inimical to democratic society.’ ” Columbia University law professor Eben Moglen wrote that “omnipresent invasive listening creates fear. And that fear is the enemy of reasoned, ordered liberty.” Surveillance is a tactic of intimidation. In the US, we already see the beginnings of this chilling effect. According to a Human Rights Watch report, journalists covering stories on the intelligence community, national security, and law enforcement have been significantly hampered by government surveillance. Sources are less likely to contact them, and they themselves are worried about being prosecuted. Human Rights Watch concludes that stories in the national interest that need to be reported don’t get reported, and that the public is less informed as a result. That’s the chilling effect right there. Lawyers working on cases where there is some intelligence interest— foreign government clients, drugs, terrorism— are also affected. Likejournalists, they worry that their conversations are monitored and that discussions with their clients will find their way into the prosecution’s hands. Post-9/ 11 surveillance has caused writers to self-censor. They avoid writing about and researching certain subjects; they’re careful about communicating with sources, colleagues, or friends abroad. A Pew Research Center study conducted just after the first Snowden articles were published found that people didn’t want to talk about the NSA online. A broader Harris poll found that nearly half of Americans have changed what they research, talk about, and write about because of NSA surveillance. Surveillance has chilled Internet use by Muslim Americans, and by groups like environmentalists, gun-rights activists, drug policy advocates, and human rights workers. After the Snowden revelations of 2013, people across the world were less likely to search personally sensitive terms on Google. A 2014 report from the UN High Commissioner on Human Rights noted, “Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association.” This isn’t paranoia. In 2012, French president Nicolas Sarkozy said in a campaign speech, “Anyone who regularly consults internet sites which promote terror or hatred or violence will be sentenced to prison.” This fear of scrutiny isn’t just about the present; it’s about the past as well. Politicians already live in a world where the opposition followsthem around constantly with cameras, hoping to record something that can be taken out of context. Everything they’ve said and done in the past is pored through and judged in the present, with an exactitude far greater than was imaginable only a few years ago. Imagine this being normal for every job applicant. Of course, surveillance doesn’t affect everyone equally. Some of us are unconcerned about government surveillance, and therefore not affected at all. Others of us, especially those of us in religious, social, ethnic, and economic groups that are out of favor with the ruling elite, will be affected more. Jeremy Bentham’s key observation in conceiving his panopticon was that people become conformist and compliant when they believe they are being observed. The panopticon is an architecture of social control. Think of how you act when a police car is driving next to you, or how an entire country acts when state agents are listening to phone calls. When we know everything is being recorded, we are less likely to speak freely and act individually. When we are constantly under the threat of judgment, criticism, and correction for our actions, we become fearful that— either now or in the uncertain future— data we leave behind will be brought back to implicate us, by whatever authority has then become focused upon our once-private and innocent acts. In response, we do nothing out of the ordinary. We lose our individuality, and society stagnates. We don’t question or challenge power. We become obedient and submissive. We’re less free.

#### **Surveillance crushes liberty—even The Economist agrees**

Schneier, 15 (Bruce (2015-03-02). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (pp. 91-92). W. W. Norton & Company. Kindle Edition.)

The biggest cost is liberty, and the risk is real enough that people across political ideologies are objecting to the sheer invasiveness and pervasiveness of the surveillance system. Even the politically conservative and probusiness Economist magazine argued, in a 2013 editorial about video surveillance, that it had gone too far: “This is where one of this newspaper’s strongly held beliefs that technological progress should generally be welcomed, not feared, runs up against an even deeper impulse, in favour of liberty. Freedom has to include some right to privacy: if every move you make is being chronicled, liberty is curtailed.”

#### **Government big data is an anathema to a democratic, liberal society**

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

To be clear, the following is not an apologia for data gathering in service of national security or commercial interests. State and corporate invasions of individual privacy have clear and much-discussed costs for society. n27 And needless to say, the government's unprecedented level of secret, suspicionless monitoring of personal communication raises myriad legal, political, and philosophical issues. We think the practice is anathema to a liberal, open democracy and inconsistent with the framework and rights protections of the U.S. Constitution.

### **Surveillance Bad-4th Amendment**

#### Current NSA mass surveillance violates a host of constitutional provisions

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

Largely due to the disclosures of Edward Snowden, the nation is now engaged in a wide-ranging discussion about the balance between national security and individual privacy. The responses include major reports, n9 several legal challenges, n10 numerous congressional hearings, n11 and a high-profile presidential address. n12 These contributions often point in different directions, sparking objections and further controversies. n13 There is disagreement not only about what should be done but also as to the factual predicates for decision making, including whether the NSA's programs have prevented acts of terrorism. n14 [\*984] What is largely missing from the debate, however, is any discussion of the consequences of mass surveillance for the rights of those accused and convicted of crime.¶ In trying to bolster the argument for one controversial surveillance statute, a federal lawmaker cited a series of criminal cases as proof that the law was effective at thwarting terrorism. n15 As it turns out, the defendants in those cases had not been notified that the NSA's programs provided information in the underlying criminal investigations. n16 Later revelations showed that the government has been engaged in a long-term ruse in which law enforcement covers up the source of information provided by the intelligence community. n17 This strikes at the heart of the American criminal justice system and likely violates a number of constitutional provisions.

### Surveillance Bad-Terrorism

#### U.S. Surveillance Lead to Chinese Cyber Tension

Clayton 14 (Mark, “ Five overlooked cos of the NSA surveillance Flap”. Christian Science Monitor. January 12)

White House momentum to finally begin dealing with Chinese cyber-espionage aimed at US corporations has largely dissipated since the document leaks, analysts say. One key casualty: less enthusiasm among US allies to cooperate with America, especially now that it's known that the NSA monitored the phone communications of top political leaders in Germany, France, Spain, and Brazil. "I don't really think we're going to make a lot of progress for a while," James Mulvenon, vice president of Defense Group Inc.'s intelligence division, said at a government roundtable in July on US-China cybersecurity issues. "I would say it [the flap over NSA activity] is probably going to delay progress six to 12 months." The US and China are still holding bilateral talks about corporate cyber-espionage, but there is little progress to report. "Our goal was to convince the Chinese that, hey, in cyberspace it's not appropriate for a nation-state to use its technical capabilities to rip off intellectual property and use it to benefit its national companies," Mr. Finan says. "That's a relatively nuanced argument that I am sure is still being made in bilateral discussions. But in order for those to take root and gain ground, they have to have public pressure, including support from US allies. Unfortunately, that level of nuance has been lost in the noise around Snowden." The timing of the revelations was most unfortunate for the US. The Obama administration had been poised to intensify efforts to crack down on Chinese cyberspying, after security firm Mandiant revealed in February 2013 that a group tied to China's military, dubbed APT1, had infiltrated corporate computer networks and stolen data from at least 141 companies spanning 20 industries since 2006. Of the targeted companies, 115 are in the US. Such theft is not peanuts. It amounts to about $300 billion a year, according to the Commission on the Theft of American Intellectual Property. That organization is spearheaded by Dennis Blair, a former director of national intelligence, and Jon Huntsman Jr., a former US ambassador to China. China is responsible for at least half of the data theft, the group reports. By March, the Obama administration had confronted China about cyberstealing, and in early June President Obama reportedly reiterated US concerns to Chinese President Xi Jinping during a "working visit." But the White House needs Congress to put a spur to the Chinese to encourage cooperation, and legislation to do that has been shoved down the agenda while lawmakers focus instead on whether and how to rein in the NSA. One Senate bill, for instance, would have created a "watch list" of countries engaged in cyberspying – and allowed the president to block imports of classes of goods if the foreign companies providing those goods have benefited from stolen US technology or proprietary information. "There was talk [in Congress] about putting visa restrictions on individual hackers or even financial sanctions" on offending nations, says Adam Segal, a senior fellow at the Council on Foreign Relations (CFR), in a phone interview. "That's all lost steam as everyone struggles to deal with the Snowden revelations."

### Surveillance Bad-Soft Power

#### U.S. Soft Power Decreased By Leaks

Clayton 14 (Mark, “ Five overlooked cos of the NSA surveillance Flap”. Christian Science Monitor. January 12)

The NSA-Snowden episode has undermined US arguments on the international stage in favor of wide access to information via the Internet and against censorship and government surveillance of citizens, experts in the US say. Though the Internet operates largely in accordance with those American principles, other nations – such as China, Russia, and some Arab states – advocate greater government control over the flow of information on the World Wide Web and access to it. "To many other countries, cybersecurity is all about governments protecting themselves from what people might be saying about them," says Mr. Borg of the US Cyber Consequences Unit. "Many want to clamp down on Internet freedoms. Doing so means wresting control of it from Americans and organizations set up by America. Snowden's revelations have given them a lot of ammunition to do that." Broad repudiation of the US position could result in an Internet that is less open than it is today, and more geared toward surveillance. "There's been this pressure for a long time," Segal says. The US has "argued the current system works and beyond expectations – and not to mess it up. But those arguments aren't going to be very powerful any longer."

### Surveillance Bad-Social Control

#### **Surveillance is a form of intimidation and social control**

Schneier, 15 (Bruce (2015-03-02). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (p. 2). W. W. Norton & Company. Kindle Edition.)

Governments also use this same data for intimidation and social control. In 2014, the government of Ukraine sent this positively Orwellian text message to people in Kiev whose phones were at a certain place during a certain time period: “Dear subscriber, you have been registered as a participant in a mass disturbance.” Don’t think this behavior is limited to totalitarian countries; in 2010, Michigan police sought information about every cell phone in service near an expected labor protest. They didn’t bother getting a warrant first. There’s a whole industry devoted to tracking you in real time. Companies use your phone to track you in stores to learn how you shop, track you on the road to determine how close you might be to a particular store, and deliver advertising to your phone based on where you are right now.

#### **Our current surveillance state has perfected panopticism in a regime of constant surveillance that remains ubiquitous and unquestioned.**

Schneier, 15 (Bruce (2015-03-02). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (p. 32). W. W. Norton & Company. Kindle Edition.)

Philosopher Jeremy Bentham conceived of his “panopticon” in the late 1700s as a way to build cheaper prisons. His idea was a prison where every inmate could be surveilled at any time, unawares. The inmate would have no choice but to assume that he was always being watched, and would therefore conform. This idea has been used as a metaphor for mass personal data collection, both on the Internet and off. On the Internet, surveillance is ubiquitous. All of us are being watched, all the time, and that data is being stored forever. This is what an information-age surveillance state looks like, and it’s efficient beyond Bentham’s wildest dreams.

#### **Ubiquitous surveillance yields a police state**

Schneier, 15 (Bruce (2015-03-02). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (p. 92-4). W. W. Norton & Company. Kindle Edition.)

In the 17th century, the French statesman Cardinal Richelieu famously said, “Show me six lines written by the most honest man in the world, and I will find enough therein to hang him.” Lavrentiy Beria, head of Joseph Stalin’s secret police in the old Soviet Union, declared, “Show me the man, and I’ll show you the crime.” Both were saying the same thing: if you have enough data about someone, you can find sufficient evidence to find him guilty of something. It’s the reason many countries’ courts prohibit the police from engaging in “fishing expeditions.” It’s the reason the US Constitution specifically prohibits general warrants— documents that basically allow the police to search for anything. General warrants can be extremely abusive; they were used by the British in colonial America as a form of social control. Ubiquitous surveillance means that anyone could be convicted of lawbreaking, once the police set their minds to it. It is incredibly dangerous to live in a world where everything you do can be stored and brought forward as evidence against you at some later date. There is significant danger in allowing the police to dig into these large data sets and find “evidence” of wrongdoing, especially in a country like the US with so many vague and punitive laws, which give prosecutors discretion over whom to charge with what, and with overly broad material witness laws. This is especially true given the expansion of the legally loaded terms “terrorism,” to include conventional criminals, and “weapons of mass destruction,” to include almost anything, including a sawed-off shotgun. The US terminology is so broad that someone who donates $ 10 to Hamas’s humanitarian arm could be considered a terrorist. Surveillance puts us at risk of abuses by those in power, even if we’re doing nothing wrong at the time of surveillance. The definition of “wrong” is often arbitrary, and can quickly change. For example, in the US in the 1930s, being a Communist or Socialist was a bit of an intellectual fad, and not considered wrong among the educated classes. In the 1950s, that changed dramatically with the witch-hunts of Senator Joseph McCarthy, when many intelligent, principled American citizens found their careers destroyed once their political history was publicly disclosed. Is someone’s reading of Occupy, Tea Party, animal rights, orgun rights websites going to become evidence of subversion in five to ten years? This situation is exacerbated by the fact that we are generating so much data and storing it indefinitely. Those fishing expeditions can go into the past, finding things you might have done 10, 15, or 20 years ago . . . and counting. Today’s adults were able to move beyond their youthful indiscretions; today’s young people will not have that freedom. Their entire histories will be on the permanent record.

### Surveillance Bad-Laundry List

#### **Mass surveillance is dangerous—it allows corporate control, racism, sexism, classism, and social control. And there’s no recourse—meaning there’s no check on the impact.**

Schneier, 15 (Bruce (2015-03-02). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (pp. 4-5). W. W. Norton & Company. Kindle Edition.)

Here is what’s true. Today’s technology gives governments and corporations robust capabilities for mass surveillance. Mass surveillance is dangerous. It enables discrimination based on almost any criteria: race, religion, class, political beliefs. It is being used to control what we see, what we can do, and, ultimately, what we say. It is being done without offering citizens recourse or any real ability to opt out, and without any meaningful checks and balances. It makes us less safe. It makes us less free. The rules we had established to protect us from these dangers under earlier technological regimes are now woefully insufficient; they are not working. We need to fix that, and we need to do it very soon.

### Surveillance Bad-Corporate Control

#### **Corporate and government interests have converged in an apparatus of constant and total surveillance**

Schneier, 15 (Bruce (2015-03-02). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (pp. 24-25). W. W. Norton & Company. Kindle Edition)

The cost of computing technology has declined rapidly in recent decades. This has been a profoundly good thing. It has become cheaper and easier for people to communicate, to publish their thoughts, to access information, and so on. But that same decline in price has also brought down the price of surveillance. As computer technologies improved, corporations were able to collect more information on everyone they did business with. As the cost of data storage became cheaper, they were able to save more data and for a longer time. As big data analysis tools became more powerful, it became profitable to save more information. This led to the surveillance-based business models I’ll talk about in Chapter 4. Government surveillance has gone from collecting data on as few people as necessary to collecting it on as many as possible. Whensurveillance was manual and expensive, it could only be justified in extreme cases. The warrant process limited police surveillance, and resource constraints and the risk of discovery limited national intelligence surveillance. Specific individuals were targeted for surveillance, and maximal information was collected on them alone. There were also strict minimization rules about not collecting information on other people. If the FBI was listening in on a mobster’s phone, for example, the listener was supposed to hang up and stop recording if the mobster’s wife or children got on the line. As technology improved and prices dropped, governments broadened their surveillance. The NSA could surveil large groups— the Soviet government, the Chinese diplomatic corps, leftist political organizations and activists— not just individuals. Roving wiretaps meant that the FBI could eavesdrop on people regardless of the device they used to communicate with. Eventually, US agencies could spy on entire populations and save the data for years. This dovetailed with a changing threat, and they continued espionage against specific governments, while expanding mass surveillance of broad populations to look for potentially dangerous individuals. I’ll talk about this in Chapter 5. The result is that corporate and government surveillance interests have converged. Both now want to know everything about everyone. The motivations are different, but the methodologies are the same. That is the primary reason for the strong public-private security partnership that I’ll talk about in Chapter 6.

