# CIRCUMVENTION

# Negative

## Yes Circumvention

### 1NC – plan circumvented

#### Reforms are not possible—the plan will be circumvented

Greenwald 2014 (Glenn [Constitutional lawyer- patriot]; CONGRESS IS IRRELEVANT ON MASS SURVEILLANCE. HERE’S WHAT MATTERS INSTEAD; Nov 19; https://firstlook.org/theintercept/2014/11/19/irrelevance-u-s-congress-stopping-nsas-mass-surveillance/; kdf)

All of that illustrates what is, to me, the most important point from all of this: the last place one should look to impose limits on the powers of the U.S. government is . . . the U.S. government. Governments don’t walk around trying to figure out how to limit their own power, and that’s particularly true of empires. The entire system in D.C. is designed at its core to prevent real reform. This Congress is not going to enact anything resembling fundamental limits on the NSA’s powers of mass surveillance. Even if it somehow did, this White House would never sign it. Even if all that miraculously happened, the fact that the U.S. intelligence community and National Security State operates with no limits and no oversight means they’d easily co-opt the entire reform process. That’s what happened after the eavesdropping scandals of the mid-1970s led to the establishment of congressional intelligence committees and a special FISA “oversight” court—the committees were instantly captured by putting in charge supreme servants of the intelligence community like Senators Dianne Feinstein and Chambliss, and Congressmen Mike Rogers and “Dutch” Ruppersberger, while the court quickly became a rubber stamp with subservient judges who operate in total secrecy. Ever since the Snowden reporting began and public opinion (in both the U.S. and globally) began radically changing, the White House’s strategy has been obvious. It’s vintage Obama: Enact something that is called “reform”—so that he can give a pretty speech telling the world that he heard and responded to their concerns—but that in actuality changes almost nothing, thus strengthening the very system he can pretend he “changed.” That’s the same tactic as Silicon Valley, which also supported this bill: Be able to point to something called “reform” so they can trick hundreds of millions of current and future users around the world into believing that their communications are now safe if they use Facebook, Google, Skype and the rest. In pretty much every interview I’ve done over the last year, I’ve been asked why there haven’t been significant changes from all the disclosures. I vehemently disagree with the premise of the question, which equates “U.S. legislative changes” with “meaningful changes.” But it has been clear from the start that U.S. legislation is not going to impose meaningful limitations on the NSA’s powers of mass surveillance, at least not fundamentally. Those limitations are going to come from—are now coming from —very different places: 1) Individuals refusing to use internet services that compromise their privacy. The FBI and other U.S. government agencies, as well as the U.K. Government, are apoplectic over new products from Google and Apple that are embedded with strong encryption, precisely because they know that such protections, while far from perfect, are serious impediments to their power of mass surveillance. To make this observation does not mean, as some deeply confused people try to suggest, that one believes that Silicon Valley companies care in the slightest about people’s privacy rights and civil liberties.

### Yes circumvention – Generic

#### Reform attempts just provide a veneer of legitimacy for national security officials

Glennon, 14 --- Professor of International Law at Tufts (Michael, Harvard National Security Journal, “National Security and Double Government,” [http://harvardnsj.org/wp-content/uploads/2014/01/Glennon-Final.pdf, JMP)](http://harvardnsj.org/wp-content/uploads/2014/01/Glennon-Final.pdf%2C%20JMP%29)

VI. Conclusion

U.S. national security policy has scarcely changed from the Bush to the Obama Administration. The theory of Walter Bagehot explains why. Bagehot described the emergence in 19th-century Britain of a “disguised republic” consisting of officials who actually exercised governmental power but remained unnoticed by the public, which continued to believe that visible, formal institutions exercised legal authority.601 Dual institutions of governance, one public and the other concealed, were referred to by Bagehot as “double government.”602 A similar process of bifurcated institutional evolution has occurred in the United States, but in reverse: a network has emerged within the federal government that exercises predominant power with respect to national security matters. It has evolved in response to structural incentives rather than invidious intent, and it consists of the several hundred executive officials who manage the military, intelligence, diplomatic, and law enforcement agencies responsible for protecting the nation’s security. These officials are as little disposed to stake out new policies as they are to abandon old ones. They define security more in military and intelligence terms rather than in political or diplomatic ones. Enough examples exist to persuade the public that the network is subject to judicial, legislative, and executive constraints. This appearance is important to its operation, for the network derives legitimacy from the ostensible authority of the public, constitutional branches of the government. The appearance of accountability is, however, largely an illusion fostered by those institutions’ pedigree, ritual, intelligibility, mystery, and superficial harmony with the network’s ambitions. The courts, Congress, and even the presidency in reality impose little constraint. Judicial review is negligible; congressional oversight dysfunctional; and presidential control nominal. Past efforts to revive these institutions have thus fallen flat. Future reform efforts are no more likely to succeed, relying as they must upon those same institutions to restore power to themselves by exercising the very power that they lack. External constraints—public opinion and the press—are insufficient to check it. Both are manipulable, and their vitality depends heavily upon the vigor of constitutionally established institutions, which would not have withered had those external constraints had real force. Nor is it likely that any such constraints can be restored through governmental efforts to inculcate greater civic virtue, which would ultimately concentrate power even further. Institutional restoration can come only from an energized body politic. The prevailing incentive structure, however, encourages the public to become less, not more, informed and engaged.

### Yes circumvention – Courts

#### Intelligence agencies will find loopholes in the plan

Rosenthal 6/12/2015 (Max J, Government's secret surveillance court may be about to get a little less secret; www.motherjones.com/politics/2015/06/usa-freedom-act-fisa-court-transparency; kdf)

"I think the transparency provisions are going to be effective for the judges who are inclined to support them and are going to be ineffective for the judges who aren't," says Steve Vladeck, a professor at American University's Washington College of Law. There are other procedural moves the government could use to limit what information is made public. The court could simply issue summaries of decisions that don't include their key parts, or the executive branch could heavily redact them. "In theory, the executive branch could comply with this part of the statute by redacting 99 percent—everything but one sentence, essentially—of an opinion," Goitein says. She admits that specific tactic is unlikely—it would be an obvious and public skirting of the law's intent—but stresses that even though the law makes important progress in disclosure, there are still many loopholes that could cut down on how much the public will get to see. "I think the history strongly suggests that the intelligence establishment will take every single little bit of rope it has," she says. "And then some."