### Surveillance Bad-Unpopular

#### NSA Surveillance unpopular

Susan Page 14 ( susan page http://www.usatoday.com/story/news/politics/2014/01/20/poll-nsa-surveillance/4638551/)

Most Americans now disapprove of the NSA's sweeping collection of phone metadata, a new USA TODAY/Pew Research Center Poll finds, and they're inclined to think there aren't adequate limits in place to what the government can collect. President Obama's announcement Friday of changes in the surveillance programs has done little to allay those concerns: By 73%-21%, those who paid attention to the speech say his proposals won't make much difference in protecting people's privacy. The poll of 1,504 adults, taken Wednesday through Sunday, shows a public that is more receptive than before to the arguments made by former NSA contractor Edward Snowden. His leak of intelligence documents since last spring has fueled a global debate over the National Security Agency's surveillance of Americans and spying on foreign leaders

Thousands of critical government buildings face high risk of cyberattacks

By SARAH WESTWOOD /15

Systems that control the elevators, lights, ventilation, and fire alarms in federal buildings are vulnerable to cyberattacks that could compromise security or result in serious harm to government workers and U.S. citizens.. In a report released within hours of high-profile social media hacks at U.S. Central Command, the Government Accountability Office said homeland security officials have little understanding of the risks presented by Internet-based control systems and don’t have a clear strategy for dealing with an attack if one were to occur. The congressional watchdog is worried that cyberattacks on the access and control systems of federal buildings could “damage the government’s credibility.” Such attacks could allow outsiders to access restricted federal buildings or result in death if fire alarms and sprinklers were switched off during a blaze, the report said. The Department of Homeland Security is responsible for protecting thousands of office complexes, laboratories and warehouses, many of which are managed by the General Services Administration. GAO has designated both federal information systems and federal property management as “high risk areas." Because functions like air conditioning, closed-circuit TV surveillance and door locks are increasingly automated and centralized, federal buildings face a heightened risk of cyberattack. Such threats can come from “corrupt employees, criminal groups, hackers, and terrorists,” GAO said. “No one in DHS is assessing the cyber risk to building and access control systems at the almost 9,000 facilities” under the agency’s protection. GSA officials have also yet to inspect the cybersecurity of control systems in hundreds of federal buildings, the report said. Between 2011 and 2014, cyber incidents involving control systems jumped from 140 to 243, an increase of 74 percent. GAO pointed to the highly-publicized breach of customer information at Target stores in 2013 as an example of the threat digital control systems can pose, claiming the attack likely occurred “after intruders obtained a heating, ventilation, and air-conditioning system vendor’s credentials to access the outermost portion” of Target’s network. Access and control systems “were not designed with cybersecurity in mind,” the report noted. What’s more, DHS has yet to “define the problem,” let alone determine what resources it will need to arm buildings against cyber attacks, the report said. Federal facilities that “store high-risk items such as weapons and drugs” are more likely to be the target of a cyber attack, according to the the report.

### Human Rights Impacts

#### Human rights solve poverty, violence, globalization, military violence, environmental destruction, and promote peace and security

Copelon 1999 (Rhonda Professor of Law and Director of the International Women's Human Rights Law Clinic at the City University of New York School of Law, New York City Law Review, 1998/99, 3 N.Y. City L. Rev. 59, L/N)

The indivisible human rights framework survived the Cold War despite U.S. machinations to truncate it in the international arena. The framework is there to shatter the myth of the superiority of the U.S. version of rights, to rebuild popular expectations, and to help develop a culture and jurisprudence of indivisible human rights. Indeed, in the face of systemic inequality and crushing poverty, violence by official and private actors, globalization of the market economy, and military and environmental depredation, the human rights framework is gaining new force and new dimensions. It is being broadened today by the movements of people in different parts of the world, particularly in the Southern Hemisphere and significantly of women, who understand the protection of human rights as a matter of individual and collective human survival and betterment. Also emerging is a notion of third-generation rights, encompassing collective rights that cannot be solved on a state-by-state basis and that call for new mechanisms of accountability, particularly affecting Northern countries. The emerging rights include human-centered sustainable development, environmental protection, peace, and security. Given the poverty and inequality in the United States as well as our role in the world, it is imperative that we bring the human rights framework to bear on both domestic and foreign policy.

#### Human rights law is a key check against sovereignty

Zeng, 9 [ZENG Lingliang, Faculty of Law, University of Macau, Macau, China, Humanizing tendency of contemporary international law, Front. Law China 2009, 4(1): 1-30

Humanization of international law has greatly enriched the contents of international law. Firstly, humanization has directly produced a series of new branches of international law, among which international human rights law, international environmental law and international criminal law are the most persuasive examples. Secondly, humanization has promoted some classic sectors of international law being continuously updated and adapted themselves to new conceptions, principles, rules and mechanism, such as various new elements in the law of sea, space law, law of diplomatic protection, humanitarian law, law of extradition, etc. In addition, humanization has urged international community to seek for dynamic links and appropriate coordination among certain sectors or areas of international law, such as the interactions between security, development, human rights and rule of law, the balance between economic development and environmental protection, the conciliation between intellectual property rights and public health, the connection between trade liberalization and core labor standards, etc. As a result of these horizontal and vertical development of humanizing international law, while sectors, areas or matters that are solely subject to domestic jurisdictions of States have been greatly decreasing, international law has been extending its scopes not only into various internal sectors of States, but also into all aspects of human life. In a word, humanizing international law symbolizes the end of absolute sovereignty and popularity of relative sovereignty both in theory and practice.

## Utah Data Center Add-On

### 2AC Utah Data Center Add-On

#### First, Section 702 is the crux of the Utah Data Center—the plan eliminates the program that keeps it alive.

Informed Trades 2013 (“A Missive on Privacy, Statism, The NSA, and Snowden,” Informed Trades. 6/22, http://www.informedtrades.com/780444-missive-privacy-statism-nsa-snowden.html)

What is not so related to the markets is the Department of Defense's intrusion of privacy in the holy name of counter-terrorism. If you're an American reading this you should be very aware of the aptly coined "PRISM" program, the "warrantless wiretapping" of phone and internet communications by the NSA; FAA Section 702, FISA, the Patriot Act, Tailored Access Operations (TAO), and Edward Snowden.¶ I suspect there will be a pseudo-scientific term called "Snowden Collective" that will be in political dictionaries soon, it describes in detail how Government officials define espionage and treason and what constitutes to hypocrisy when the State actually starts to fear one person that it has to call him a "highschool dropout" and a "liar" merely to maintain a consistent PR; lies are told to patch the previous lies; installment after installment will come and go, each paying homage to the truth which will be denied and condemned by the State.¶ It is appalling how much power the State has actually amassed since the Vietnam War when the perpetual propaganda program to mold the susceptible minds of the average American, because when all formalities and insignias are removed, it is indeed within Washington's foreign policy to intervene in affairs that bears absolutely no tangent to its interests. Yet it is precisely this that makes the State feel normal.¶ In short, the State's cyber-espionage, intelligence indexing and data mining programs mostly "mandated" without official majority congressional approvals or public referendums have become an obsession. It isn't a want and most definitely isn't a need (although this is an area of contention up for scholarly debate), but an obsession many aren't cognizant about. Much more on this comical panoply later. Whistle Blower Edward Snowden has been a valiant vigilante in sounding the clarion, he placed his life and those in proximity of him at great peril and is in my eyes, a forerunner for global awareness. The revelation of PRISM was just a caricature of the NSA's various surveillance programs since 2009 when Obama took office and the Congressional bipartisanship really resonated. Technology has brought us closer, made us more interconnected then ever before, improved the quality of life by quantums, but has also opened us up and made us vulnerable.¶ PRISM's Just The Tip Of The Iceberg¶ The NSA has 2 primary ways of intelligence surveillance: PRISM (direct server intrusion); and under FAA section 702 (intercepting flows from communication conduits). In turns out that later revelations about the Defense Department's data collection modus operandi have placed PRISM is a different light, that of a lower tiered information filtering apparatus. Zero Hedge brought to prescient attention of an Associated Press article where PRISM was said to be part of a larger data mining architecture dubbed "hovering". The supernova scale of the State's information gathering program puts even the most sinister secret intelligence that star in sci-fi films to contempt as a former NSA official commented, "You have to assume everything is being collected." And as you will read further down this article, Snowden did not say PRISM was the greatest chimera in the State's arsenal, he merely gave journalists a starting point to carry out their own digging; so one can safely say that PRISM and "warrantless wiretapping" programs in place since 2009 are just facets of the brilliantly cut diamond. Much more on PRISM and its sister programs below.¶ BLUFFdale, Just Don't Try Your Luck¶ What the State essentially does is under its data collection architecture is to intercept (but not block) data flowing through the parent optical-fiber cables, the "backbone" of the Internet, create carbon copies raw data, and archive the digital files in servers located in classified regions within CONUS. It takes an enormous about of processing power to duplicate all that streaming data (at the speed of light since the signals are of the electromagnetic spectrum, light or otherwise), and simultaneously index and assign basically logical sequencing to them so that they can be accessed in the future. The NSA's data center (Intelligence Community Comprehensive National Cybersecurity Initiative Data Center) is rumored, although with credible facts, to be in Bluffdale, a bowl-shaped valley "in the shadow of Utah’s Wasatch Range to the east and the Oquirrh Mountains to the west". The climate is dry, arid, but most importantly cold. Apart from a few thousand polygamists, there is little sign of human life, a perfect location for the NSA's most industrious project yet.¶ Now why did I mentioned a cool climate to be auxiliary to this data center? Simple, it allows it to function much more effectively because as the BBC reported last week, global data centers consuming about 2% of the world's energy production; that is a lot of joules spent on processing data. But tactically, in the event of any power outage, the complex's cooling systems can be run at a minimum capacity while the servers can remain function albeit at much lower clock speeds; the crux of which means the Utah Data Center as it is so squarely named can continue to operate on backup power supplies.¶ Popular technology site wired.com stated in 2012 that the complex consumes 65Mw of power on an average day, and has backup generators which have enough fuel on site to run the super-machine at half capacity for 3 days. In short, the data center is self-sustaining; it has its own water supply, electrical substations, and a security force that is armed to the teeth. If anything made Buffdale conspicuous, it would be physical security measures; fences, automatic turrets, armored vehicles, infrared spectrum cameras and the likes.¶ So what are the capabilities of this data matrix? Again according to wired.com, the complex that is speculated to be completed by September 2013, will be flourished with 100,000 sq ft of single story space for servers and cabling, and an additional 900,000 sq ft for support and administration. The ultimate goal for its data storing capacity is rumored to be a "Yottabyte" (the equivalent of 500^16 pages of text).¶ I quote wired.com to provide some perspective, necessary when dealing in galactic scales:¶ Quote:¶ "It needs that capacity because, according to a recent report by Cisco, global Internet traffic will quadruple from 2010 to 2015, reaching 966 exabytes per year. (A million exabytes equal a yottabyte.) In terms of scale, Eric Schmidt, Google’s former CEO, once estimated that the total of all human knowledge created from the dawn of man to 2003 totaled 5 exabytes. And the data flow shows no sign of slowing. In 2011 more than 2 billion of the world’s 6.9 billion people were connected to the Internet. By 2015, market research firm IDC estimates, there will be 2.7 billion users. Thus, the NSA’s need for a 1-million-square-foot data storehouse."¶ The metadata that the NSA collects (all throughout America'a domestic web and telecommunications flows, and transnational international web flows) and achieves (at the Utah Data Center) actually mean nothing in its inert form. Binary codes will remains uncracked, even terabytes of metadata taken in singularity wouldn't mean a thing because the combinations and permutations for that data set are infinite. Here is where programs like PRISM fall into the labyrinth of giant modules. The swath of data has to be analyzed eventually and as omnipotent as the NSA is, it cannot by any far shot analyze and correlate individual data points; that would be analogous to placing a time limit when traveling at light speed to the edge of the known universe. Programs like PRISM, and another lesser known crypto-code cracking program called "Stellar Wind" were engineered to selectively categorize information and then break them down into granular pieces so that they would be of utility to intelligence agents like the CIA and FBI. Think of it like those pesky BitCoin miners, which are essentially very complex algorithms hosted on processors rubbing at very fast clock speeds.

#### **Second, The UDC is the backbone of a turnkey totalitarian state**

Bamford 12 (James, fmr. Professor of Journalism at Univ. of Calif. at Berkeley and recipient, National Magazine Award for Reporting, “THE NSA IS BUILDING THE COUNTRY’S BIGGEST SPY CENTER (WATCH WHAT YOU SAY),” *Wired Magazine*, March 15, http://www.wired.com/2012/03/ff\_nsadatacenter/)

Given the facility’s scale and the fact that a terabyte of data can now be stored on a flash drive the size of a man’s pinky, the potential amount of information that could be housed in Bluffdale is truly staggering. But so is the exponential growth in the amount of intelligence data being produced every day by the eavesdropping sensors of the NSA and other intelligence agencies. As a result of this “expanding array of theater airborne and other sensor networks,” as a 2007 Department of Defense report puts it, the Pentagon is attempting to expand its worldwide communications network, known as the Global Information Grid, to handle yottabytes (1024 bytes) of data. (A yottabyte is a septillion bytes—so large that no one has yet coined a term for the next higher magnitude.)¶ It needs that capacity because, according to a recent report by Cisco, global Internet traffic will quadruple from 2010 to 2015, reaching 966 exabytes per year. (A million exabytes equal a yottabyte.) In terms of scale, Eric Schmidt, Google’s former CEO, once estimated that the total of all human knowledge created from the dawn of man to 2003 totaled 5 exabytes. And the data flow shows no sign of slowing. In 2011 more than 2 billion of the world’s 6.9 billion people were connected to the Internet. By 2015, market research firm IDC estimates, there will be 2.7 billion users. Thus, the NSA’s need for a 1-million-square-foot data storehouse. Should the agency ever fill the Utah center with a yottabyte of information, it would be equal to about 500 quintillion (500,000,000,000,000,000,000) pages of text.¶ The data stored in Bluffdale will naturally go far beyond the world’s billions of public web pages. The NSA is more interested in the so-called invisible web, also known as the deep web or deepnet—data beyond the reach of the public. This includes password-protected data, US and foreign government communications, and noncommercial file-sharing between trusted peers. “The deep web contains government reports, databases, and other sources of information of high value to DOD and the intelligence community,” according to a 2010 Defense Science Board report. “Alternative tools are needed to find and index data in the deep web … Stealing the classified secrets of a potential adversary is where the [intelligence] community is most comfortable.” With its new Utah Data Center, the NSA will at last have the technical capability to store, and rummage through, all those stolen secrets. The question, of course, is how the agency defines who is, and who is not, “a potential adversary.”¶ THE NSA’S SPY NETWORK¶ Once it’s operational, the Utah Data Center will become, in effect, the NSA’s cloud. The center will be fed data collected by the agency’s eavesdropping satellites, overseas listening posts, and secret monitoring rooms in telecom facilities throughout the US. All that data will then be accessible to the NSA’s code breakers, data-miners, China analysts, counterterrorism specialists, and others working at its Fort Meade headquarters and around the world. Here’s how the data center appears to fit into the NSA’s global puzzle.—J.B.¶ Before yottabytes of data from the deep web and elsewhere can begin piling up inside the servers of the NSA’s new center, they must be collected. To better accomplish that, the agency has undergone the largest building boom in its history, including installing secret electronic monitoring rooms in major US telecom facilities. Controlled by the NSA, these highly secured spaces are where the agency taps into the US communications networks, a practice that came to light during the Bush years but was never acknowledged by the agency. The broad outlines of the so-called warrantless-wiretapping program have long been exposed—how the NSA secretly and illegally bypassed the Foreign Intelligence Surveillance Court, which was supposed to oversee and authorize highly targeted domestic eavesdropping; how the program allowed wholesale monitoring of millions of American phone calls and email. In the wake of the program’s exposure, Congress passed the FISA Amendments Act of 2008, which largely made the practices legal. Telecoms that had agreed to participate in the illegal activity were granted immunity from prosecution and lawsuits. What wasn’t revealed until now, however, was the enormity of this ongoing domestic spying program.¶ For the first time, a former NSA official has gone on the record to describe the program, codenamed Stellar Wind, in detail. William Binney was a senior NSA crypto-mathematician largely responsible for automating the agency’s worldwide eavesdropping network. A tall man with strands of black hair across the front of his scalp and dark, determined eyes behind thick-rimmed glasses, the 68-year-old spent nearly four decades breaking codes and finding new ways to channel billions of private phone calls and email messages from around the world into the NSA’s bulging databases. As chief and one of the two cofounders of the agency’s Signals Intelligence Automation Research Center, Binney and his team designed much of the infrastructure that’s still likely used to intercept international and foreign communications.¶ He explains that the agency could have installed its tapping gear at the nation’s cable landing stations—the more than two dozen sites on the periphery of the US where fiber-optic cables come ashore. If it had taken that route, the NSA would have been able to limit its eavesdropping to just international communications, which at the time was all that was allowed under US law. Instead it chose to put the wiretapping rooms at key junction points throughout the country—large, windowless buildings known as switches—thus gaining access to not just international communications but also to most of the domestic traffic flowing through the US. The network of intercept stations goes far beyond the single room in an AT&T building in San Francisco exposed by a whistle-blower in 2006. “I think there’s 10 to 20 of them,” Binney says. “That’s not just San Francisco; they have them in the middle of the country and also on the East Coast.”¶ The eavesdropping on Americans doesn’t stop at the telecom switches. To capture satellite communications in and out of the US, the agency also monitors AT&T’s powerful earth stations, satellite receivers in locations that include Roaring Creek and Salt Creek. Tucked away on a back road in rural Catawissa, Pennsylvania, Roaring Creek’s three 105-foot dishes handle much of the country’s communications to and from Europe and the Middle East. And on an isolated stretch of land in remote Arbuckle, California, three similar dishes at the company’s Salt Creek station service the Pacific Rim and Asia.¶ The former NSA official held his thumb and forefinger close together: “We are that far from a turnkey totalitarian state.”¶ Binney left the NSA in late 2001, shortly after the agency launched its warrantless-wiretapping program. “They violated the Constitution setting it up,” he says bluntly. “But they didn’t care. They were going to do it anyway, and they were going to crucify anyone who stood in the way. When they started violating the Constitution, I couldn’t stay.” Binney says Stellar Wind was far larger than has been publicly disclosed and included not just eavesdropping on domestic phone calls but the inspection of domestic email. At the outset the program recorded 320 million calls a day, he says, which represented about 73 to 80 percent of the total volume of the agency’s worldwide intercepts. The haul only grew from there. According to Binney—who has maintained close contact with agency employees until a few years ago—the taps in the secret rooms dotting the country are actually powered by highly sophisticated software programs that conduct “deep packet inspection,” examining Internet traffic as it passes through the 10-gigabit-per-second cables at the speed of light.

### Utah Data Center is Expanding

#### **Inherency: UDC is only expanding now**

Strasenburgh 15 (Audrey, Contributor, Cache Valley Daily News, “C7 initiates plans to expand its Utah data center,” Cache Valley Daily News, Saturday, June 20, 2015 5:00 am http://www.cachevalleydaily.com/news/article\_d053828c-16c0-11e5-a454-e31e75cbc16c.html)

Bluffdale, UT-based data center operator C7 Data Centers recently announced the beginning of Phase 2 constructions at its flagship Granite Point II Utah data center.¶ According to a May 22 Data Center Knowledge article, Phase 2 will add an additional 30,000 square feet to C7's facility, and is projected to be completed by October 2015. Currently, the company's 35,000 square-foot facility, which opened in 2013, is nearing its capacity.¶ In addition to upping its data capacity, C7 will expand its data center's power capacity during Phase 2 construction. When Phase 2 is complete, C7's Granite Point campus will boast more than 11 megawatts of power capacity to serve the 250,000 square-foot campus. The company has an additional onsite substation planned for 2016, which will add more than 20 megawatts of power capacity, TechRockies reports.¶ The Granite Point data center's location in the cold Utah desert provides an advantage for efficiently keeping its servers cool. The server manufacturing industry, a $14 billion economic powerhouse, is notorious for creating machines that can generate enough heat energy to warm several homes.¶ The center employs a combination of ambient air and cold air containment and actuated cooling to regulate its server room temperatures. And because of Granite Point's cooling efficiencies, C7 reports it can deliver as much as 75 - 80% of its power capacity to the critical load versus the industry average of 50 to 60%.¶ Over the last few years, Utah has become a prime location for data centers, given its low energy rates, ambient air cooling capabilities and low risk profile for new ventures. C7 CEO Wes Swenson said Granite Point II stands apart from its competition as a result of Utah's favorable climate for data centers.¶ “Granite Point II is an extreme departure in data center design from the typical industry standard; in its aesthetic, ‘just in time’ effectiveness and efficiency in provisioning and cooling,” Swenson said in a release. “We have had an overwhelming response to the product; it’s not like anything else in the market.”

#### **The UDC is an iconic national symbol that holds all personal communication**

Shado 14 (Sean, Reporter for CloudWedge Magazine, “An Overview of the NSA’s Utah Data Center” *Cloud Wedge Magazine*, Dec 9, 2014 http://www.cloudwedge.com/4891-an-overview-of-the-nsas-utah-data-center/)

Probably the most notorious federal data center, the USA’s National Security Agency operates what is known as the UtahDataCenter. The UDC has nearly 1.5 million square feet of facilities space at CampWilliams. The site hosts a data center that contains 100,000 square feet of floor space that can be used for servers and networking apparatus. The UtahDataCenter finished construction at the end of 2013. The total construction costs for the facility totaled $1.5 billion dollars.¶ Much of what the UtahDataCenter actually does is classified. It is rumored that the facility has so much storage capacity that it could store exabytes or larger. In order to put 1 exabyte into perspective, the calculation breaks down into 1 billion gigabytes. What could the facility be doing with all of the memory? Documents show that the building was built to support the Comprehensive National Cybersecurity Initiative. Other analysts believe that the facility is being used to store communications data pertaining to those who are using online and mobile services.¶ Depending upon who you ask, the UtahDataCenter facility is tasked for specific missions. According to a Wired article published in 2012, writer James Bamford mentions that the datacenter holds “all forms of communication, including the complete contents of private emails, cell phone calls, and Internet searches, as well as all types of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital ‘pocket litter’.”¶ The NSA refutes that claim and in 2013, an NSA spokesperson mentioned that, “Many unfounded allegations have been made about the planned activities of the Utah Data Center, one of the biggest misconceptions about NSA is that we are unlawfully listening in on, or reading emails of, U.S. citizens. This is simply not the case.”¶ While we aren’t clear on the true purpose of the UtahDataCenter, it is clear that this monstrous structure serves a distinct purpose for the National Security Agency. Because of that, the contingency measures that the NSA has put into place ensure that this structure would continue to function during the time of a disaster.

### **Data Centers Bad-Surveillance**

#### **The NSA makes no distinction between domestic and foreign surveillance—the UDC makes snooping ubiquitous**

The Guardian 13 (Rory Carroll, Western US Reporter, “Welcome to Utah, the NSA’s desert home for eavesdropping on America,” *The Guardian*, June 14, http://www.theguardian.com/world/2013/jun/14/nsa-utah-data-facility)

Welcome to the Utah Data Center, a new home for the NSA's exponentially expanding information trove. The $1.7bn facility, two years in the making, will soon host supercomputers to store gargantuan quantities of data from emails, phone calls, Google searches and other sources. Sited on an unused swath of the national guard base, by September it will employ around 200 technicians, span 1m sq ft and use 65 megawatts of power.¶ This week Utah roasted in near-record temperatures ideal for fires and thunderstorms, putting the state under a hazardous weather outlook advisory. The NSA could have done with a similar warning for the scorching criticism of its surveillance activities, a sudden reversal of scrutiny for the agency and its Utah complex.¶ Deep in Mormon country between the Wasatch and Oquirrh mountains, nestled on the outskirts of Bluffdale (population 7,598), it was designed to be largely anonymous. Instead, after Guardian disclosures of data-mining programs involving millions of Americans, the Utah Data Center provokes an urgent question: what exactly will it do?¶ The NSA says it will not illegally eavesdrop on Americans but is otherwise vague. Its scale is not in doubt. Since January 2011 a reported 10,000 labourers have built four 25,000-sq ft halls filled with servers and cables, plus an additional 900,000 sq ft of space for technical support and administration. Generators and huge fuel and water tanks will make the site self-sustaining in an emergency.¶ Outside experts disagreed on the centre's potential. Some said it will just store data. Others envisaged a capacity to not just store but analyse and break codes, enabling technicians here to potentially snoop on the entire population for decades to come.¶ William Binney, a mathematician who worked at the NSA for almost 40 years and helped automate its worldwide eavesdropping, said Utah's computers could store data at the rate of 20 terabytes – the equivalent of the Library of Congress – per minute. "Technically it's not that complicated. You just need to work out an indexing scheme to order it."¶ Binney, who left the agency in 2001 and blew the whistle on its domestic spying, said the centre could absorb and store data for "hundreds of years" and allow agencies such as the FBI to retroactively use the information.¶ He said the centre will likely have spare capacity for "brute force attacks" – using speed and data hoards to detect patterns and break encrypted messages in the so-called deep web where governments, corporations and other organisations keep secrets. There would be no distinction between domestic and foreign targets. "It makes no difference anymore to them."¶ James Bamford, author of The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America, said the public had yet to grasp the significance of Utah's data-mining. "It's basically a hard-drive. It's also a cloud, a warehouse. It'll be storing not just text and audio but pictures and video. There's a lackadaisical attitude to this. People pay no attention until it's too late." Bamford wrote a cover story about the centre for Wired last year.¶ Brewster Kahle, a co-founder of the Internet Archive, a San Francisco-based non-profit that hoovers up knowledge in a digital equivalent of the library of Alexandria, said technology facilitated near-ubiquitous snooping. "If one had the opportunity to collect all the voice traffic in the US it would cost less than the Pentagon spends on paperclips. Storage these days is trivial, it's not a problem."

#### **The UDC is the final piece in the NSA’s intelligence intrusion program**

Bamford 12 (James, fmr. Professor of Journalism at Univ. of Calif. at Berkeley and recipient, National Magazine Award for Reporting, “THE NSA IS BUILDING THE COUNTRY’S BIGGEST SPY CENTER (WATCH WHAT YOU SAY),” *Wired Magazine*, March 15, http://www.wired.com/2012/03/ff\_nsadatacenter/)

The NSA has become the largest, most covert, and potentially most intrusive intelligence agency ever.¶ Under construction by contractors with top-secret clearances, the blandly named Utah Data Center is being built for the National Security Agency. A project of immense secrecy, it is the final piece in a complex puzzle assembled over the past decade. Its purpose: to intercept, decipher, analyze, and store vast swaths of the world’s communications as they zap down from satellites and zip through the underground and undersea cables of international, foreign, and domestic networks. The heavily fortified $2 billion center should be up and running in September 2013. Flowing through its servers and routers and stored in near-bottomless databases will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital “pocket litter.” It is, in some measure, the realization of the “total information awareness” program created during the first term of the Bush administration—an effort that was killed by Congress in 2003 after it caused an outcry over its potential for invading Americans’ privacy.¶ But “this is more than just a data center,” says one senior intelligence official who until recently was involved with the program. The mammoth Bluffdale center will have another important and far more secret role that until now has gone unrevealed. It is also critical, he says, for breaking codes. And code-breaking is crucial, because much of the data that the center will handle—financial information, stock transactions, business deals, foreign military and diplomatic secrets, legal documents, confidential personal communications—will be heavily encrypted. According to another top official also involved with the program, the NSA made an enormous breakthrough several years ago in its ability to cryptanalyze, or break, unfathomably complex encryption systems employed by not only governments around the world but also many average computer users in the US. The upshot, according to this official: “Everybody’s a target; everybody with communication is a target.”¶ For the NSA, overflowing with tens of billions of dollars in post-9/11 budget awards, the cryptanalysis breakthrough came at a time of explosive growth, in size as well as in power. Established as an arm of the Department of Defense following Pearl Harbor, with the primary purpose of preventing another surprise assault, the NSA suffered a series of humiliations in the post-Cold War years. Caught offguard by an escalating series of terrorist attacks—the first World Trade Center bombing, the blowing up of US embassies in East Africa, the attack on the USS Cole in Yemen, and finally the devastation of 9/11—some began questioning the agency’s very reason for being. In response, the NSA has quietly been reborn. And while there is little indication that its actual effectiveness has improved—after all, despite numerous pieces of evidence and intelligence-gathering opportunities, it missed the near-disastrous attempted attacks by the underwear bomber on a flight to Detroit in 2009 and by the car bomber in Times Square in 2010—there is no doubt that it has transformed itself into the largest, most covert, and potentially most intrusive intelligence agency ever created.¶ In the process—and for the first time since Watergate and the other scandals of the Nixon administration—the NSA has turned its surveillance apparatus on the US and its citizens. It has established listening posts throughout the nation to collect and sift through billions of email messages and phone calls, whether they originate within the country or overseas. It has created a supercomputer of almost unimaginable speed to look for patterns and unscramble codes. Finally, the agency has begun building a place to store all the trillions of words and thoughts and whispers captured in its electronic net. And, of course, it’s all being done in secret. To those on the inside, the old adage that NSA stands for Never Say Anything applies more than ever.

#### **Surveillance bad—it is politicized and turned against us**

Bamford 12 (James, fmr. Professor of Journalism at Univ. of Calif. at Berkeley and recipient, National Magazine Award for Reporting, “THE NSA IS BUILDING THE COUNTRY’S BIGGEST SPY CENTER (WATCH WHAT YOU SAY),” *Wired Magazine*, March 15, http://www.wired.com/2012/03/ff\_nsadatacenter/)

But there is, of course, reason for anyone to be distressed about the practice. Once the door is open for the government to spy on US citizens, there are often great temptations to abuse that power for political purposes, as when Richard Nixon eavesdropped on his political enemies during Watergate and ordered the NSA to spy on antiwar protesters. Those and other abuses prompted Congress to enact prohibitions in the mid-1970s against domestic spying.

#### **The UDC has an ominous role in the surveillance state—it eliminates private communication and subverts state institutions**

Anderson, 15 (Martin, Martin has a background in technology journalism, but has also contributed his technical and writing skills to a broad range of publications, websites and publishing houses, including Dennis Publishing and Press Holdings Ltd., “Utah data centre critical to help the NSA ‘eliminate all private communications’, says Snowden journalist,” *The Stack*, April 8, http://thestack.com/glenn-greenwald-utah-data-center-bluffdale-080415)

The journalist and ex-lawyer who came to prominence by helping Edward Snowden to disclose the secrets of the National Security Agency has spoken of ‘government inside the government’ and the critical role of the NSA’s ‘Intelligence Community Comprehensive National Cybersecurity Initiative Data Center’ at a gathering in Utah, describing the plant as having an “ominous role in the surveillance state”.¶ Speaking at the Utah Museum of Fine Arts at the University of Utah, former lawyer and Guardian journalist Glenn Greenwald discussed the scope of the NSA’s mandate to collect information, and criticised the agency’s broad remit:¶ “It's not, like, 'Collect a lot of it,'” said Greenwald, "or even, like, 'Collect all the terrorist communications,'…It's like saying the goal of the NSA is to eliminate all private communications."¶ Greenwald is said to have stated that the Utah Data Centre at Bluffdale ‘helps solve that problem’.¶ Dubbed ‘the spy center’ by local media, the data centre at Utah occupies 1 million square feet and contains four 25,000 square foot data halls backed up by 60,000 tons of cooling equipment and caters to a 65mw peak demand. It is reported to have a maximum capacity of a yottabyte of information (1024 bytes), equivalent to 500 quintillion pages of text.¶ Greenwald said at the event “The better [the government's] capacity for storage, and the more space they have to do it the longer they can keep the data,”¶ The journalist, who lives a reportedly eccentric life in Rio de Janeiro, was one of two reporters that caught NSA fugitive Edward Snowden’s eye when he was considering how to disseminate information he had retrieved from his time with the agency. Greenwald’s 2013 meeting with Snowden is reputed to have led to the disclosure to him of thousands of pages of harvested NSA documents.¶ Greenwald, speaking as part of the university’s surveillance-themed Secrecy Week, also implicitly criticised the University of Utah by suggesting that a university should not open up its campus to government agencies just because it might provide abundant funding, asserting “That sort of subverts the concept of universities”. The University of Utah has provided courses for students intended to lead to work at the Bluffdale data centre.

### Data Centers Bad-Democracy

#### NSA Data Center Leads to Dictatorship

Irving 13 (Clive, “Behold the NSA’s Dark Star: The Utah Data Center”. DailyBeast. June 8) http://www.thedailybeast.com/articles/2013/06/08/behold-the-nsa-s-dark-star-the-utah-data-center.html

Remember the Stasi, the secret police who operated in East Germany when it was a communist state? When the Berlin Wall came down, East Germans discovered they had been living in a society so rotted by paranoia that at least one in three of its adult citizens were spying on the other two. From this springs what I call the Stasi Principle: a state’s appetite for collecting intelligence expands in direct relationship to its technical ability to do so. In the case of East Germany, this ended up producing warehouses stuffed with bulging files containing the minutely observed details of the everyday, humdrum lives of millions. The product was both banal and, in its range and results, terrifying (a world caught beautifully in the film The Lives of Others). In the case of the U.S., the apotheosis of the same mind-set lies in a sprawling complex at Camp Williams, Utah, due to start operating this fall. Billions of dollars have gone into creating this cyberintelligence facility for the National Security Agency. There’s no official explanation of the Utah Data Center’s real mission, except that it’s the largest of a network of data farms including sites in Colorado, Georgia, and Maryland. But it’s obviously been built to vastly increase the agency’s capacity to suck in, digest, analyze, and store whatever the intelligence community decides to collect. As of this week, we know a lot more about the kind of data that includes. Of course, the U.S. is still far from being the police state that East Germany was. But I do think we need to better understand how this technological juggernaut works, what its scope really is—and particularly we need to appreciate how our political acceptance of this scale of surveillance is shaping the kind of society we are.