#### Court’s will fail

Greenwald 2014 (Glenn [Constitutional lawyer- patriot]; CONGRESS IS IRRELEVANT ON MASS SURVEILLANCE. HERE’S WHAT MATTERS INSTEAD; Nov 19; https://firstlook.org/theintercept/2014/11/19/irrelevance-u-s-congress-stopping-nsas-mass-surveillance/; kdf)

3) U.S. court proceedings. A U.S. federal judge already ruled that the NSA’s domestic bulk collection program likely violates the 4th Amendment, and in doing so, obliterated many of the government’s underlying justifications. Multiple cases are now on appeal, almost certainly headed to the Supreme Court. None of this was possible in the absence of Snowden disclosures. For a variety of reasons, when it comes to placing real limits on the NSA, I place almost as little faith in the judiciary as I do in the Congress and executive branch. To begin with, the Supreme Court is dominated by five right-wing justices on whom the Obama Justice Department has repeatedly relied to endorse their most extreme civil-liberties-destroying theories. For another, of all the U.S. institutions that have completely abdicated their role in the post-9/11 era, the federal judiciary has probably been the worst, the most consistently subservient to the National Security State.

### Yes Circumvention – Drones

#### The plan will get circumvented, they’ll find other aircraft

Stanley 2015 (Jay [Senior policy analyst, ACLU speech, privacy & tech project]; What's spooky about the FBI's fleey of spy planes?; https://www.aclu.org/blog/free-future/whats-spooky-about-fbis-fleet-spy-planes; kdf)

Following up on a May story by the Washington Post about mysterious aircraft spotted circling over Baltimore, the Associated Press reported today that the FBI maintains a secret air force with scores of small aircraft registered with 13 front companies under apparently false names, and that these planes fly over American cities frequently. Obviously law enforcement has been using aircraft for many decades. So what’s spooky about this story? Several things: These are not your grandparents’ surveillance aircraft. As I discussed when the Baltimore story broke, there are several very powerful mass-surveillance technologies that utilize low-circling manned aircraft, including “Dirtboxes” and persistent wide-area surveillance in which an entire 25-square mile area can be monitored, and vehicles tracked, for extended periods of time by a single camera. We need more information about the scope of surveillance these planes are being used for. The FBI told the AP that its fleet was “not equipped, designed or used for bulk collection activities or mass surveillance.” We are glad to hear that—but that statement bears more interrogation. For example the AP reports that the FBI “occasionally” uses Dirtboxes (aka “IMSI catchers” or “cell-site simulators”) on the aircraft. Those certainly qualify as mass surveillance devices. If the FBI is only using the aircraft when it has a specific target rather than for broad fishing expeditions, that would be a good thing—but that is not the same thing as saying that data on masses of people is not being swept up. The FBI told the AP that “under a new policy it has recently begun obtaining court orders to use cell-site simulators.” But we don’t know what kind of “court orders” they’re getting to use the devices. Rather than warrants, they may just be obtaining “pen register” orders, as we have seen done by local police in Baltimore and elsewhere. The sheer scope of the program. A 2010 federal budget document found by the AP mentions at least 115 planes in the FBI’s fleet, and the FBI has flown over 100 flights over more than 30 American cities in recent weeks, the AP found. Surveillance turning inward. One trend we’ve seen in the last 15 years or so is a great “Turning Inward,” as US surveillance capabilities originally built to spy on the Soviet Union and other overseas targets have swung inward on the American people. The FBI has a spy plane fleet, hidden behind shell companies with three-letter names and headed by ghost CEOS with signatures that don’t match over time— it’s all very CIA. Yet these are American cities that they’re flying over. Cessnas today, drones tomorrow. Another thing that makes these flights spooky is the prospect that manned aircraft may soon be replaced with drones. And that will make it all the cheaper and easier to deploy these flights all the more frequently over even more American cities and towns. And unlike manned aircraft, drones may not be easy to track through web sites like flightradar24.com, which shows the manned aircraft currently in the air around the world and played a key role in uncovering the FBI’s air force. It is true that under orders from President Obama the DOJ recently promulgated a privacy policy for its use of drones, but that policy is not very airtight—for example, it says DOJ agencies can’t use the planes “solely for the purpose of monitoring activities protected by the First Amendment.” That is good, but when agencies want to do surveillance they always claim to have other reasons so the monitoring is not “solely” for such monitoring. In the end, it doesn’t make sense for drones to be subject to privacy regulations, but not manned aircraft. Manned aircraft can and do raise very real privacy concerns; for example their use in persistent wide-area surveillance, and in voyeurism incidents. But manned aircraft are not regulated today, because historically they have been expensive and their use therefore relatively rare, and their surveillance abilities well-understood and relatively limited. What this story tells us is that their use is now more widespread than we thought—and we know their surveillance capabilities are growing by leaps and bounds. Drones, by raising the prospect of endless free and easy aerial surveillance, have brought to the fore issues that already existed with manned aircraft, and new regulations designed to protect against aerial surveillance should not distinguish between manned and unmanned aircraft. Law enforcement has been using aircraft for many decades. So what’s spooky about reports of FBI fleet of low-circling planes?

### Yes Circumvention – Executive

#### Executive will just ignore Congress and FISA typically defers to it

Bendix & Quirk, 15 --- \*assistant professor of political science at Keene State College, AND \*\*Phil Lind Chair in U.S. Politics and Representation at the University of British Columbia (March 2015, William Bendix and Paul J. Quirk, “Secrecy and negligence: How Congress lost control of domestic surveillance,” <http://www.brookings.edu/~/media/research/files/papers/2015/03/02-secrecy-negligence-congres-surveillance-bendix-quirk/ctibendixquirksecrecyv3.pdf>, JMP)

Even if Congress at some point enacted new restrictions on surveillance, the executive might ignore the law and continue to make policy unilaterally. The job of reviewing executive conduct would again fall to the FISA Court.56 In view of this court’s history of broad deference to the executive, Congress would have a challenge to ensure that legislative policies were faithfully implemented.

#### Executive lawyers provides the means to circumvent the plan

Shane, 12 --- Jacob E. Davis and Jacob E. Davis II Chair in Law, The Ohio State University Moritz School of Law (Peter M., Journal of National Security Law & Policy, “Executive Branch Self-Policing in Times of Crisis: The Challenges for Conscientious Legal Analysis,” 5 J. Nat'l Security L. & Pol'y 507))

II. The Breakdown of Government Lawyering The military and foreign policy disasters generated by presidential unilateralism demonstrate the practical importance of maintaining a pluralist view of checks and balances. Political officials are not simply rational actors who respond with dispassionate calculation to evidence and circumstance. Facts and options are always filtered through ideological prisms. Presidentialism narrows the prism. Pluralism works to offset that filtering. Pluralism guards against too much distortion by seeking to maximize the number of meaningful institutional voices in the policy making process. Equally troubling is the risk of presidentialism to the rule of law. Even in normal times, a heavy burden falls on government attorneys in virtually every agency. Government lawyering frequently represents the exclusive avenue through which the law is actually brought to bear on decisionmaking. This professional review within the executive branch is crucial. Most government decisions are simply too low in visibility, or too diffuse in impact, to elicit judicial review or congressional oversight as ways of monitoring legal compliance. Yet, the ideological prism of presidentialism can bend the light of the law so that nothing is seen other than the claimed prerogatives of the sitting chief executive. Champions of executive power - even skilled lawyers who should know better - wind up asserting that, to an extraordinary extent, the President as a matter of constitutional entitlement is simply not subject to legal regulation by either of the other two branches of government. [\*511] Government attorneys must understand their unique roles as both advisers and advocates. In adversarial proceedings before courts of law, it may be fine for each of two contesting sides, including the government, to have a zealous, and not wholly impartial, presentation, with the judge acting as a neutral decisionmaker. But in their advisory function, government lawyers must play a more objective, even quasi-adjudicative, role. They must give the law their most conscientious interpretation. If they fail in that task, frequently there will be no one else effectively situated to do the job of assuring diligence in legal compliance. Government lawyers imbued with the ideology of presidentialism too easily abandon their professional obligations as advisers and too readily become ethically blinkered advocates for unchecked executive power. Jack Goldsmith headed the Office of Legal Counsel (OLC) for a little less than ten months in 2003-2004. Of the work done by some government attorneys and top officials after 9/11, he said they dealt with FISA limitations on warrantless surveillance by the National Security Agency (NSA) "the way they dealt with other laws they didn't like: they blew through them in secret based on flimsy legal opinions that they guarded closely so no one could question the legal basis for the operations." n7 He describes a 2003 meeting with David Addington, who was Counsel and later Chief of Staff to Vice President Dick Cheney, in which Addington denied the NSA Inspector General's request to see a copy of OLC's legal analysis in support of the NSA surveillance program. Before Goldsmith arrived at OLC, "not even NSA lawyers were allowed to see the Justice Department's legal analysis of what NSA was doing." n8 OLC's analysis of the legality of NSA surveillance, issued on January 19, 2006, justified the program on two grounds: the President's inherent war powers and the Authorization for Use of Military Force (AUMF). However, the AUMF did not say anything about electronic surveillance. In 1978, Congress expressly stated that no statute other than the Foreign Intelligence Surveillance Act (FISA) or Title III - the law that applies to ordinary federal criminal prosecution - provides authority for electronic surveillance by the federal government. The AUMF could supersede FISA by repealing it, but only by making the repeal explicit. An argument that the AUMF implicitly repealed FISA necessarily falls short. OLC also argued that the President had an inherent constitutional power to conduct the NSA program no matter what FISA said. According to OLC, if FISA of 1978, as amended, were read to preclude the NSA program, the statute would be unconstitutional. n9 [\*512] What prompted the Justice Department to argue in this fashion? One answer might be that Justice Department lawyers are institutionally expected to advocate for the President's powers and simply adopt the most ambitious arguments consistent with appropriate standards of professional competence in legal research and analysis. However, it is not the responsibility of Justice Department lawyers to advocate for every contemplated assertion of presidential authority, no matter how far-fetched. Even in my brief period at Justice, I witnessed multiple and significant examples of Department lawyers refusing to provide analytic support for legally ill-conceived proposals for executive action. Moreover, it is difficult to make a case for the professional competence of the FISA memorandum. Although the Justice Department manages to elaborate its views in over forty pages of single-spaced and highly technical verbiage, its memorandum never confronts the enormity of the initiative it is endorsing or the power of alternative arguments. Instead, it proffers distinctions from contrary precedents that are often, in a word, silly. Even if the authors felt institutionally constrained to reach a particular bottom line, the failure to assert any principle limiting the claims being made and the too-frequent lack of rhetorical judgment in structuring their argument suggest something other than diligent lawyering was at play. What accounted for the bad arguments was political and professional pressure. When I worked at Justice, the refusal to take positions that could not be defended by respectable standards did not harm the lawyer. As anyone who has ever worked in an organization knows, however, informal pressure can be an extraordinarily effective method of stifling disagreement and guiding decisions in the way top management desires. We know that supervision of the process of executive branch lawyering on the NSA memorandum was significantly usurped by the Office of the Vice President. David Addington, the Vice President's Counsel, and John Yoo, then a deputy in OLC, worked together to craft a series of arguments for unprecedented claims of executive power to pursue the campaign against terrorism. n10 Jack Goldsmith reports that Addington blackballed from future advancement in the executive branch any lawyer who dared cross swords with him. n11 The deficiencies of legal analysis of NSA surveillance were replicated in other initiatives after 9/11, including the treatment of persons captured and suspected of aiding and abetting terrorism. The Justice Department, through OLC, produced legal opinions stating, in effect, that anyone [\*513] captured in the Afghanistan campaign had few, if any, rights under U.S. or international law and certainly no rights susceptible to vindication in U.S. courts. n12 The function of these legal opinions - indeed, their obvious purpose - was to ratify a scheme of maximum license to do with the detainees whatever the military, the CIA, or any other U.S. authority might choose to do with them. The Administration's lawyering process cleared the path to horrors at the Abu Ghraib prison and Guantanamo - crimes whose stain upon our national honor is likely to remain, for decades at least, firmly embedded in the world's collective memory, deeply undermining our image and influence abroad. It is understandable that the Administration would want some flexibility in dealing with a threat it rightly regarded as in some ways unprecedented and of very grave magnitude. And yet, to move the detainees so completely beyond the realm of normal legal process was itself a plainly risky strategy in terms of compromising international support, exposing U.S. military personnel to mistreatment, risking the honor of U.S. military culture, and weakening the fabric of international law generally in its protection of both combatants and civilians during wartime. The desire for flexibility was understandable, but not at the cost of all other values. On a number of the most important points discussed in the OLC lawyers' memoranda, the courts subsequently held them to be wrong. Contrary to OLC, the Supreme Court held that foreign detainees at Guantanamo who challenged their classification as enemy combatants were entitled to judicial review of the legality of their detention. n13 Contrary to OLC, the Court held that the Geneva Conventions protected the detainees, whether or not they strictly qualified as prisoners of war. n14 Contrary to OLC and Justice Department briefs, the Court held that the military commissions as originally constituted were not sufficiently protective of the detainees' rights to permit their use for war crimes trials. n15 On all of these questions, whether of morality, policy, or law, there were at least serious arguments to be entertained by both sides. The fact that the Administration reached incorrect conclusions is, in itself, only a limited indictment of its lawyering. Even good lawyers make mistakes, and the fact that executive branch lawyers would consistently make mistakes erring on the side of executive authority is not in itself damning. What is damning, however, is that on critical questions - questions going to the core of national honor and identity - executive branch lawyering was not just [\*514] wrong, misguided, or ethically insensitive. It was incompetent. It was so sloppy, so one-sided, and at times so laughably unpersuasive that it cannot be defended as ethical lawyering in any context. Tax advice this bad would be malpractice. Government lawyering this bad should be grounds for discharge.