#### Utah Center Causes Public Unrest

Palleata 15 (Damian, “A top secret NSA site draws swipes, shrugs”. Wall Street Journal. May 1) http://www.wsj.com/articles/a-top-secret-nsa-site-draws-swipes-shrugs-1430523735

As a defiant statement against what it sees as government overreach, a group of Utahans “adopted” the desert highway that leads to the National Security Agency’s secretive and sprawling new facility in Bluffdale. Their novel plan: While collecting trash along their stretch of road, they would simultaneously protest outside the NSA building, spreading the “Restore the Fourth” message in favor of Fourth Amendment protections against illegal search and seizure. But their plan soon wilted thanks to a lack of organization and a lack of enthusiasm for more protests. “What we’re working on now is consolidating and coordinating our actions with other organizations,” said Dan Garfield, who leads Restore the Fourth’s Utah chapter. He said there is no timeline for the next protest. The stalled effort highlights the ambivalence in Utah and in Washington, D.C., over secret government surveillance programs. Section 215 of the USA Patriot Act, which the government has used to justify its bulk telephone-record collection program, expires at the end of this month, giving hope to the agency’s critics that they can make major changes. But the rise of the Islamic State extremist group has encouraged more outspoken support for the NSA, including by several potential presidential candidates, complicating negotiations about what to do with the expiring powers. In Utah, plenty of people don’t seem bothered by the NSA presence. “You get just about anybody into a conversation about it and it’s not high on their list of things to be worried about,” said Pete Ashdown, who runs a private data center in Salt Lake City, about 20 miles to the north, and who opposes the facility. Mr. Ashdown was one of many Utahans who received a tour of the facility while it was being built a few years ago. He said he was told by NSA officials that the site was chosen because “power is cheap and the people are patriotic.” “I kind of read that as a subtext that the people aren’t going to question what is going on out here,” he said. Which raises the question: What is going on out there? A number of the facility’s neighbors, even its supporters, say they have no idea. The government built the giant facility known simply as the “Utah Data Center” on property controlled and secured by the Utah National Guard, which means the public has no access. It has roughly 200 employees, but the agency won’t say what it does there, or which data it stores. Mr. Ashdown and one other person who was given a tour of the facility, which opened last year, said they were told little about what sort of information the agency collects. An NSA spokeswoman wouldn’t provide details about what is done at the facility. “The Utah Data Center is a U.S. Intelligence Community facility,” she said in an email. “The National Security Agency is the executive agent for the center, which houses systems that serve the Intelligence Community.”

#### Utah Data Center Polarizes Legislators

Palleata 15 (Damian, “A top secret NSA site draws swipes, shrugs”. Wall Street Journal. May 1) http://www.wsj.com/articles/a-top-secret-nsa-site-draws-swipes-shrugs-1430523735

Among the state’s predominantly Republican political leaders, support for the facility is mixed. Gov. Gary Herbert is a staunch backer, saying the data center provides high-paying jobs lured by Utah’s abundance of low-cost power. But other Republicans want the NSA to leave. Marc Roberts, a state representative from Santaquin, has introduced legislation that would shut off water to the Bluffdale facility, essentially forcing the NSA to shut down all of its computers, which use the water to cool. But Mr. Roberts’s legislation went nowhere in the Utah capitol, something he chalked up to a general confusion about what to do with the state’s large, secretive resident. “I think a lot of the representatives and senators, they don’t necessarily like what the NSA is doing or what they are hearing the NSA is doing, but they aren’t too sure of what to do about it or if we can do anything about it,” he said. In Washington, Senate Majority Leader Mitch McConnell (R., Ky.) and Senate Judiciary Committee Chairman Charles Grassley (R., Iowa) have warned that stripping the NSA’s powers could put Americans at risk because terrorists would be harder to track. Meanwhile, House Judiciary Committee Chairman Bob Goodlatte (R., Va.) passed a bill through his committee Thursday 25-2 that would end the bulk collection program but still allow the agency to obtain data on a one-off basis if approved by a secret court. It isn’t clear how that sort of arrangement might affect the facility in Bluffdale. The city’s mayor, Derk Timothy, who helped negotiate a contract last year to sell the Utah Data Center 56 million gallons of water for $300,000, has spent more than a year defending the agency’s presence with locals, saying the NSA has brought in jobs and helped develop the rural area’s infrastructure. He said he has no idea what goes on there, but he thinks that is for a reason. “You wouldn’t want them to tell you everything, then it’s like, ‘Hey, you dumb federal government, you laid out the whole plan so everybody interested in opposing our country is able to thwart your efforts,’ ” Mr. Timothy said. “But on the other hand, being the secret nature of it, it’s natural to wonder, what are they doing?”

### Data Centers Bad-Resources

#### Data centers are wasting resources

Gandhi 11 (Anshul Carnegie Mellon University, Pittsburgh, PA, US anshulg@cs.cmu.edu, July 28 2011 http://ieeexplore.ieee.org/xpls/abs\_all.jsp?arnumber=6008611)

Data centers are very expensive to operate due to the power and cooling requirements of IT equipment. The EPA predicts that energy consumption in data centers will exceed 100 billion kWh in 2011, at an estimated cost of $7.4 billion [10]. Rising energy costs, regulatory requirements and social concerns over green house gas emissions amplify the importance of energy efficiency. However, energy efficiency is for naught if the data center cannot deliver IT services according to predefined SLA or QoS goals, as SLA violations result in lost business revenue. For example, Amazon found that every additional 100ms of latency costs them a 1% loss in sales, and Google observed that an extra 500ms in search page generation time reduced traffic by 20% [2]. Today, SLA violations are often avoided by overprovisioning IT resources. This results in excessive energy consumption. Thus, an important question in data center resource management is how to correctly provision IT equipment, such that SLA requirements are met while minimizing energy consumption.

#### Massive amounts of water is required for data centers

Miller 12 (Rich on August 14, 2012 http://www.datacenterknowledge.com/archives/2012/08/14/data-center-water-use-moves-to-center-stage/)

The enormous volume of water required to cool high-density server farms is making water management a growing priority for data center operators. A 15-megawatt data center can use up to 360,000 gallons of water a day, according to one estimate. Why do data centers use so much water? The move to cloud computing is concentrating enormous computing power in mega-data centers containing hundreds of thousands of servers. In many designs, all the heat from those servers is managed through cooling towers, where hot waste water from the data center is cooled, with the heat being removed through evaporation. Most of the water that remains is returned to the data center cooling system, while some is drained out of the system to remove any sediment, a process known as blowdown.

#### Data centers require huge amounts of water

FitzGerald 15 (Drew The Wall Street Journal June 24, 2015 http://www.wsj.com/articles/SB10007111583511843695404581067903126039290)

Silicon Valley’s appetite for data is well known. Its thirst is less understood. Amid record drought in California and other parts of the American West, the machines that support everything from Instagram photos to Netflix movie marathons require substantial quantities of water for the air-conditioning systems needed to keep the servers cool. California has more than 800 data centers, the most of any state, according to an estimate by tech consultancy 451 Research LLC that excludes smaller computer rooms that businesses use. Based on that and estimates for water use, the state’s data centers consume roughly as much water in a year as 158,000 Olympic sized swimming pools. At a time when California authorities are telling waiters not to automatically offer water, data centers’ water use has largely escaped scrutiny. While data centers water needs are small relative to agriculture and power producers, their growth is entangling the state’s most successful business with its most pressing environmental problem

#### Data centers use massive amounts of energy

GLANZ SEPT. 22, 2012 (JAMES bureau chief of The New York Times[ http://www.nytimes.com/2012/09/23/technology/data-centers-waste-vast-amounts-of-energy-belying-industry-image.html?\_r=0)

A yearlong examination by The New York Times has revealed that this foundation of the information industry is sharply at odds with its image of sleek efficiency and environmental friendliness. Most data centers, by design, consume vast amounts of energy in an incongruously wasteful manner, interviews and documents show. Online companies typically run their facilities at maximum capacity around the clock, whatever the demand. As a result, data centers can waste 90 percent or more of the electricity they pull off the grid, The Times found. To guard against a power failure, they further rely on banks of generators that emit diesel exhaust. The pollution from data centers has increasingly been cited by the authorities for violating clean air regulations, documents show. In Silicon Valley, many data centers appear on the state government’s Toxic Air Contaminant Inventory, a roster of the area’s top stationary diesel polluters.

#### Data centers are extremely inefficient at handling energy

Golden 13 (Mark Golden, Precourt Institute for Energy at Stanford University July 19, 2013 https://energy.stanford.edu/news/data-centers-can-slash-co2-emissions-88-or-more)

“Pretty much every organization whose main job is not computing has done a poor job of improving efficiency,” said Eric Masanet of Northwestern University’s McCormick School of Engineering and a coauthor of the paper. “Some have made progress, but nowhere near what’s possible. Most can’t even tell you how many servers they have, let alone the servers’ utilization.” Department heads at such organizations typically want to keep control of their servers rather than centralize, which eliminates most potential optimization. And the managers who order and operate the equipment are often not accountable for energy costs or efficiency – a major institutional barrier to sustainable computing. “The utilities and IT departments have separate budgets, and neither operates with the goal of saving the company money overall,” said Koomey. “The IT people don’t care about putting in an efficient server, because they don’t pay the electric bill. Once you fix the institutional problems, then the company can move quickly, because the needed equipment is off-the-shelf and the energy management practices are well understood.”

### Data Centers Bad-Water

#### **The UDC guzzles water—6.6 million gallon in August of 14 alone.**

Carlisle, 15 (Nate, Justice and Safety Reporter for the Salt Lake Tribune, “NSA Utah Data Center using more water,” *The Salt Lake Tribune*,First Published Feb 02 2015)

More water poured into the National Security Agency's Utah Data Center in 2014 than in previous years, but the facility is still paying for water that it is not using.¶ Records provided by Bluffdale show Data Center water usage spiked to 6.6 million gallons during August. For the months of January through November — the time frame reviewed by The Tribune — the water usage was higher than it was for those months in 2013.¶ The NSA paid Bulffdale $31,692.10 for the months of January through March, and again for June through November.¶ In the months of April and May, the bill was $36,417 per month even though the Utah Data Center used less water than it would in the summer.¶ Bluffdale City Manager Mark Reid on Friday said he did not know why the April and May bills were greater. Bluffdale city attorney Vaughn Pickell said the city had no comment on the NSA's water bill.¶ NSA spokeswoman Vanee Vines on Friday declined to discuss water usage at the Utah Data Center.¶ "We are unable to discuss the secure operations of the Utah Data Center," Vines said. "Construction has been completed."¶ The NSA had previously stated the Utah Data Center would be operational in the fall of 2013. In October of that year, the Wall Street Journal reported electrical problems were hampering the facility.¶ Water usage was more sporadic in 2013 — peaking sharply in July then plummeting through the fall before increasing again in December.¶ In 2014, the changes were not as dramatic.¶ Water is essential to help cool the facility and computing components for the center, a massive digital storage hub for the NSA and other intelligence agencies.¶ U.S. Army Corps of Engineer plans called for the center to use 1.7 million gallons a day. Bluffdale City Council minutes indicate that figure was later reduced to 1.2 million gallons a day.

#### Utah is on the brink of a water shortage

Cathy Allred 2014 (Cathy Allred,

Lehi City administrators have alerted businesses and residents that municipal water is in cautionary yellow phase II based on its Lehi Water Shortage Plan for a moderate water shortage. "We are trying to be conservative. We are trying to be prepared. It’s an opportunity for us to again educate our residents about the use of water,” said Derek Todd, Lehi city administrator. The green first phase is voluntary conservation and the third or red phase is a more stringent mandatory plan. Phase II is being enacted in Lehi during the community’s peak irrigation season because local pressurized irrigation levels are between 50 to 70 percent of capacity. Sprinkler irrigation is prohibited in Lehi and the other cities between 10 a.m. and 6 p.m. and limited to three days a week according to city or county street addresses. Those with odd-numbered addresses will water Mondays, Wednesdays and Fridays. Even-numbered addresses are to water on Tuesdays, Thursdays, Saturdays. Spot watering is allowed on Sundays. Several voluntary water conservation programs in Utah County suggest using the same guidelines. American Fork as a city has already begun its mandatory conservation measures. Most mandatory conservation ordinances go into effect June 1. “We are going into the yellow caution phase where we conserve the water we have so we have enough to last us the rest of the year,” Lehi Mayor Bert Wilson said. Hard surface washing is also prohibited, except for health and safety reasons. City staff will continuously monitor pressurized irrigation water levels and change the water shortage phase when necessary. “We are excited to see how that goes. We have done a lot for our water system this year, but we still need to be cautious,” Todd said. Two wells are being drilled to add more water to the system and two new reservoirs are ready to come online. The second driest state for precipitation in the nation, Utah is beginning its third season of a drought.

#### NSA Utah Data Center using more water

Nate Carlisle, 2015 ( nate Carlisle http://www.sltrib.com/home/2118801-155/nsa-utah-data-center-using-more, feb. 2 2015 )

More water poured into the National Security Agency's Utah Data Center in 2014 than in previous years, but the facility is still paying for water that it is not using. Records provided by Bluffdale show Data Center water usage spiked to 6.6 million gallons during August. For the months of January through November — the time frame reviewed by The Tribune — the water usage was higher than it was for those months in 2013. The NSA paid Bulffdale $31,692.10 for the months of January through March, and again for June through November. In the months of April and May, the bill was $36,417 per month even though the Utah Data Center used less water than it would in the summer. Bluffdale City Manager Mark Reid on Friday said he did not know why the April and May bills were greater. Bluffdale city attorney Vaughn Pickell said the city had no comment on the NSA's water bill. NSA spokeswoman Vanee Vines on Friday declined to discuss water usage at the Utah Data Center. "We are unable to discuss the secure operations of the Utah Data Center," Vines said. "Construction has been completed." The NSA had previously stated the Utah Data Center would be operational in the fall of 2013. In October of that year, the Wall Street Journal reported electrical problems were hampering the facility. Water usage was more sporadic in 2013 — peaking sharply in July then plummeting through the fall before increasing again in December. In 2014, the changes were not as dramatic. Water is essential to help cool the facility and computing components for the center, a massive digital storage hub for the NSA and other intelligence agencies. U.S. Army Corps of Engineer plans called for the center to use 1.7 million gallons a day. Bluffdale City Council minutes indicate that figure was later reduced to 1.2 million gallons a day. Bluffdale built a $3 million water-delivery system for the center. To ensure it would be able to repay the bond, the city required minimum monthly payments — called "take or pay" — from the NSA. But the contract assumes the NSA will exceed those minimums, at which point Bluffdale begins charging the NSA at a rate that currently amounts to $2.05 per 1,000 gallons. The version of the contract between the NSA and Bluffdale released by the city redacts the planned amounts of the minimum payments and the Utah Data Center's projected water usage. It is unclear how much more water the NSA could receive with the minimum payment. A bill in the Utah Legislature targets the cooperation Bluffdale and the state have given the NSA. HB150 sponsored by Marc Roberts, R-Santaquin, requires that state and local governments "refuse material support or assistance to any federal data collection and surveillance agency." A current draft of the bill says existing agreements with such surveillance agencies can continue through the length of the contract, but may not be renewed after July 1. At a hearing in November, lawmakers expressed concern, but no outright opposition, to Roberts' bill. They were worried it was too broad. A fiscal note attached to HB150 this month says that if interpreted narrowly, the bill will not impact the state's budget. If interpreted broadly, the fiscal note says, the bill would prohibit Utah from taking $458.3 million in federal funds in the current fiscal year and cost Utah $1.75 billion in ongoing federal funds beginning next year.

#### Data centers use too much power

Offnow 15 (offnow http://www.offnow.org/locations march 2015)

the Baltimore Sun reported that the NSA had maxed out capacity of the Baltimore-area power grid via Baltimore Gas and Electric. Insiders reported that “The NSA is already unable to install some costly and sophisticated new equipment. At minimum, the problem could produce disruptions leading to outages and power surges. At worst, it could force a virtual shutdown of the agency.” Provided by Baltimore Gas and Electric, the cost of electricity at Fort Meade was probably one of NSA’s single biggest expenses, according to Matthew Aid, author of The Secret Sentry: The Untold History of the National Security Agency (Bloomsbury Press, 2009). He estimated the agency could end up spending 95 percent less on electricity in Utah than in Maryland.