### Yes Circumvention – Encryption

#### Yes circumvention – supercomputing brute attacks, voluntary cooperation, hacking, and subterfuge

Perloth, et al 13 (Nicole, technology and cybersecurity reporter for The New York Times, guest lecturer at Stanford’s graduate schools of business and communications, former deputy editor at Forbes, winner of the Society of American Business Editors and Writers award for best technology coverage in 2013, voted the top cybersecurity journalist by the SANS Institute in 2014, graduate of Stanford University’s Graduate School of Journalism, and Princeton University; Scott Shane, journalist for The New York Times, reporting principally about the United States intelligence community, former Moscow correspondent for The Baltimore Sun; “NSA Able to Foil Basic Safeguards of Privacy on Web, <http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0>) BJ

The agency, according to the documents and interviews with industry officials, deployed custom-built, superfast computers to break codes, and began collaborating with technology companies in the United States and abroad to build entry points into their products. The documents do not identify which companies have participated. The N.S.A. hacked into target computers to snare messages before they were encrypted. In some cases, companies say they were coerced by the government into handing over their master encryption keys or building in a back door. And the agency used its influence as the world’s most experienced code maker to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world. “For the past decade, N.S.A. has led an aggressive, multipronged effort to break widely used Internet encryption technologies,” said a 2010 memo describing a briefing about N.S.A. accomplishments for employees of its British counterpart, Government Communications Headquarters, or GCHQ. “Cryptanalytic capabilities are now coming online. Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable.”

#### NSA supercomputers can always decrypt

PTI 13 (The Economic Times, “NSA cracked online encryption technology”, 6 September 2013, http://articles.economictimes.indiatimes.com/2013-09-06/news/41835321\_1\_encryption-nsa-gchq)

Intelligence agencies of the US and the UK have teamed up to crack the encryption technology designed to provide online privacy that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, Internet chats and phone calls. The National Security Agency of the United States and its British counterpart Government Communications Headquarters (GCHQ) have cracked the encryption by using supercomputers, court orders, and some cooperation from technology companies, according to multiple media reports in the US and UK. The classified documents leaked by whistleblower Edward Snowden show the NSA has cracked much of the encryption that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, Internet chats and phone calls, the reports said. News articles by The Guardian, The New York Times and ProPublica reported that these classified documents reveal that unlike commonly presumed in the public, none of the data on internet is safe from prying eyes, including those of the government, and the NSA wants to keep it that way. "The agency treats its recent successes in deciphering protected information as among its most closely guarded secrets," The New York Times said. The NSA deployed custom-built, superfast computers to break codes, and began collaborating with technology companies in the US and abroad to build entry points into their products, but the documents do not identify which of the IT companies participated in it. The agency hacked into target computers to snare messages before they were encrypted, the report said. In some cases, companies say they were coerced by the government into handing over their master encryption keys or building in a back door. "And the agency used its influence as the world's most experienced code maker to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world," the report said. "For the past decade, NSA has led an aggressive, multipronged effort to break widely used Internet encryption technologies," said a 2010 memo describing a briefing about NSA accomplishments for employees of the GCHQ. The media outlets said they were asked by the intelligence officials not to publish the articles arguing that this might prompt foreign targets to switch to new forms of encryption or communications that would be harder to collect or read. The news organisations removed some specific facts but decided to publish the article because of the value of a public debate about government actions that weaken the most powerful privacy tools, media outlets reported.

#### Encryption doesn’t solve – Random number generators

Wayner 5/5/14 – Peter Wayner is contributing editor at InfoWorld and the author of more than 16 books on diverse topics, including open source software ("Free for All"), autonomous cars ("Future Ride"), privacy-enhanced computation ("Translucent Databases"), digital transactions ("Digital Cash"), and steganography ("Disappearing Cryptography"). (“Peter Wayner”; 11 reasons encryption is (almost) dead; http://www.infoworld.com/article/2607386/encryption/11-reasons-encryption-is--almost--dead.html)//pk

Encryption's weak link No. 8: Backdoors aplenty Sometimes programmers make mistakes. They forget to check the size of an input, or they skip clearing the memory before releasing it. It could be anything. Eventually, someone finds the hole and starts exploiting it. Some of the most forward-thinking companies release a steady stream of fixes that never seems to end, and they should be commended. But the relentless surge of security patches suggests there won't be an end anytime soon. By the time you've finished reading this, there are probably two new patches for you to install. Any of these holes could compromise your encryption. It could patch the file and turn the algorithm into mush. Or it could leak the key through some other path. There's no end to the malice that can be caused by a backdoor. Encryption's weak link No. 9: Bad random-number generators Most of the hype around encryption focuses on the strength of the encryption algorithm, but this usually blips over the fact that the key-selection algorithm is just as important. Your encryption can be superstrong, but if the eavesdropper can guess the key, it won't matter. This is important because many encryption routines need a trustworthy source of random numbers to help pick the key. Some attackers will simply substitute their own random-number generator and use it to undermine the key choice. The algorithm remains strong, but the keys are easy to guess by anyone who knows the way the random-number generator was compromised.

#### Even if backdoors are closed, NSA will just move on to hacking

Kopstein 7/17/15 <Joshua, cyberculture journalist and researcher and writer for AlJazeera, 7/17/15, “The feds don’t need digital backdoors – they can hack you”, Aljazeera, http://america.aljazeera.com/opinions/2015/7/the-feds-dont-need-digital-backdoors-they-can-hack-you.html>//wx

The massive hack of Hacking Team, a surveillance company notorious for selling spyware to repressive regimes, brought a wave of unrestrained schadenfreude to many social media feeds last week. A mysterious hacker [spilled more than 400 gigabytes](http://america.aljazeera.com/articles/2015/7/6/hacking.html%22%20%5Ct%20%22_blank) of the company’s emails, internal documents, source code and more across the Internet, allowing journalists to lay bare the inner workings of one of the most controversial players in the booming government surveillance industry. Privacy advocates have long been fascinated and appalled by Hacking Team, and for good reason. Its flagship spyware suite, Remote Control System, or RCS, is a [flashily advertised](https://www.youtube.com/watch?v=gxoYE8jzX0s" \t "_blank) “hacking suite for governmental interception” that allows police to quietly take control of electronic devices — reading emails and texts, recording keystrokes, snooping on Skype calls, even eavesdropping on the device’s microphone and webcam. Security researchers at the University of Toronto [previously discovered](https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/%22%20%5Ct%20%22_blank) the software targeting activists and journalists from the United Arab Emirates, Morocco and Ethiopia, using a hidden network of servers based in 21 countries. The company’s leaked emails and documents display a disturbing nonchalance about all of this, confirming highly questionable clients including Sudan, Ethiopia, Saudi Arabia, Uzbekistan, Bahrain, Kazakhstan and Tunisia, [among many others](http://motherboard.vice.com/read/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech%22%20%5Ct%20%22_blank). The U.S. government is also a customer: The Drug Enforcement Administration, Federal Bureau of Investigation and U.S. Army have all bought Hacking Team’s spyware, which is sold as a service with software updates and full customer support. The company also has plans for a U.S. branch, and is currently using [a front company](http://motherboard.vice.com/read/the-dea-has-been-secretly-buying-hacking-tools-from-an-italian-company%22%20%5Ct%20%22_blank) called Cicom USA to [drum up business with other North American agencies](https://twitter.com/CDA/status/618089403681009664%22%20%5Ct%20%22_blank) including the U.S. Department of Homeland Security, the Bureau of Alcohol Tobacco and Firearms, the New York City Police Department and the Royal Canadian Mounted Police. Of course, it’s ironic that none of this would have likely come to light if not for an act of hacking. But if there’s a singular lesson of the post-Snowden era, it’s that [extreme acts of transparency are sometimes the only remedy](http://america.aljazeera.com/opinions/2015/1/foia-congress-leaks.html%22%20%5Ct%20%22_blank) for extreme corporate and government secrecy. Armed with the knowledge that these intrusive tools are being sold to governments around the world, we must now begin a long-overdue debate about how, where and when — not to mention if — governments should be allowed to hack their own citizens. In the U.S., that debate could not come any sooner. Despite the fact that a lack of security led to the hack of the Office of Personnel Management, compromising a staggering [21 million government employee records](http://america.aljazeera.com/articles/2015/7/9/us-personnel-office-over-25-million-records-affected-by-hacking.html%22%20%5Ct%20%22_blank), U.S. law enforcement agencies such as the FBI are continuing [a campaign of fear](http://america.aljazeera.com/opinions/2015/4/feds-are-using-fear-not-facts-in-anti-encryption-crusade.html%22%20%5Ct%20%22_blank) against widespread encryption. They’re demanding that companies such as Apple and Google insert backdoors into their products so they can unscramble messages from criminals and terrorists, claiming that their inability to do so is causing investigations to “go dark.” But one important takeaway from the Hacking Team leak is that government agencies are doing just fine without backdoors. A key feature of Hacking Team’s software, and targeted surveillance in general, is the ability to overcome encryption by compromising individual “endpoints,” such as a computer or smartphone. But the documents show this capability is sometimes redundant. The FBI, for example, is so fully invested in homegrown hacking tools that it only bought Hacking Team spyware as a “backup” solution, according to leaked emails. If we reject digital backdoors — and we should — we can’t be unprepared when more unregulated hacking powers are the next thing on the FBI’s wish list. The FBI has been in the hacking business since the 1990s, yet its use of these tools and tactics has never been sufficiently scrutinized. In a rare public decision in 2013, a judge in Texas [denied an FBI request](http://www.theverge.com/2013/4/26/4269266/judge-denies-fbi-request-to-install-webcam-spyware-on-suspects-pc%22%20%5Ct%20%22_blank) to send spyware to an unidentified suspect’s computer, criticizing its “vague assurances” that innocent parties wouldn’t be affected. The FBI has since [argued it doesn’t need a warrant](http://arstechnica.com/tech-policy/2014/10/us-says-it-can-hack-into-foreign-based-servers-without-warrants/%22%20%5Ct%20%22_blank) to hack servers and electronic devices, even when they belong to targets whose identities and locations are unknown. This March, [a federal rule change](http://www.nationaljournal.com/tech/fbi-s-plan-to-expand-hacking-power-advances-despite-privacy-fears-20150316%22%20%5Ct%20%22_blank) that Google warned was a “monumental” constitutional threat granted judges the authority to let the FBI do just that. Amazingly, the FBI’s new authority to hack hasn’t decreased the momentum of its quest for backdoors. During a Congressional hearing last week, FBI director James Comey invoked the bogeyman of the Islamic State in Iraq and the Levant (ISIL) to illustrate the dangers of encryption, but once again failed to provide any actual evidence of the problem. (On the contrary, a recent government [report](http://www.uscourts.gov/statistics-reports/wiretap-report-2014%22%20%5Ct%20%22_blank) found only 4 cases last year in which federal and state wiretaps couldn’t circumvent encryption.) Sen. Sheldon Whitehouse (D-Rhode Island) even suggested that if commercial encryption prevents law enforcement access, companies such as Apple and Google that deploy it should be [held legally liable](http://motherboard.vice.com/read/senator-crime-victims-should-be-able-to-sue-apple-google-for-encrypting-data%22%20%5Ct%20%22_blank). At the same time, [a new report](http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf%22%20%5Ct%20%22_blank) (PDF) from some of the world’s most prominent security experts authoritatively concluded that enforcing backdoors would be disastrous for security. To wit: You can’t build a backdoor for the FBI that can’t also be found and exploited by Chinese hackers, Russian cybercriminals or any other advanced adversary that cares to look. On Thursday, the Web’s international standards body, the World Wide Web Consortium,[concurred](https://w3ctag.github.io/encryption-finding/%22%20%5Ct%20%22_blank), writing, “It is impossible to build systems that can securely support ‘exceptional access’ capabilities without breaking the trust guarantees of the web platform.” Boiled down, the crypto debate really becomes a question of mass surveillance versus targeted surveillance. Backdoors would remove the technical barriers preventing governments from having unfettered access to everyone’s communications. Hacking, meanwhile, circumvents those barriers using highly invasive but much more targeted means. Of the two options, the latter seems vastly preferable. Surveillance should be rare, and hacking forces authorities to make a cost-benefit analysis. That’s because computers are generally hacked by exploiting hidden flaws in software code; since those flaws are eventually found and patched, it often that means the attacker needs to be really sure the target is worth it. The problem is that law enforcement wants both backdoors and hacking powers — and we still haven’t had a debate about the latter. What kind of suspects should law enforcement be allowed to hack? What will stop authorities from planting evidence on someone’s computer? Given the well-known [problem of attribution](https://medium.com/message/attribution-is-hard-4164f8389eb8%22%20%5Ct%20%22_blank) in online crime investigations, how will they ensure they’re hacking the right person and that no innocents will get caught up in the process? These are questions that need to be debated and answered now. If we reject backdoors [the way we did two decades ago](http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html%22%20%5Ct%20%22_blank) — and we should — we can’t be unprepared when more unregulated hacking powers are the next thing on the FBI’s wish list.