### **Data Centers Bad-Privacy**

#### Data Center Extends Ability to Over Step Privacy Rights

Irving 13 (Clive, “Behold the NSA’s Dark Star: The Utah Data Center”. DailyBeast. June 8) http://www.thedailybeast.com/articles/2013/06/08/behold-the-nsa-s-dark-star-the-utah-data-center.html

The national-security industrial complex is now of the size, power, and influence of the military-industrial complex of the Cold War, which President Eisenhower first defined and warned of. As then, this complex uses the national interest as a reason for having to operate in secrecy, and invokes patriotism—literally in the PATRIOT Act—to create a political consensus. Nineteen terrorists with minimal technology—box cutters—have enabled the counterterrorism industry to enjoy unbounded reach. White House Deputy Press Secretary Josh Earnest used the familiar argument to defend the newly disclosed surveillance: it was, he said, “a critical tool in protecting the nation from terror threats as it allows counterterrorism personnel to discover whether known or suspected terrorists have been in contact with other persons who may be engaged in terror activities, particularly people located inside the United States.” That’s actually a simplification. Surveillance has two fundamental purposes: to track the known and discover the unknown. It’s hard to comprehend the science involved. How, for example, do you cull billions of bytes of data a second in a way that discriminates between the useless and the essential? Only one thing is for sure, and that is that the policy driving the velocity of the NSA’s ever-expanding sweeps is first to make those sweeps as global and indiscriminate as possible and then to apply algorithms able to instantly see the significant from the insignificant. If only it were that simple. It is patently easy to defend the resources devoted to intelligence gathering by saying that many attacks have been thwarted, without saying what and where they were. Neither the Boston Marathon atrocity nor the London assassination of a British soldier were detected in advance, even though intelligence services in both countries had the perpetrators on their radar. There is a certain kind of intellectual depravity in trying to have us accept that all surveillance is good for us. Politicians of both parties who now say there is nothing new in what has been revealed, that this was all authorized and kosher, are captives of this depravity, because they don’t really know any more than we do where to draw the line. Where is it absolutely essential to violate privacy and where not? This is made even worse by the cover of enormous technical complexity. At least the Stasi’s low-tech methods could be seen for what they were, part of a cumbersome and gross bureaucratic machine, essentially human in its systems, allowing culpability to be clearly assigned. In our case there is the Dark Star factor, like the Utah operation, working on robotic principles, not dependent on putting bugs in chandeliers, leaving no fingerprints, and capable of awesome penetration. We have the ultimate machine of the Paranoid State, an Orwellian apparatus that intoxicates its operators with its efficiency, enthralls its masters with its omniscience, and emasculates its political overseers with its promise of efficacy.

### Data Centers Bad-Economics

#### Utah Data Center Not Economical

DailyMail 13 (“Utah Data Center: The NSA’s two new spying facilities storing your data is seven times the size of the pentagon”. Daily Mail. July 27) http://www.dailymail.co.uk/news/article-2379575/Utah-Data-Center-The-NSAs-new-spying-facilities-storing-data-SEVEN-TIMES-size-Pentagon.html

The NSA is now building a facility that will make it more than seven times the size of the Pentagon, making the secretive compounds the biggest in the country. In addition to building a $1.9billion data center in Utah, crews also started construction on a computing center that is expected to cost $792million near Baltimore. Together, the two facilities total 228 acres, much of which is dedicated to the collection of emails and phone calls that it was recently revealed the NSA stores without an individual knowledge. Much attention has been paid to the secretive practices of the NSA since consultant Edward Snowden leaked classified documents proving that the intelligence agency had free reign to the electronic footprint of people, both in and out of the country, who used certain phone carriers. NSA official Harvey Davis told Defense One that the Utah facility is 'only brick and mortar' but they need the space because 'it's required to be big' as a result of their growing surveillance. 'I think we're crossing into content,' he told the site. Mike Baker, a former cover field operations officer for the CIA, told Fox News that the paranoia surrounding the billion dollar project was understandable yet exaggerated, adding that the main problem was the size of the data collection warehouse. 'The fact that they’re building a new data center isn’t news,' Baker told Fox News. 'They’ve got several other [similar] facilities. The size of this is what is creating the stir.' Once built, the million square foot centre will be more than five times the size of the US Capitol, and will use an estimated $40m of electricity every year, according to one estimate.

### Data Centers Bad-General

#### Data Center Uneffective

Hill 13 (Kashmir, “The NSA’s hugely expensive utah data center has major electrical problems and basically isn’t working, Forbes. October 7) http://www.forbes.com/sites/kashmirhill/2013/10/07/the-nsas-hugely-expensive-utah-data-center-has-major-electrical-problems-and-basically-isnt-working/

Well, this is good news for those with privacy concerns about the NSA and terrible news for those concerned about government spending. The National Security Agency’s new billion-dollar-plus data center in Bluffdale, Utah was supposed to go online in September, but the Wall Street Journal’s Siobhan Gorman reports that it has major electrical problems and that the facility known as “the country’s biggest spy center” is presently nearly unusable: Chronic electrical surges at the massive new data-storage facility central to the National Security Agency’s spying operation have destroyed hundreds of thousands of dollars worth of machinery and delayed the center’s opening for a year, according to project documents and current and former officials. There have been 10 meltdowns in the past 13 months that have prevented the NSA from using computers at its new Utah data-storage center, slated to be the spy agency’s largest, according to project documents reviewed by The Wall Street Journal. Glenn Greenwald isn’t the only one dropping explosive material on the NSA. According to the Wall Street Journal, the data center’s electrical problems include “arc failures,” a.k.a. “a flash of lightning inside a 2-foot box,” which results in fiery explosions, melted metal and circuit failure. More terrifying, this has happened ten times, most recently on September 25, reports the WSJ, which reviewed project documents and reports and talked to contractors involved. The report blames the NSA “fast tracking” the Utah project and thus bypassing “regular quality controls in design and construction.” Whoops. Worse, it sounds from the WSJ’s reporting as if the contractors — architectural firm KlingStubbins which designed the electrical system, along with construction companies Balfour Beatty Construction, DPR Construction and Big-D Construction Corp — are still scrambling to figure out what’s causing the problems. The Army Corps of Engineers sent its “Tiger Team” to sort things out this summer but they were unable to pinpoint exactly what’s wrong. “The problem, and we all know it, is that they put the appliances too close together,” a person familar with the database construction told FORBES, describing the arcs as creating “kill zones.” “They used wiring that’s not adequate to the task. We all talked about the fact that it wasn’t going to work.” “The Utah Data Center is one of the U.S. Defense Department’s largest ongoing construction projects in the continental United States,” says an NSA spokesperson. “This Intelligence Community facility will host the power, space, cooling, and communications needed to support specialized computing. The center sits on approximately 247 acres, includes 1.2 million square feet of enclosed space, and is completing acceptance testing. The failures that occurred during testing have been mitigated. A project of this magnitude requires stringent management, oversight, and testing before the government accepts any building.” When I wrote about the Utah data center holding less information than was previously thought given the current limitations of technology in this space, some critics scoffed. They suggested that the NSA is far more advanced in its technology than companies like Google and Facebook with which I was drawing comparisons. This report from the WSJ about the flawed plans for the data center encourages some skepticism about NSA tech. And it definitely raises questions about the NSA budget. The center itself cost over a billion dollars to build, has a $1 million+ monthly electricity bill, and has cost up to $100,000 each time a “kill zone” happens. Those numbers are as disturbing as the privacy concerns raised by the Snowden leaks.

### Data Centers Bad-Cyber Security

#### The UDC makes state-run utilities a target for cyber terrorism

Associated Press 15 (“Cyber-attacks rising in Utah, likely due to NSA facility,” *Associated Press*, February 6, http://ksn.com/2015/02/06/cyber-attacks-rising-in-utah-likely-due-to-nsa-facility/)

But both Forno and Junio agree the NSA data center could draw the attention of hackers who think they can target state-run utilities that power the center. Being able to disrupt an NSA operation in any way would bring international notoriety to a foreign state or criminal group, Junio said.¶ State officials acknowledge that part of the increase is driven by an overall rise in hacking across the country. Hackers’ motivations vary, and it was impossible to determine what might be behind the activity in Utah.¶ Some steal personal information, like customer lists, to commit identity theft. Some take control of email servers to steal messages, send unwanted advertising or disguise the origin of their communications. Some steal corporate or government secrets from email or cloud servers, or use unlocked file servers as digital “dead drops” for their hacking tools, pirated movies, stolen files and more.¶ For hackers seeking notoriety, the NSA would be a prized target because it employs the world’s best hackers and routinely gives advice about how to keep computers safe from online criminals.

#### UDC causes cyber terrorism

Associated Press 15 (“Cyber-attacks rising in Utah, likely due to NSA facility,” *Associated Press*, February 6, http://ksn.com/2015/02/06/cyber-attacks-rising-in-utah-likely-due-to-nsa-facility/)

SALT LAKE CITY (AP) — Utah state officials have seen what they describe as a sharp uptick in attempts to hack into state computers in the last two years, and they think it related to the NSA data center south of Salt Lake City.¶ The increase began in early 2013 as international attention focused on the NSA’s $1.7 billion warehouse to store massive amounts of information gathered secretly from phone calls and emails.¶ “In the cyber world, that’s a big deal,” Utah Public Safety Commissioner Keith Squires told a state legislative committee this week.¶ While most of the attempts are likely innocuous, cyber experts say it is possible low-level hackers, “hactivists” unhappy with the NSA’s tactics, and some foreign criminal groups might erroneously think the state systems are linked to the NSA.¶ “Maybe these hackers are thinking: ‘If we can attack state systems, we can get info that NSA isn’t releasing,” said Richard Forno, director of the University of Maryland, Baltimore County’s, graduate cybersecurity program.¶ The state tracks the attempts with an automated system it purchased after a breach of health care information in 2012. The system detects, stops and counts the attempts to get into the computers, Squires said.¶ With that new equipment in place in January 2013, the state was seeing an average of 50,000 a day with spikes up to 20 million, Squires told The Associated Press. In February 2013, the number rose to an average of 75 million attacks a day, with up to 500 million on some days.¶ Attacks include direct attacks on websites, emails fishing for passwords, and something called “port scans,” where people probe a computer looking for weak spots.

#### While hackers get better tools, the good guys will be in short supply

Mike Horn 2013 (mike horn http://venturebeat.com/2013/12/31/security-in-2014/ December 31, 2013)

For the casual observer, security predictions for 2014 might be as simple as declaring “more and scarier threats,” but subscribing to that view is a gross over-simplification. Security isn’t just about tools or attacks, but about the people involved. We see people, process, and technology changing in 2014 within the security industry. We repeatedly hear that it takes up to eight years for security staff to develop the skills, insights, and raw operational ability to understand and process security breaches effectively. Some universities have just launched “IT Security” programs in 2013, which is a good start, but we predict that even with the launch of education programs, the curricula will be improperly balanced, with the majority of students and programs focusing on forensics and detection, where many automated tools already exist. Schools have started to recognize this problem, but are not immediately diversifying the education. This leads to a greater shortage of skilled security analysts and further leads to workforce poaching and newsworthy hiring bonuses for security analysts. While people don’t like their actions being tracked in the general public, businesses can use employee behavior as a tool for threat identification. If a system has been compromised, it might use an employee’s identity to access systems or escalate privileges. Any change in privileged access patterns is an anomaly worth looking into. As a result, in 2014 companies will start to monitor network access patterns from personnel more aggressively. Once new Common Vulnerabilities and Exposures (CVEs) are publicly acknowledged, we expect even shorter times to develop kit-based exploits and widespread release. Just as there are software automation tools for rapid software development, those tools and technologies will be applied more frequently to malware. The speed at which Cutwail developers replaced the BlackHole exploit kit with the Magnitude kit is just a sample of what is to come. In 2014, we’ll see malware development modularized with push-button vulnerability inclusion in an interface as simple as that of Zeus Builder. In 2013, we saw a confirmation that malware developers could subscribe to “anti-virus detection as a service” tools to make sure that their attacks had no or limited AV detection. At the same time, there was a rise in the benign behavior of malware — creating legitimate files, dropping dozens of non-malicious files, HTTP GET requests to legitimate sites, and more. Of course, if only one out of 100 files was malicious and only one of 15 network calls was malicious, the attackers could run wild security analysts who were busy checking the other 99 files and 14 non-malicious sites. These will include the human behavior analysis discussed earlier, as well as additional forms of anomaly detection, improved sandboxing, anti-evasion analysis tools, and real-time distribution of new threat data. New detection capabilities will also put pressure on security staff to learn about new technologies as well as evaluate, buy, and implement the technologies they choose. Wait, did we say there was a skills shortage? Individual technologies may provide single source filtering, but security analysts will still be faced with processing security alerts from legacy detection tools as well as from newer detection tools — filtered or not. To solve this problem, security integration and coordination providers will gain ground, as will attempts at open consortia for sharing and processing security data. By the end of 2014, organizations will realize that post-detection security alerts are a fact of life, and that their incident response and containment teams need to catch up. Educators and chief security officers will embrace the fact that detected threats need rapid containment, even before full forensics can be completed. I am a bit conservative on these views, but forward-looking security teams are probably seeing these trends take shape now and are already preparing.

#### Massive Utah cyberattacks — up to 300 million per day — may be aimed at NSA facility

Lee Davidson 15 (lee davidson http://www.sltrib.com/news/2135491-155/massive-utah-cyber-attacks-may-be feb 10 2015)

Five years ago, Utah government computer systems faced 25,000 to 30,000 attempted cyberattacks every day. At the time, Utah Public Safety Commissioner Keith Squires thought that was massive. "But this last year we have had spikes of over 300 million attacks against the state databases" each day: a 10,000-fold increase. Why? Squires says it is probably because Utah is home to the new, secretive National Security Agency computer center, and hackers believe they can somehow get to it through state computer systems. "I really do believe it was all the attention drawn to the NSA facility. In the cyberworld, that's a big deal," Squires told a legislative budget committee Tuesday. "I watched as those increases jumped so much over the last few years. And talking to counterparts in other states, they weren't seeing that amount of increase like we were." Rep. Curt Oda, R-Clearfield, said the state should approach NSA or the federal government for money to help in defending against the cyberattacks. "They are costing us a ton of money," Oda said. "They need to pony up." Squires — whose department includes a team that investigates cybercrimes not only against the state, but also against its residents — said any time the state finds itself in controversy, cyberattacks seem to increase. For example, Col. Daniel Fuhr, superintendent of the Utah Highway Patrol, said news media photos of a controversial shooting of a young black man last year in Saratoga Springs showed a marked UHP car in the background. Even though UHP was not involved in the shooting, Fuhr immediately had his personal credit cards and bank accounts come under heavy cyberattack. He said it led to "long nights of ensuring your credit card numbers are intact, and all your bank numbers are changed over. My poor sweet wife was livid." Squires said the leap in cyberattacks "tells you just how exponentially this has increased over the years, how many more criminals are realizing it is easier to steal from individuals, and businesses and government online and [with] less chance of getting caught" than robbing a bank. Rep. Eric Hutchings, R-Kearns, co-chairman of the committee, said it shows the increasing value of the state cybercrimes unit — which he added he personally realized when his identity was stolen and a criminal in Texas charged $80,000 worth of business-telephone equipment to him. He said the company that was victimized "just reported it to insurance, and wrote it off," even though Hutchings noted the amount stolen was equivalent to 16 typical bank robberies. "What a wonderful criminal environment to be in, where people don't even look for you," Hutchings said. "But if you rob 16 banks, you would be on the FBI's most wanted [list]. You rob it out of my credit, 'Eh, whatever, it's the cost of doing business.' "

#### Social Security Numbers Of Every Federal Employee Stolen In Data Breach, Union Says

AP 2015 (ap news http://www.huffingtonpost.com/2015/06/11/federal-government-data-breach\_n\_7564218.html June 2015)

Hackers stole personnel data and Social Security numbers for every federal employee, a government worker union said Thursday, asserting that the cyber theft of U.S. employee information was more damaging than the Obama administration has acknowledged. Sen. Harry Reid, the Democratic leader, said on the Senate floor that the December hack into Office of Personnel Management data was carried out by "the Chinese" without specifying whether he meant the Chinese government or individuals. Reid is one of eight lawmakers briefed on the most secret intelligence information. U.S. officials have declined to publicly blame China, which has denied involvement. J. David Cox, president of the American Federation of Government Employees, said in a letter to OPM director Katherine Archuleta that based on the incomplete information the union received from OPM, "We believe that the Central Personnel Data File was the targeted database, and that the hackers are now in possession of all personnel data for every federal employee, every federal retiree, and up to one million former federal employees." The OPM data file contains the records of non-military, non-intelligence executive branch employees, which covers most federal civilian employees but not, for example, members of Congress and their staffs. The union believes the hackers stole military records and veterans' status information, address, birth date, job and pay history, health insurance, life insurance and pension information; and age, gender and race data, he said. The letter was obtained by The Associated Press. The union, which does not have direct access to the investigation, said it is basing its assessment on "sketchy" information provided by OPM. The agency has sought to downplay the damage, saying what was taken "could include" personnel file information such as Social Security numbers and birth dates. "We believe that Social Security numbers were not encrypted, a cybersecurity failure that is absolutely indefensible and outrageous," Cox said in the letter. The union called the breach "an abysmal failure on the part of the agency to guard data that has been entrusted to it by the federal workforce." Samuel Schumach, an OPM spokesman, said that "for security reasons, we will not discuss specifics of the information that might have been compromised." The central personnel data file contains up to 780 separate pieces of information about an employee. Cox complained in the letter that "very little substantive information has been shared with us, despite the fact that we represent more than 670,000 federal employees in departments and agencies throughout the executive branch." The union's release and Reid's comment in the Senate put into sharper focus what is looking like a massive cyber espionage success by China. Sen. Susan Collins, an intelligence committee member, has also said the hack came from China. Mike Rogers, the former chairman of the House intelligence committee, said last week that Chinese intelligence agencies have for some time been seeking to assemble a database of information about Americans. Those personal details can be used for blackmail, or also to shape bogus emails designed to appear legitimate while injecting spyware on the networks of government agencies or businesses Chinese hackers are trying to penetrate. U.S. intelligence officials say China, like the U.S., spies for national security advantage. Unlike the U.S., they say, China also engages in large-scale theft of corporate secrets for the benefit of state-sponsored enterprises that compete with Western companies. Nearly every major U.S. company has been hacked from China, they say. The Office of Personnel Management is also a repository for extremely sensitive information assembled through background investigations of employees and contractors who hold security clearances. OPM's Schumach has said there is "no evidence" that information was taken. But there is growing skepticism among intelligence agency employees and contractors about that claim. In the Senate on Thursday, Democrats blocked a Republican effort to add a cybersecurity bill to a sweeping defense measure. The vote was 56-40, four votes short of the number necessary. Democrats had warned of the dangers of cyberspying after the theft of government personnel files, but Democrats voted against moving ahead on the legislation, frustrated with the GOP-led effort to tie the two bills together. President Barack Obama has threatened to veto the defense legislation over budget changes by the GOP. "The issue of cybersecurity is simply too important to be used as a political chit and tucked away in separate legislation." said Sen. Chris Coons, D-Del.