### Yes Circumvention – FBI

#### FBI will circumvent the plan – empirics

Lendman 2015 (Stephen; Unconstitutional mass FBI aerial surveillance; Jun 10; www.thesleuthjournal.com/unconstitutional-mass-fbi-aerial-surveillance/; kdf)

Free and open societies don’t spy on their citizens. They don’t invent phony threats as justification. America is a belligerent nation waging endless wars of aggression against invented enemies. Fear-mongering is rife. It’s done to rape, ravage and destroy one country after another. It’s a tactic used to scare people to believe they’re safer by sacrificing fundamental freedoms. Mass surveillance is a defining rogue state characteristic. Post-9/11, government-usurped authority turned America into a police state. Big Brother watches everyone. Tuesday Senate passage of the USA Freedom Act (the renamed Patriot Act) changed little. Government intrusion into the private lives of its citizens remains largely unchanged. The only good news is that USAF slightly rolled back its intrusiveness instead of giving spy agencies more powers. History shows restrictions imposed are easily circumvented or ignored. A separate article discusses systematic FBI misuse of Patriot Act authority. Bureau secrecy and cover-up make it impossible to know the full extent of its lawlessness. It operates ad libitum with minimum oversight and accountability. One example is its mass surveillance of US citizens by drones and other aircraft. On June 2, AP reported “(s)cores of low-flying planes circling American cities…” “They’re “part of a civilian air force operated by the FBI and obscured behind fictitious companies…” It’s not secret. It’s been reported before. In July 2013, the agency admitted using drones for domestic surveillance numerous times without court authorized warrants or other forms of oversight. At the time, deputy director Stephen D. Kelly said “(t)he FBI uses UAVs in very limited circumstances to conduct surveillance when there is a specific operational need.” “Since late 2006, the FBI has conducted surveillance using UAVs in eight criminal cases and two national security cases.” Former FBI director Robert Meuller admitted spying on US citizens with no “operational guidelines.” Warrantless spying by any means threatens everyone. No probable cause is needed. No restraints are imposed. Constitutional protections are circumvented. Once a program is established, it takes on a life of its own. In the last decade, FBI aerial spying expanded to “civilian air force” level. In April alone, AP identified at least 50 FBI aircraft conducting more than 100 flights over urban and rural areas in 11 states. It cited a 2009 budget document indicating 115 planes, including 90 Cessna aircraft. FBI aerial spying is longstanding. Today, drones and other aircraft are equipped with high-tech cameras for close-up visual surveillance as well as technology able to monitor thousands of cell phones – a blatant breach of privacy. According to Senate Judiciary Committee chairman Charles Grassley (R. IA): “It’s important that federal law enforcement personnel have the tools they need to find and catch criminals.” “But whenever an operation may also monitor the activities of Americans who are not the intended target, we must make darn sure that safeguards are in place to protect the civil liberties of innocent Americans.” No safeguards whatever exist – nor does Congress back up high-minded rhetoric with effective policies protecting the public from abusive government practices. Rogue agencies like the FBI, NSA, CIA, DEA and Homeland Security operate by their own rules – easily circumventing weak and ineffective restraints on their authority.