### Energy Use Bad

#### Energy is the largest contributor to co2 emissions

EPA 15 (May 7, 2015 http://www.epa.gov/climatechange/ghgemissions/gases/co2.html )

Carbon dioxide (CO2) is the primary greenhouse gas emitted through human activities. In 2013, CO2 accounted for about 82% of all U.S. greenhouse gas emissions from human activities. Carbon dioxide is naturally present in the atmosphere as part of the Earth's carbon cycle (the natural circulation of carbon among the atmosphere, oceans, soil, plants, and animals). Human activities are altering the carbon cycle—both by adding more CO2 to the atmosphere and by influencing the ability of natural sinks, like forests, to remove CO2 from the atmosphere. While CO2 emissions come from a variety of natural sources, human-related emissions are responsible for the increase that has occurred in the atmosphere since the industrial revolution. Electricity is a significant source of energy in the United States and is used to power homes, business, and industry. The combustion of fossil fuels to generate electricity is the largest single source of CO2 emissions in the nation, accounting for about 37% of total U.S. CO2 emissions and 31% of total U.S. greenhouse gas emissions in 2013. The type of fossil fuel used to generate electricity will emit different amounts of CO2. To produce a given amount of electricity, burning coal will produce more CO2 than oil or natural gas.

#### Co2 increases, increase temperature

GPwayne 2015 (https://www.skepticalscience.com/empirical-evidence-for-co2-enhanced-greenhouse-effect.htm)

The greenhouse effect works like this: Energy arrives from the sun in the form of visible light and ultraviolet radiation. The Earth then emits some of this energy as infrared radiation. Greenhouse gases in the atmosphere 'capture' some of this heat, then re-emit it in all directions - including back to the Earth's surface. Through this process, CO2 and other greenhouse gases keep the Earth’s surface 33°Celsius (59.4°F) warmer than it would be without them. We have added 42% more CO2, and temperatures have gone up. There should be some evidence that links CO2 to the temperature rise. So far, the average global temperature has gone up by about 0.8 degrees C (1.4°F): "According to an ongoing temperature analysis conducted by scientists at NASA’s Goddard Institute for Space Studies (GISS)…the average global temperature on Earth has increased by about 0.8°Celsius (1.4°Fahrenheit) since 1880. Two-thirds of the warming has occurred since 1975, at a rate of roughly 0.15-0.20°C per decade."

### Global Warming Impact

#### Global warming causes massive problems globally

Shaftel 15 (Holly July 8, 2015 http://climate.nasa.gov/effects/)

Global climate change has already had observable effects on the environment. Glaciers have shrunk, ice on rivers and lakes is breaking up earlier, plant and animal ranges have shifted and trees are flowering sooner. Effects that scientists had predicted in the past would result from global climate change are now occurring: loss of sea ice, accelerated sea level rise and longer, more intense heat waves. Taken as a whole, the range of published evidence indicates that the net damage costs of climate change are likely to be significant and to increase over time. - Intergovernmental Panel on Climate Change Scientists have high confidence that global temperatures will continue to rise for decades to come, largely due to greenhouse gasses produced by human activities. The Intergovernmental Panel on Climate Change (IPCC), which includes more than 1,300 scientists from the United States and other countries, forecasts a temperature rise of 2.5 to 10 degrees Fahrenheit over the next century. According to the IPCC, the extent of climate change effects on individual regions will vary over time and with the ability of different societal and environmental systems to mitigate or adapt to change. The IPCC predicts that increases in global mean temperature of less than 1.8 to 5.4 degrees Fahrenheit (1 to 3 degrees Celsius) above 1990 levels will produce beneficial impacts in some regions and harmful ones in others. Net annual costs will increase over time as global temperatures increase. "Taken as a whole," the IPCC states, "the range of published evidence indicates that the net damage costs of climate change are likely to be significant and to increase over time." 1 Below are some of the impacts that are currently visible throughout the U.S. and will continue to affect these regions, according to the Third National Climate Assessment Report 2, released by the U.S. Global Change Research Program: Northeast. Heat waves, heavy downpours, and sea level rise pose growing challenges to many aspects of life in the Northeast. Infrastructure, agriculture, fisheries, and ecosystems will be increasingly compromised. Many states and cities are beginning to incorporate climate change into their planning. Northwest. Changes in the timing of streamflow reduce water supplies for competing demands. Sea level rise, erosion, inundation, risks to infrastructure, and increasing ocean acidity pose major threats. Increasing wildfire, insect outbreaks, and tree diseases are causing widespread tree die-off. Southeast. Sea level rise poses widespread and continuing threats to the region’s economy and environment. Extreme heat will affect health, energy, agriculture, and more. Decreased water availability will have economic and environmental impacts. Midwest. Extreme heat, heavy downpours, and flooding will affect infrastructure, health, agriculture, forestry, transportation, air and water quality, and more. Climate change will also exacerbate a range of risks to the Great Lakes. Southwest. Increased heat, drought, and insect outbreaks, all linked to climate change, have increased wildfires. Declining water supplies, reduced agricultural yields, health impacts in cities due to heat, and flooding and erosion in coastal areas are additional concerns.

# Answers to Neg Stuff

### AT: T-Domestic

#### Multiple loopholes allow the NSA to engage in domestic surveillance under Section 702

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

What this means is that even if the NSA applies an IP filter to eliminate communications that appear to be within the United States, it may nevertheless monitor domestic conversations by nature of them being routed through foreign servers. In this manner, a student in Chicago may send an e-mail to a student in Boston [\*164] that gets routed through a server in Canada. Through no intent or design of the individual in Chicago, the message becomes international and thus subject to NSA surveillance.¶ Third, further collection of domestic conversations takes place through the NSA's intercept of what are called multi-communication transactions, or MCTs. It is important to distinguish here between a transaction and a communication. Some transactions have only single communications associated with them. These are referred to as SCTs. Other transactions contain multiple communications. If even one of the communications in an MCT falls within the NSA's surveillance, all of the communications bundled into the MCT are collected.¶ The consequence is of significant import. FISC estimated in 2011 that somewhere between 300,000 and 400,000 MCTs were being collected annually on the basis of "about" communication--where the "active user" was not the target. So hundreds of thousands of communications were being collected that did not include the target as either the sender or the recipient of the communication. n183

#### The NSA uses 702 loopholes to subvert Section 702 and 703—allows surveillance on domestic targets

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

Targeting procedures require NSA analysts to make a determination regarding the location and legal status of a potential target (together referred to as the "foreignness determination"). n184 Two related interpretations have allowed the NSA to push the statutory limits: first is the assumption, having looked at the evidence available, that a target outside the United States or in an unknown location is a non-U.S. person, absent evidence to the contrary; second, where the target is not known to be inside the United States, the NSA presumes that the target is located outside domestic borders. These assumptions raise question about the level of due diligence required to ascertain status and location, tilt the deck in favor of allowing collection, and create, in at least some cases, a circular pattern.¶ The FAA is largely silent about what burden must be borne by the government to establish whether the target is a U.S. person. Instead, Section 702 directs the Attorney General to adopt targeting procedures reasonably designed (a) to ensure acquisition is limited to persons reasonably believed to be outside U.S.; and (b) to prevent the acquisition of domestic communications. n185¶ In other words, the statute only requires that the NSA not know (a) that the target is in the U.S.; or (b) that it is intercepting entirely domestic communications. There is nothing in the targeting requirements requiring intelligence agencies to take certain steps to ascertain whether the target is a U.S. person or what must be done to ascertain the target's location.¶ Sections 703 and 704, which are designed to deal with U.S. persons, say nothing in turn about what is required to demonstrate whether a target either is or is not a U.S. person. n186 Instead, these provisions address situations where the applicant has probable cause to believe that the target is a person outside the United States and is a foreign power, an agent of a foreign power, or an officer or employee thereof. n187¶ [\*166] In the absence of statutory guidance, the NSA interprets the statute to allow the agency to assume that the target is a non-U.S. person where there is not sufficient evidence to the contrary. n188 The NSA's minimization procedures explain:¶ A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person. n189¶ Thus, an important question is what specific steps must the NSA take in order to determine the legal status of the target. n190¶ The Targeting Procedures do not set a high bar. When referring to databases or other surveillance systems that could be consulted to determine whether the target is a U.S. person or a non-U.S. person, the document uses the word "may"--the present tense articulation of a mere possibility. As an auxiliary verb, it adds a functional meaning to the resultant clause--specifically, in the case of "may," to intone possibility in a manner that equally incorporates the possibility of "may not." The NSA thus may consult its databases to determine whether a target is a U.S. person. It also may decide not to. At no point does the document itself suggest what the NSA "must" do. n191

#### We have congressional intent on our side. Congress intended the NSA to expand domestic surveillance under Section 702.

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

In 2008 Congress anticipated that the intelligence community would inadvertently collect U.S. persons' communications in the process of targeting non-U.S. persons under Section 702. Legislators acknowledged the possibility, and Congress inserted special back-end protections via minimization procedures and the inclusion of explicit limits. But outside of a handful of exceptions, members did not publicly anticipate that the executive would engage in such large-scale, programmatic collection, so as to undermine Sections 703 and 704. n216 Legislators who did publicly recognize the potential for programmatic surveillance opposed the statute on precisely those grounds. Not a single member who recognized the potential for programmatic surveillance defended the use of the authorities in this way.¶ Even if Congress did not initially understand the implications of the FAA, the executive subsequently informed the House and Senate Intelligence Committees about PRISM and upstream collection. Congress's subsequent failure to end the programs--indeed, its decision to reauthorize the FAA in 2012--suggests that the legislature intended the intelligence community to continue interpreting the statute in a manner that supported the programs. Arguments that the legislature was too hampered by classification to either read or respond to intelligence community reports fail to appreciate Congress's interpretation of its own authorities with regard to classification.

### AT: Terrorism DA

#### Turn: Mass data collection trades off with targeted surveillance that stops terrorism—every successful NSA action proves we control the link.

Schneier, 15 (Bruce (2015-03-02). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (p. 139-41). W. W. Norton & Company. Kindle Edition.)

This point was made in the 9/ 11 Commission Report. That report described a failure to “connect the dots,” which proponents of mass surveillance claim requires collection of more data. But what the report actually said was that the intelligence community had all the information about the plot without mass surveillance, and that the failures were the result of inadequate analysis. Mass surveillance didn’t catch underwear bomber Umar Farouk Abdulmutallab in 2006, even though his father had repeatedly warned the US government that he was dangerous. And the liquid bombers (they’re the reason governments prohibit passengers from bringing large bottles of liquids, creams, and gels on airplanes in their carry-on luggage) were captured in 2006 in their London apartment not due to mass surveillance but through traditional investigative police work. Whenever we learn about an NSA success, it invariably comes from targeted surveillance rather than from mass surveillance. One analysis showed that the FBI identifies potential terrorist plots from reports of suspicious activity, reports of plots, and investigations of other, unrelated, crimes. This is a critical point. Ubiquitous surveillance and data mining are not suitable tools for finding dedicated criminals or terrorists. We taxpayers are wasting billions on mass-surveillance programs, and not getting the security we’ve been promised. More importantly, the money we’re wasting on these ineffective surveillance programs is not being spent on investigation, intelligence, and emergency response: tactics that have been proven to work.¶ Mass surveillance and data mining are much more suitable for tasks of population discrimination: finding people with certain political beliefs, people who are friends with certain individuals, people who are members of secret societies, and people who attend certain meetings and rallies. Those are all individuals of interest to a government intent on social control like China. The reason data mining works to find them is that, like credit card fraudsters, political dissidents are likely to share a well-defined profile. Additionally, under authoritarian rule the inevitable false alarms are less of a problem; charging innocent people with sedition instills fear in the populace. More than just being ineffective, the NSA’s surveillance efforts have actually made us less secure. In order to understand how, I need to explain a bit about Internet security, encryption, and computer vulnerabilities. The following three sections are short but important.

#### AT Terrorism: Mass surveillance cannot prevent terrorism for 3 reasons: 1) false positives, 2) uniqueness of attacks and 3) clandestine nature

Schneier, 15 (Bruce (2015-03-02). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (p. 136-9). W. W. Norton & Company. Kindle Edition.)