#### Recent Inspector General report confirms the plan gets circumvented

Lendman 2015 (Stephen; FBI Misuse of Patriot Act Authority; Jun 3; sjlendman.blogspot.com/2015/06/fbi-misuse-of-patriot-act-authority.html; kdf)

America is a police state. The FBI is the nation's Gestapo. It's abuse of power and misconduct are longstanding. It's an instrument for systematically violating civil liberties. It's a rogue agency operating unconstitutionally. Bureau secrecy and cover-up make it impossible to know the full extent of its lawlessness. It operates with minimal oversight and accountability. A new Justice Department Office of the Inspector General (OIG) report titled "A Review of the FBI's Use of Section 215 Orders: Assessment of Progress in Implementing Recommendations and Examination of Use in 2007 - through 2009." Section 215 of the Patriot Act tramples on Bill of Rights protections. Its language is vague and deceptive. It's used to permit unconstitutional meta-data mining. It allows police state investigatory practices. It authorizes government access to "any tangible item" - including personal financial records and transactions, medical records, phone conversations, emails, other Internet use and whatever else Washington wants to monitor. FBI powers are sweeping. They're greatly enhanced. They're used extrajudicially. Anyone can be spied on for any reason or none at all. No probable cause, reasonable grounds, or suspicions are needed. Exercising free expression makes you vulnerable. Section 215 is unconstitutional. It permits warrantless searches without probable cause. It violates First Amendment rights by mandating secrecy. It prohibits targeted subjects from telling others what's happening to them. It compromises free expression, assembly and association by authorizing the FBI to investigate anyone based on what they say, write, or do with regard to groups they belong to or associate with. It violates Fourth and Fifth Amendment protections by not telling targeted subjects their privacy was compromised. It subverts fundamental freedoms for contrived, exaggerated, or nonexistent security reasons. Section 215 powers expire on June 1 if Congress fails to extend them. So far, enough votes are lacking to do so. The battle continues. Senate Majority Leader Mitch McConnell called for another reauthorization vote on Sunday, May 31 before the provision expires. House leaders oppose re-extension. In early May, the US Second Circuit Court of Appeals struck down bulk NSA phone spying. It ruled Section 215 doesn't permit bulk collection of Americans' phone records. A three-judge panel ruled unanimously - overturning a lower court decision. It said collecting and storing meta-data "anywhere in the private sector (constitutes) an unprecedented and unwarranted contraction of the privacy expectations of all Americans." The FBI administers the law. It gets secretive virtually rubber-stamp Foreign Intelligence Surveillance Court (FISC) authorization for the NSA and itself to do so. OIG's new report discusses the FBI's egregious abuse of Section 215 powers. The 2005 Patriot Act Reauthorization required the agency to follow "minimization procedures" to limit the amount of private information collected, retained, disseminated and used - often inappropriately. The FBI failed to comply until March 2013 - nor NSA. Illegal interpretation of Section 215 persists. NSA abuse of power is notorious. The FBI concocted a set of so-called "Interim Procedures" under which it unilaterally decided it could obey its congressionally mandated procedures by declaring its preexisting duties enough. Section 215 minimization procedures in force contain vague language with lots of wiggle room permitting retention of information "necessary to understand foreign intelligence." In other words, whatever the FBI claims it needs to protect against alleged foreign threats (real or invented) is OK to collect, retain and use in whatever way the agency wishes - undermining privacy protections. The FBI, like the NSA, is a secretive agency operating unaccountably. Whatever it does is OK because nothing is done constrain it. Illegal surveillance persists out-of-control. Section 215 is a license for abuse. Secrecy hides the worst of what goes on. Even when federal courts strike down abusive practices, they persist. Agencies like the FBI and NSA operate extrajudicially. Reform is only possible by shutting them down entirely - replacing them with heavily constrained new agencies operating under strict regulations and oversight.

#### FBI surveillance continues even after restrictions on its activities

Fisher, 4 --- Associate Professor of Law and Director, Center for Social Justice, Seton Hall Law School (Winter 2004, Linda E., Arizona Law Review, “Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups,” 46 Ariz. L. Rev. 621, Lexis, JMP)

The history of the FBI and other law enforcement surveillance gives scant comfort to those engaged in lawful political and religious activities who are [\*623] concerned about becoming targets of surveillance. n5 From its inception until restrictions on its activities were imposed in the mid-1970s - and even sometimes thereafter - the FBI regularly conducted politically motivated surveillance, choosing targets based on their political or religious beliefs. As part of its investigations, it compiled and widely disseminated political dossiers, engaged in warrantless searches, and disrupted the lawful First Amendment activities of a wide array of groups opposed to government policy. n6 Local police "Red Squads" did the same. n7 During the war in Vietnam, the CIA, despite restriction of its mission to foreign intelligence, also conducted domestic surveillance operations. n8 Religious groups engaged in political activity were among the targets of intelligence agency investigations. n9

### Yes Circumvention – NSA

#### The NSA will circumvent the plan

Ackerman 2015 (Spencer; Fears NSA will seek to undermine surveillance reform; Jun 1; www.theguardian.com/us-news/2015/jun/01/nsa-surveillance-patriot-act-congress-secret-law; kdf)