The NSA repeatedly uses a connect-the-dots metaphor to justify its surveillance activities. Again and again— after 9/ 11, after the Underwear Bomber, after the Boston Marathon bombings— government is criticized for not connecting the dots. However, this is a terribly misleading metaphor. Connecting the dots in a coloring book is easy, because they’re all numbered and visible. In real life, the dots can only be recognized after the fact. That doesn’t stop us from demanding to know why the authorities couldn’t connect the dots. The warning signs left by the Fort Hood shooter, the Boston Marathon bombers, and the Isla Vista shooter look obvious in hindsight. Nassim Taleb, an expert on risk engineering, calls this tendency the “narrative fallacy.” Humans are natural storytellers, and the world of stories is much more tidy, predictable, and coherent than reality. Millions of people behave strangely enough to attract the FBI’s notice, and almost all of them are harmless. The TSA’s no-fly list has over 20,000 people on it. The Terrorist Identities Datamart Environment, also known as the watch list, has 680,000, 40% of whom have “no recognized terrorist group affiliation.” Data mining is offered as the technique that will enable us to connect those dots. But while corporations are successfully mining our personal data in order to target advertising, detect financial fraud, and perform other tasks, three critical issues make data mining an inappropriate tool for finding terrorists. The first, and most important, issue is error rates. For advertising, data mining can be successful even with a large error rate, but finding terrorists requires a much higher degree of accuracy than data-mining systems can possibly provide. Data mining works best when you’re searching for a well-defined profile, when there are a reasonable number of events per year, and when the cost of false alarms is low. Detecting credit card fraud is one of data mining’s security success stories: all credit card companies mine their transaction databases for spending patterns that indicate a stolen card. There are over a billion active credit cards in circulation in the United States, and nearly 8% of those are fraudulently used each year. Many credit card thefts share a pattern— purchases in locations not normally frequented by the cardholder, and purchases of travel, luxury goods, and easily fenced items— and in many cases data-mining systems can minimize the losses by preventing fraudulent transactions. The only cost of a false alarm is a phone call to the cardholder asking her to verify a couple of her purchases. Similarly, the IRS uses data mining to identify tax evaders, the police use it to predict crime hot spots, and banks use it to predict loan defaults. These applications have had mixed success, based on the data and the application, but they’re all within the scope of what data mining can accomplish. Terrorist plots are different, mostly because whereas fraud is common, terrorist attacks are very rare. This means that even highly accurate terrorism prediction systems will be so flooded with false alarms that they will be useless. The reason lies in the mathematics of detection. All detection systems have errors, and system designers can tune them to minimize either false positives or false negatives. In a terrorist-detection system, a false positive occurs when the system mistakenly identifies something harmless as a threat. A false negative occurs when the system misses an actual attack. Depending on how you “tune” your detection system, you can increase the number of false positives to assure you are less likely to miss an attack, or you can reduce the number of false positives at the expense of missing attacks. Because terrorist attacks are so rare, false positives completely overwhelm the system, no matter how well you tune. And I mean completely: millions of people will be falsely accused for every real terrorist plot the system finds, if it ever finds any. We might be able to deal with all of the innocents being flagged by the system if the cost of false positives were minor. Think about the full-body scanners at airports. Those alert all the time when scanning people. But a TSA officer can easily check for a false alarm with a simple pat-down. This doesn’t work for a more general data-based terrorism-detection system. Each alert requires a lengthy investigation to determine whether it’s real or not. That takes time and money, and prevents intelligence officers from doing other productive work. Or, more pithily, when you’re watching everything, you’re not seeing anything. The US intelligence community also likens finding a terrorist plot to looking for a needle in a haystack. And, as former NSA director General Keith Alexander said, “you need the haystack to find the needle.” That statement perfectly illustrates the problem with mass surveillance and bulk collection. When you’re looking for the needle, the last thing you want to do is pile lots more hay on it. More specifically, there is no scientific rationale for believing that adding irrelevant data about innocent people makes it easier to find a terrorist attack, and lots of evidence that it does not. You might be adding slightly more signal, but you’re also adding much more noise. And despite the NSA’s “collect it all” mentality, its own documents bear this out. The military intelligence community even talks about the problem of “drinking from a fire hose”: having so much irrelevant data that it’s impossible to find the important bits. We saw this problem with the NSA’s eavesdropping program: the false positives overwhelmed the system. In the years after 9/ 11, the NSA passed to the FBI thousands of tips per month; every one of them turned out to be a false alarm. The cost was enormous, and ended up frustrating the FBI agents who were obligated to investigate all the tips. We also saw this with the Suspicious Activity Reports— or SAR— database: tens of thousands of reports, and no actual results. And all the telephone metadata the NSA collected led to just one success: the conviction of a taxi driver who sent $ 8,500 to a Somali group that posed no direct threat to the US— and that was probably trumped up so the NSA would have better talking points in front of Congress. The second problem with using data-mining techniques to try to uncover terrorist plots is that each attack is unique. Who would have guessed that two pressure-cooker bombs would be delivered to the Boston Marathon finish line in backpacks by a Boston college kid and his older brother? Each rare individual who carries out a terrorist attack will have a disproportionate impact on the criteria used to decide who’s a likely terrorist, leading to ineffective detection strategies. The third problem is that the people the NSA is trying to find are wily, and they’re trying to avoid detection. In the world of personalized marketing, the typical surveillance subject isn’t trying to hide his activities. That is not true in a police or national security context. An adversarial relationship makes the problem much harder, and means that most commercial big data analysis tools just don’t work. A commercial tool can simply ignore people trying to hide and assume benign behavior on the part of everyone else. Government data-mining techniques can’t do that, because those are the very people they’re looking for. Adversaries vary in the sophistication of their ability to avoid surveillance. Most criminals and terrorists— and political dissidents, sad to say— are pretty unsavvy and make lots of mistakes. But that’s no justification for data mining; targeted surveillance could potentially identify them just as well. The question is whether mass surveillance performs sufficiently better than targeted surveillance to justify its extremely high costs. Several analyses of all the NSA’s efforts indicate that it does not. The three problems listed above cannot be fixed. Data mining is simply the wrong tool for this job, which means that all the mass surveillance required to feed it cannot be justified. When he was NSA director, General Keith Alexander argued that ubiquitous surveillance would have enabled the NSA to prevent 9/ 11. That seems unlikely. He wasn’t able to prevent the Boston Marathon bombings in 2013, even though one of the bombers was on the terrorist watch list and both had sloppy social media trails— and this was after a dozen post-9/ 11 years of honing techniques. The NSA collected data on the Tsarnaevs before the bombing, but hadn’t realized that it was more important than the data they collected on millions of other people.

### AT: TPP Ptx:

#### The advantage solves your TPP disad—removing localized barriers to a global internet creates pathways for trade, business, logistics, media, and supply chain management

Gresser 14 (Edward, Director of Progressive Economy, “21st Century Trade Policy: The Internet and the Next Generation’s Global Economy,” January 31, http://www.progressive-economy.org/wp-content/uploads/2014/01/21st.Century.Trade\_.pdf)

Ambassador Kirk’s vaguely mysterious phrase – “21st-century trade agreement” – implies two things: That there is something different about trade in the 21st century, and that policy needs to evolve in response. The concept’s meaning, however, has never been entirely clear. Trade itself tends to grow over time, agreements become incrementally more complex – but this has been going on for many years. But Kirk was correct to suggest that there has also been a more abrupt change in trade: the sudden emergence of the Internet as a pathway for trade in services, for small-scale business, logistics and supply-chain management, arts and media, and more.¶ This change does require policy to adapt and to take on some new missions. The TPP agreement is moving toward a likely conclusion this spring, and Congress has begun a discussion of Trade Promotion Authority. As both proceed, the question the uniquely ‘21st-century’ aspects of policy can help answer is about the nature of the global economy of 2030: perhaps one in which the Internet helps create a more affluent, more pluralistic, and more humane global economy; or, alternatively, one in which the digital world fragments, thickens, and ultimately comes to mirror the divisions of the physical world.

# Case Neg

### States CP

#### Text:

The 50 United States should promulgate legislation to ban data collection facilities in their states, refuse to supply water and electricity to NSA facilities, prohibit state officials from using warrantless data in law enforcement investigations, and NSA partnerships with public, state-run Universities or Colleges.

#### Observation I: Net Benefits

We solve the harms of surveillance and compete through net-benefits [explain].

#### Observation II: Solvency:

#### States can curtail surveillance—by ending partnerships with Colleges/Unviersities, refusing to supply electricity and water, and prohibiting state use of warrants, they can eliminate NSA surveillance

OFFNOW 15 (“THE PLAN,” http://www.offnow.org/plan)

THE PLAN¶ It's easy to feel helpless when facing a government that has the power or claims the authority to spy on virtually everybody in the world with impunity.¶ BUT IT CAN BE STOPPED.¶ In 1975, Sen. Frank Church warned America about the federal spy program, saying that if a dictator took over the NSA it “could enable [him] to impose total tyranny."¶ And that was before the advent of the Internet.¶ Here we are almost 40 years later and Congress hasn’t done a thing about it. In fact, things are actually far worse. Politicians in D.C. have repeatedly failed to fix the issue, even in the wake of leaked documents and damning revelations.¶ In The Art of War, Sun Tzu advised this strategy: “Attack him where he is unprepared, appear where you are not expected.”¶ The NSA expects its opponents to “attack” from the same front they always have: Washington D.C. It’s ready for that.¶ But it does have an Achilles Heel.¶ MAXED OUT¶ In 2006, the Baltimore Sun reported that the NSA had maxed out capacity of the Baltimore-area power grid.¶ “The NSA is already unable to install some costly and sophisticated new equipment. At minimum, the problem could produce disruptions leading to outages and power surges. At worst, it could force a virtual shutdown of the agency.”¶ FACT: The spy agency needs resources like water and electricity. It simply cannot operate its facilities without these essential resources.¶ State and local governments often supply them. For instance, the NSA storage facility in Bluffdale, Utah, will reportedly use up to 1.7 million gallons of water every single day when fully operational. The city holds the contract to supply that water.¶ It doesn't have to.¶ Nothing requires state or local governments to help the federal government violate your rights!¶ Under the legal principle known as the anti-commandeering doctrine, the Supreme Court has consistently held that the federal government cannot force states to help implement or enforce federal acts or programs. It rests primarily on four Supreme Court cases: Prigg v. Pennsylvania (1842), New York v. US (1992), Printz v. US (1997) and National Federation of Businesses v. Sebelius (2012).¶ Printz serves the cornerstone.¶ “The Federal Government may neither issue directives requiring the States to address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program…such commands are fundamentally incompatible with our constitutional system of dual sovereignty.”¶ 1. RESOURCES¶ Instead of relying on the federal government to reform its own spy program, the OffNow plan involves working at the state level to create an environment that makes it politically and logistically impossible for the NSA and other federal agencies to continue illegal surveillance programs.¶ The strategy centers around state and local legislation designed to deprive the NSA and other agencies engaged in warrantless spying of the resources and cooperation they need to operate and accomplish their goals.¶ The short version? We intend to pull the rug out from under them, box them in and shut them down.¶ This model legislation (HERE), ready for introduction in any state, would ban a state (and all its political subdivisions) from providing assistance or material support in any way to federal spying programs.¶ This would include, but is not limited to:¶ Refusing to supply water or electricity from state or locally-owned or operated utilities.¶ Ending NSA partnerships with public universities and colleges.¶ Prohibiting state officials from using warrantless data given to them by federal agencies¶ ¶ Within the scope of current jurisprudence, state law cannot prevent the federal government from bringing in its own supplies. But, the 2006 power grid issue indicates that in many situations, the federal government simply cannot do this on its own.¶ As a legal matter, contracts for water, electricity and other resources and services are simply voluntary agreements made between the federal government (or its agents) and the state or local government. States legitimately can and should decide whether to honor the request based on the state’s own set of priorities. ¶ The states and local communities should simply turn it off.¶ In fact, Nevada took this path against the powerful Department of Energy, and won.

### Extend: States CP Solvency

#### States can solve—6 ways

OFFNOW 15 (“THE PLAN,” http://www.offnow.org/plan)

STRATEGY¶ Former NSA technical leader and whistleblower William Binney says, "There have been at least 15-20 trillion constitutional violations" by the NSA.¶ We must engage a multi-prong strategy to deal with a surveillance establishment so well-entrenched and broad in scope.¶ Currently, many activists are engaged in the support of lawsuits or Congressional legislation to limit or stop the NSA. But waiting for these to play out positively could prove a dangerous game of chicken.¶ By approaching the surveillance state on multiple fronts, it is possible to overwhelm it and make its programs too difficult or costly to carry out. A program to Turn it Off and thwart the surveillance state through state legislation intersects in six main areas:¶ 1. Denying federal agencies engaged in warrantless surveillance the resources they need to operate.¶ 2. Prohibiting the introduction of warrantless information collected by the feds and shared with state and local law enforcement in state criminal proceedings.¶ 3. Ending warrantless location tracking of cellphones, and physical surveillance by drones.¶ 4. Ending cooperative partnerships between universities and the NSA.¶ 5. Penalizing corporations that cooperate with mass, warrantless surveillance.¶ 6. Addressing state and local actions that feed into the larger surveillance-state, such as fusion centers, suspicious activity reporting, surveillance cameras and license plate readers.¶ SAY "NO!"¶ Rosa Parks demonstrated the power of "No!"¶ When she refused to give up her seat on that Montgomery city bus, she ignited a fire that ultimately consumed Jim Crow.¶ We possess that same power today. State and local governments can say, "No!" to warrantless spying and simply refuse to cooperate with it.¶ This one word gives us the power to reject mass surveillance and restore privacy. But it can only happen if we muster up the necessary courage to act.¶ “The only tired I was…was tired of giving in," Parks later said.¶ Are you tired? Are you tired of sitting back and feeling helpless as the federal government violates your privacy? Are you tired of excuses and justifications from Washington politicians? Are you tired of being ignored?¶ Then take action!¶ Say, "No!"¶ Join us as we work to take apart the surveillance state!

#### Texas Bill Would Turn Off Power to Massive NSA Surveillance Facility

Mike Maharrey 2015 (mike maharrey http://blog.tenthamendmentcenter.com/2015/03/texas-bill-would-turn-off-power-to-massive-nsa-surveillance-facility/ march 26 2015)

Texas legislator introduced a bill that would stop the independent Texas power grid from being used to power mass, warrantless surveillance by the NSA. Rep. Jonathan Stickland (R) introduced House Bill 3916 (HB3916) on March 13. The legislation would prohibit any political subdivision in Texas from providing water or electricity to any federal agency “involved in the routine surveillance or collection and storage of bulk telephone or e-mail records or related metadata concerning any citizen of the United States and that claims the legal authority to collect and store the bulk telephone or e-mail records or metadata concerning any citizen of the United States without the citizen’s consent or a search warrant that describes the person, place, or thing to be searched or seized.” “No water and no electricity means no super-computers. That will shut down NSA operations in Texas. If Congress doesn’t want to reform the NSA then we’ll just turn it off,” OffNow founder and associate director Michael Boldin said.

### CP Solvency: Congress doesn’t enforce

#### Congress chooses not to act on surveillance oversight—history is on our side

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

What is different, at least with regard to FISA (albeit consistent with other areas of national security law), is the clandestine nature of the reporting and the restrictions placed on committee and non-committee members who may have access to the information. Members may not know of the existence of, or details about, programs that would enable them to ask pertinent questions or to delve further into how authorities are being exercised. The result is that Congress may agree to laws without fully understanding the implications of their actions.¶ One could argue that this happens all the time. It is part of the good faith exercise that is part and parcel of the legislative process. Legislators accord their colleagues, who develop an expertise in certain areas, a degree of deference. But one distinction, in regard to national security, is that the stakes are particularly high. It is precisely this concern that arose during enactment of the FAA in 2008. Congress was being asked to pass legislation that gave telecommunication companies indemnity, but only a minority of the members of both chambers had been briefed on the President's Surveillance Program. The question, according to Senator Specter, was whether the limited briefing amounted to an unconstitutional [\*182] delegation of authority. n246 For Senator Whitehouse, the issue was less one of constitutionality and more one of simple legislative prudence: whether the Senate ought to substitute its good faith in the few for a determination that ought to be made by the judiciary. n247 What was at stake was the rule of law.¶ In the case of Section 702, the intelligence community did not just keep the committees informed, but prior to the renewal debates, it made its classified briefings widely available to all Members of Congress. n248 The May 2012 report, for instance, available to [\*183] Members of Congress more than a year before the Snowden revelations, detailed PRISM and upstream collection. n249¶ As to the second claim, could Congress have stopped the program if it so wished? The answer to this question is more difficult. Congress ostensibly had both private and public mechanisms it could employ to subject the program to more scrutiny and to change aspects considered repugnant as either a statutory or Constitutional matter. It could have conditioned continuation of the authorities, for instance, on curbing TFA collection, or shifting the assumptions regarding identity or location. Alternatively, it could have suspended funding for the program. It did none of these things. The House did not hold any hearings on how the law was operating prior to voting on whether to renew the FAA. n250 Publicly, Congress could have declassified materials, opened the NSA's programs to broader discussion, and subjected the executive to citizens' scrutiny. It chose not to do so.

### Courts CP

#### Congress consistently fails to provide oversight on surveillance issues—TFAs prove

Donohue 15 (Laura, Prof of Law at Georgetown U Law Center, “Security vs. Freedom: Contemporary Controversies: The Thirty-Third Annual Federalist Society National Student Symposium on Law and Public Policy 2014: Article: Section 702 and the Collection of International Telephone and Internet Content,” 38 Harv. J.L. & Pub. Pol'y 117, Winter 2015, L/N)

[\*159] Even if Congress did not initially appreciate the potential for programmatic collection, however, certainly by 2012 the intelligence community had made enough information available to Congress for Members to make an informed decision. This does not mean that all Members were fully informed. But to the extent that Members selected not to access the material or to take a public stand on the matter, particularly in light of the legislature's reading of its authorities with regard to classification, fault lies with Congress.¶ The Foreign Intelligence Surveillance Court failed to step into the gap. In 2011, FISC realized the implications of the NSA's interpretation of to, from or about (TFA) collection. However, in light of the seriousness of the NSA's aim (protecting national security), and the limitations imposed by the types of technologies being used, the Court read the statute in a manner that found the targeting procedures to be consistent with the statute.¶ To the extent that NSA's TFA and assumptions regarding the target's foreignness undermine the law as it is written, the legislature failed to perform effective oversight. Congress similarly neglected to uphold the limit placed on the intelligence community to not knowingly collect domestic conversations. Instead, it relied on FISC to do so--a task that the Court failed to do. In a classified environment, when so much information is cloaked from public view, it becomes even more important for the government to ensure that the authorities as they are publicly presented are consistent with the manner in which they are being exercised.

### AT: Cyber Terror

#### Neg Most cyber terrorism is low-level noise not meaningful intelligence collection

Associated Press 15 (“Cyber-attacks rising in Utah, likely due to NSA facility,” *Associated Press*, February 6, http://ksn.com/2015/02/06/cyber-attacks-rising-in-utah-likely-due-to-nsa-facility/)

Tim Junio, a cybersecurity researcher at Stanford University, said what officials refer to as “attacks” are likely just “noise from low-tech people rather than concerted efforts for meaningful foreign intelligence collection.”

### Digital Innocence Turn

#### Not all big data is bad—NSA databases can provide exculpatory evidence that proves “digital innocence”

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

Such stories are not part of the dueling narratives in America's current debate over pervasive government surveillance, which, depending on one's perspective, either leads to a dystopian panoptic society or prevents another 9/11. The choice is pitched as whether the information should be gathered, and, if so, when, where, and how much. A different question needs to be asked: Who will have access to the data? For the most part today, only the government and corporate entities gather and tap the stores of information about the populace. This creates a dangerous imbalance where only the most powerful public and private actors may draw upon data about the general population. Some experts have argued for the tables to be turned by increasing the capacity of individuals to find out information about [\*986] their surveillance. n26 If the powerful are going to spy on us and collect data about our lives, shouldn't we know what information is being gathered and have access to the resulting databases?¶ This argument takes on a constitutional dimension when the information is wielded by law enforcement to accuse, convict, and punish. Modern surveillance technology can provide both inculpating and exculpating evidence. Electronic eavesdropping can catch the guilty red-handed, but it can also provide alibis for the wrongfully accused and convicted. With citizens' lives increasingly logged and tracked, online and off, the chance of finding evidence tending to prove innocence only increases. The breadth and depth of corporate and government surveillance seem to guarantee the existence of exonerating evidence, stored somewhere, proving the innocence of suspects and defendants. Assuming computer engineers can refine the tools necessary to find it, proof of innocence will be uncovered in some yet-to-be-determined number of cases. This Article calls for the development of a new concept - digital innocence - seeking to leverage the tools and content of Big Data to prevent wrongful convictions and provide hard proof of actual innocence for those already convicted.

#### Surveillance data can exonerate the innocent

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

In 2005, San Francisco introduced cameras at hotspots throughout the city as a way of bringing down the overall crime rate. But the cameras were soon put to a different purpose. "More than just a crime-fighting tool," the cameras "have also become a tool exploited by defense lawyers who often seek footage from the cameras to exonerate falsely accused clients." n29 In one case, a man was cleared of a murder charge when footage showed him defending a disabled woman. n30 Public defenders are now trained to ask for the data, with a third of all requests for footage coming from defense attorneys. n31¶ A similar phenomenon is unfolding around law enforcement recording, typically done by citizens filming police in action. n32 Mobile recording devices have become a check on abuse of power and, as was the case for some Occupy Wall Street protestors, a means of proving [\*988] one's innocence. n33 Elsewhere, dashboard-mounted video cameras have become indispensable for motorists who rely upon the captured images as a means to protect themselves against erroneous or crooked traffic enforcement. n34 At times, however, the government's own recordings have helped free the innocent. In a recent case, a New Jersey man charged with resisting arrest and assault was cleared after the defense requested and received a police dash-cam video, which both exonerated him and exposed wrongdoing by several officers. n35 "If we hadn't had the tapes in this case," defense counsel said, "an innocent man would be in jail today." n36¶ These examples are merely the faintest ripple of a coming tide of digital evidence. An important report by the National Academy of Sciences (NAS) described the development of "an emerging forensic science discipline":¶ ¶ The proliferation of computers and related devices over the past 30 years has led to significant changes in and the expansion of the types of criminal activities that generate digital evidence. Initially, computers were either the weapon or the object of the crime... . As computers became more popular, they became storage containers for evidence... . Finally, digital media have become witnesses to daily activities... . As a result, almost every crime could have digital evidence associated with it. n37¶ ¶ Clearly, digital evidence can incriminate the guilty. But the NAS report - which documented the possibilities and perils of other forensic disciplines for the factually innocent n38 - failed to discuss the potential of digital evidence to exonerate the wrongfully accused and convicted.

#### The history of DNA technology proves—tech advances in surveillance can blaze a trail for digital innocence.

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

This shortcoming in the literature is understandable. To broach the topic of digital innocence in the age of Big Data, rights-minded scholars would have to confront yet another temptation in a Faustian bargain that already trades privacy and liberty for knowledge, convenience, and security. n43 Alternatively, scholars might have to assume arguendo that mass surveillance will continue despite powerful objections. As seen in our introductory caveat, we are deeply troubled by the massive and relentless tracking of people's interactions, particularly when done by the government. But we are also concerned that [\*990] the current debate has failed to take into consideration an important cost of mass surveillance: the non-derogable obligation to provide access to potentially exonerating information. By exploring the concept of digital innocence, this Article seeks to make clear that government and corporate entities will have to pay a price if they intend to (and are allowed to) monitor the entirety of people's lives.¶ The second scholarly category offers an analogous enterprise to the one we have undertaken here: the literature on the DNA revolution in wrongful convictions. n44 This scholarship is not concerned with the concept we have described as digital innocence and only hints at the possibility, n45 but it still serves as a good example of how technological advance can change the legal debate surrounding innocence, suggesting how our concept might fit into the overall scheme of the law. In fact, the path of DNA technology through legal institutions may serve as a trail for digital innocence. n46 Proof-of-innocence technologies exert a unique influence on the criminal justice system. Although prosecutors do not always respond well to wrongful conviction claims - especially those premised on human error, such as false confessions and mistaken witness identifications - hard scientific proof of innocence is more likely to move the government to drop charges or acquiesce to the release of an inmate. n47 The DNA technology literature therefore sets the stage for a discussion about the broader role of technology in establishing innocence.¶ The literature also provides insights on the application and pace of technological advance. n48 Evidence in criminal cases changes with technology, n49 as developments help finger the guilty but also have the power to exonerate the wrongfully accused or convicted. Typically, however, new technology is first used to convict and only years later, if ever, used to acquit. n50 Moreover, lags in the exoneration of defendants [\*991] are often characterized by issues of storage, followed by improvements in the testing technology. n51 Along these lines, DNA analysis initially was the province of prosecutors but over time became essential to claims of actual innocence. n52 If a wrongfully convicted defendant was lucky, biological evidence of the real perpetrator was properly stored, sometimes for years, until the capacity and technology were developed to test the evidence. n53

#### The jury is still out—no proof data will be used for digital innocence and, in the squo, ev is used overwhelmingly to convict.

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

As suggested by the language quoted from the NAS report, data science and Big Data technologies have been overwhelmingly used to convict. n54 Prosecutors often gather cookie data, n55 search terms, n56 web-surfing history, n57 and cell-site location information as part of their case against the accused. n58 But in the future, this data need not accrue exclusively to the benefit of prosecutors. n59 As search algorithms get better and private citizens obtain access to data-mining tools and technologies, defense counsel might have a significantly greater ability to prove actual innocence by finding some specific video from a local camera, for instance, or by cross-referencing geolocation information from a cellphone, thereby showing that the defendant was not at a given place at a given time. n60 The question is whether the massive amounts of data gathered about every American citizen will result in a similar or even greater potential to exonerate the innocent.

#### DNA Proves—tech can be used for exhoneration

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

Certainly, the DNA revolution has placed a spotlight on the entire criminal justice system. Generations of defense lawyers struggled to free inmates who they believed to be innocent, but the available [\*993] means to upend convictions were limited to recantations by witnesses and confessions by the actual perpetrators. Even in the rare cases where such evidence surfaced, defense claims were often procedurally barred. n75¶ ¶ In what seems like a flash, DNA tests performed during the last decade of the [twentieth] century not only have freed sixty-four individuals but have exposed a system of law that has been far too complacent about its fairness and accuracy... .¶ Now the fabric of false guilt is laid bare, and the same vivid threads bind ... . Sometimes eyewitnesses make mistakes. Snitches tell lies. Confessions are coerced or fabricated. Racism trumps the truth. Lab tests are rigged. Defense lawyers sleep. Prosecutors lie. n76

#### Big data could have a greater backward-reaching impact on exonerating the innocent than DNA

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

The single discipline of DNA technology cannot serve as the comprehensive source of information needed to meaningfully reduce the incidence of wrongful convictions. The coming wave of Big Data information technologies has the potential to provide hard proof of actual innocence in many of the non-DNA cases. In fact, data-mining [\*994] technology could have an even greater backward-reaching impact on the criminal justice system. Mindboggling amounts of data are being gathered and stored, although defendants currently lack the capacity to access the contents or to isolate factors that might demonstrate their innocence. n81 The discrepancy between the present collection of large amounts of data, and the now budding industry of analyzing and drawing connections from and between that data, means that there are now people in prison who will be exonerated when the data-mining tools become good enough to locate and aggregate proof of their innocence.

#### The innocence movement proves—big data will be used to exonerate the innocent

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

The DNA revolution and concomitant actual innocence movement provide glimpses of the future for digital innocence. Among other things, dozens of innocence projects have opened around the country; national conferences are held on wrongful conviction every year; professional training on the sources and prevention of wrongful convictions is widely available to defense attorneys and other criminal justice actors; and every state has enacted post-conviction DNA testing statutes often accompanied by provisions for the preservation of biological evidence. One could imagine similar efforts focused on Big Data technologies, such as the creation of a "Digital Innocence Project," which could provide legal representation in cases of actual innocence; curate online communities and develop open source resources; educate defense lawyers, prosecutors, and judges; and positively shape the law by, for instance, seeking the expansion of DNA-specific statutes to include evidence gleaned from data science.

#### Turn: the Utah Data Center provides evidence that could exonerate the innocent—digital innocence is only possible with large-scale storage facilities.

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

The most significant characteristic of databases relevant to digital innocence is the rate of storage increase. n92 Growth in storage capacity means the data that might exonerate a defendant is stored but not necessarily parsed. n93 That data might reside in a telecommunication provider's cell-site location information, or in the photographs of a user-generated content website, or in e-mail, or text messages. n94 The odds of storing a piece of exonerating evidence must grow at least linearly as a function of the increase in storage capacity (i.e., storing more of what is already being stored) and as a function of the increase in types of information stored (i.e., storing additional kinds of information). [\*997] Actually, there is reason to believe that the ability to prove innocence digitally will increase more than linearly. Bigger databases allow algorithms to make more connections, n95 and more connections yield the ability to monetize more data, which in turn creates even bigger databases. n96¶ Storage has now reached the point where the product of ubiquitous surveillance can be stored on a semi-permanent basis, as datacenters have gotten bigger and better at a seemingly ever-increasing rate. n97 The PRISM program and like government surveillance require massive data storage. "Full-take" systems, such as the United Kingdom's TEMPORA program, also require enormous storage because they ingest everything passing through a given conduit. Moreover, Congress is once again considering the Cyber Intelligence Sharing and Protection Act (CISPA), which would permit sharing of intelligence information with corporations, and vice versa, supposedly to combat cyber-threats. n98 This form of deep data mining can only function, however, if sufficient storage is available to save the data pending use.¶ Unsurprisingly, there are reports of large datacenters constructed with precisely this sort of data mining in mind. Termed the largest in the country, the NSA's mammoth facility in Bluffdale, Utah, is intended to store and parse data captured from worldwide electronic communications. n99 When completed, the Bluffdale Center will be five times the size of the U.S. Capitol. n100 According to reports, the project was ready for operation in September 2013. The information to be parsed includes "complete contents of private e-mails, cellphone calls, and Google searches, as well as all sorts of personal data trails - parking receipts, travel itineraries, bookstore purchases" - and much more. n101

#### Big data could provide exculpatory evidence

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

By enhancing pre-digital media, it is also possible to data mine the past. n146 Although analog recordings of video and sound have supported convictions for years, the tapes are often blurry or the sounds unclear and therefore subject to challenge. The situation has changed with the marriage of digital technology with sophisticated search algorithms. n147 This technology may help reveal more information from background noise on analog-taped telephone calls or other recordings than was ascertainable at the time of trial. Likewise, state-of-the-art graphics programs can resolve blurred features on pre-digital tapes, which then might show that the wrong person was convicted. n148¶ These new types of information could play an ever-larger part in defense and post-conviction exoneration efforts. n149 Obtaining access to data will be an impediment in such efforts, n150 although presumably the hurdle will be at its lowest for broadly shared social media. n151 Information from social media is often publicly posted, publicly stored, and even publicly searchable for a limited time. It may not be permanently stored outside of the virtual wall of the social network itself, however, and semi-closed ecosystems like Facebook can be hard to research. But tweets and blogs are often stored by wayback machines [\*1005] or Internet archives, n152 and in some cases, Google itself keeps a record of an archived page. n153 This quasi-public data could be an important source of exculpatory evidence as access and search tools grow in strength.

#### Connected databases can prove digital innocence

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

At first, digital innocence may be proved by single "smoking gun" pieces of evidence culled from now-colossal datasets. But just as guilt is often established by piecing together different pieces of data into a convincing pattern, innocence might be demonstrated in a similar fashion by linked data and pattern analysis. The more linked data the system can access, the more patterns that may emerge, even from unlikely concatenations of data points. This methodology is most advanced in advertising. As mentioned, advertisers have access to large commercial databases, providing information they sell to one another in a semi-closed ecosystem. Access to this ecosystem is either through deals for entire databases or by access to databases that draw on these stores. The databases are increasingly linked, permitting an advertiser to target potential customers based not just on their physical proximity to the seller's location, their web-surfing pattern, their credit card purchasing history, or their recent life events (e.g., births, funerals, and vacations), but rather on a combination of all this information. n154¶ Connected databases yield insights that individual databases do not. Knowing where someone is in real space may augment information about his browsing history, while knowing a user's social network can supplement information about his purchasing history. n155 Advertisers routinely target those consumers who are thought leaders, whose purchasing decisions affect others in their social network, by cross-referencing knowledge of purchasing history with social network information. This permits advertisers to optimize advertising efforts by focusing customer services and perks on influential members of a network. n156 The same type of cross-linking is a common feature of law enforcement's use of data. Police start by examining text messages, cellphone connections, and social networks. The connection of communication [\*1006] history (i.e., text, voice, and Internet) with geolocation data and social network mapping can be a heady technique. n157

### AT: 4th Amendment

#### Empirically, there’s no expectation of privacy on the internet—means it won’t trigger 4th amendment violations

Fairfield and Luna 14 (Joshua-Prof of Law, Washington and Lee; Erik, Sydney Lewis Prof of Law, Washington and Lee, “Digital Innocence,” 99 Cornell L. Rev. 981, L/N)

The government's authority to conduct digital surveillance and draw upon the fruits of Big Data traces back to relatively low-tech eavesdropping and wiretapping. For decades, these practices were legally uncontroversial based on the theory that listening devices without an accompanying physical trespass did not violate the Fourth Amendment. n164 Even when the Supreme Court held that federal legislation precluded the introduction at trial of conversations overheard on wiretaps by law enforcement, n165 the Justice Department took the position that it was still permissible to conduct warrantless electronic surveillance to gather intelligence for national security purposes. n166¶ In 1967, the Court's decision in Katz v. United States n167 rejected the prevailing doctrine that had allowed warrantless wiretapping but now "ignores the vital role that the public telephone has come to play in private communication." n168 In the ensuing decades, the Katz [\*1008] test for when state action implicates the Fourth Amendment would be interpreted as requiring an expectation of privacy that "society is prepared to recognize as 'reasonable.'" n169 Somewhat ironically, the case that safeguarded conversations by telephone, one of the seminal breakthroughs in modern communications, did not provide much protection against subsequent advances of technology. More often than not, the Supreme Court has held that a given investigative technique does not violate a reasonable expectation of privacy and therefore does not trigger the Fourth Amendment at all. n170¶ Two features of this jurisprudence are especially important for electronic surveillance: (1) data about data (i.e., metadata) may be considered deficient of any content that might engender a privacy expectation, n171 and (2) data may lose the protection afforded by a reasonable expectation of privacy once the information is provided to third parties. n172 Thus, the government may eavesdrop on otherwise private conversations in residences transmitted by wired informants, n173 obtain records detailing an individual's otherwise private financial information, n174 and install pen registers on home phone numbers to determine whom someone is calling. n175 In the latter [\*1009] instance, the Supreme Court's decision in Smith v. Maryland held that, by conveying numerical information to a phone company, an individual "assumed the risk" this information would be provided to government agents. n176 Given that Big Data is the aggregation of data about data, and that all data online is handed off to ISPs in some form or another, the foregoing principles have been (over)extended to place the entire Internet outside of meaningful constitutional protections, thereby allowing massive, suspicionless, and even prospective data gathering by government.