Privacy advocates fear the National Security Agency will attempt to weaken new restrictions on the bulk collection of Americans’ phone and email records with a barrage of creative legal wrangles, as the first major reform of US surveillance powers in a generation looked likely to be a foregone conclusion on Monday. The USA Freedom Act, a bill banning the NSA from collecting US phone data in bulk and compelling disclosure of any novel legal arguments for widespread surveillance before a secret court, has already been passed by the House of Representatives and on Sunday night the Senate voted 77 to 17 to proceed to debate on it. Between that bill and a landmark recent ruling from a federal appeals court that rejected a longstanding government justification for bulk surveillance, civil libertarians think they stand a chance at stopping attempts by intelligence lawyers to undermine reform in secret. Attorneys for the intelligence agencies react scornfully to the suggestion that they will stretch their authorities to the breaking point. Yet reformers remember that such legal tactics during the George W Bush administration allowed the NSA to shoehorn bulk phone records collection into the Patriot Act. Rand Paul, the Kentucky senator and Republican presidential candidate who was key to allowing sweeping US surveillance powers to lapse on Sunday night, warned that NSA lawyers would now make mincemeat of the USA Freedom Act’s prohibitions on bulk phone records collection by taking an expansive view of the bill’s definitions, thanks to a pliant, secret surveillance court. “My fear, though, is that the people who interpret this work at a place known as the rubber stamp factory, the Fisa [court],” Paul said on the Senate floor on Sunday. Paul’s Democratic ally, Senator Ron Wyden, warned the intelligence agencies and the Obama administration against attempting to unravel NSA reform. “My time on the intelligence committee has taught me to always be vigilant for secret interpretations of the law and new surveillance techniques that Congress doesn’t know about,” Wyden, a member of the intelligence committee, told the Guardian. “Americans were rightly outraged when they learned that US intelligence agencies relied on secret law to monitor millions of law-abiding US citizens. The American people are now on high alert for new secret interpretations of the law, and intelligence agencies and the Justice Department would do well to keep that lesson in mind.” The USA Freedom Act is supposed to prevent what Wyden calls “secret law”. It contains a provision requiring congressional notification in the event of a novel legal interpretation presented to the secret Fisa court overseeing surveillance. Yet in recent memory, the US government permitted the NSA to circumvent the Fisa court entirely. Not a single Fisa court judge was aware of Stellar Wind, the NSA’s post-9/11 constellation of bulk surveillance programs, from 2001 to 2004.

### Fill-in

#### A litany of other programs prove the aff fails

Cohn and Crocker 2015 (Cindy & Andrew [Electronic Frontier Foundation]; Don’t Worry, The Government Still Has Plenty Of Surveillance Power Despite Section 215 Sunset; Jun 2; www.defendingdissent.org/now/dont-worry-the-government-still-has-plenty-of-surveillance-power-despite-section-215-sunset/; kdf)

The story being spun by the defenders of Section 215 of the Patriot Act and the Obama Administration is that if the law sunsets entirely, the government will lose critical surveillance capabilities. The fearmongering includes President Obama, who said: “heaven forbid we’ve got a problem where we could’ve prevented a terrorist attack or could’ve apprehended someone who was engaged in dangerous activity but we didn’t do so.” So how real is this concern? Not very. Section 215 is only one of a number of largely overlapping surveillance authorities, and the loss of the current version of the law will leave the government with a range of tools that is still incredibly powerful. First, there’s the most famous use of Section 215—the bulk collection of telephone records by the NSA. Of course, no matter what law the government relies on, bulk surveillance is unconstitutional. But equally importantly, it doesn’t work. Every assessment about the bulk collection of telephone records, including two by hand-picked administration panels, have concluded that “collecting it all” hasn’t materially aided any terrorism investigation. The same goes for other still-secret bulk surveillance programs under Section 215, the latest evidence of which came in a recently released oversight report by the Justice Department’s Office of the Inspector General (OIG). And then there’s the matter of targeted investigations. The ACLU’s Jameel Jaffer has explainedthat this too is scaremongering, because “the sunset of Section 215 wouldn’t affect the government’s ability to conduct targeted investigations of terrorist threats.” That’s because even without Section 215, the government still has broad powers to collect information during its national security investigations. EFF believes that many of these laws can be scaled back and made more transparent as well, but given the current situation, these are the tools in the national security investigators’ toolbox: Pen Registers: These allow the government to collect “dialing, routing, addressing, or signaling information” including telephone numbers dialed and Internet metadata such as IP addresses and email headers. There are two pen register statutes, one for foreign intelligence surveillance and one for law enforcement. Both rely require only that the pen register be likely to obtain information relevant to a national security or criminal investigation respectively. Until the end of 2011, the NSA used the Foreign Intelligence Surveillance Act (FISA) pen register statute to conduct mass surveillance of Internet metadata, much as it still uses Section 215 for mass collection of telephone records. The Pre-Patriot Act Business Records Provision: Before the passage of the Patriot Act in 2001, FISA contained a provision allowing the government to obtain business records from transportation carriers and storage facilities. Harley Geiger of the Center for Democracy and Technology has pointed out that under a June 1 sunset, FISA would simply revert to this provision. An ECPA “D Order”: Under Section 2703(d) of the Electronic Communications Privacy Act (ECPA), the government can get a court order for information from ISPs or other communications providers about their customers, including the sorts of metadata the government gets with Section 215. To get a D Order, the government must provide “specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation.” Grand Jury Subpoenas: Given that Section 215 explicitly says that the FISA Court (FISC) “may only require the production of a tangible thing if such thing can be obtained” with a grand jury subpoena, it’s apparent that a grand jury subpoena is a reasonable substitute, at least where a grand jury can be convened. National Security Letters (NSLs): Similar to subpoenas, NSLs allow intelligence agencies to collect records from a range of entities including telecommunications providers, financial institutions, credit reporting bureaus, travel agencies and others. Nearly all NSLs include self-certified gag orders, which EFF has successfully challenged as unconstitutional. Nevertheless, the FBI and other agencies can use NSLs to collect much the same information as Section 215, although the government has also misused NSLs to obtain communication records not authorized by the NSL statute. Administrative Subpoenas: Many federal agencies have the authority to issue subpoenas for customer records in their normal course of business. These authorities are extremely widespread, comprising 335 different statutes by one count. FISA Warrants: Under FISA, the government can get warrants from the FISC forelectronic surveillance and physical searches in the context of national security investigations. Although these require a higher showing—probable cause—statistics compiled by EPIC show the FISC routinely issues them, and has done so since FISA was passed in 1978.

#### Other countries spy on US citizens –the ultimate violation of privacy

Wittes June 18, 2015 (Benjamin [editor in chief of Lawfare and a Senior Fellow in Governance Studies at the Brookings Institution]; Turns out privacy groups are outraged about the OPM Hack-At me; www.lawfareblog.com/turns-out-privacy-groups-are-outraged-about-opm-hack—-me; kdf)

The other day, I wrote a little piece about the silence among our self-appointed privacy guardians at the monstrous breach of privacy perpetrated by the Chinese in the OPM hack. The piece made the (I think) modest observation that privacy groups—who have denounced NSA collection obsessively though it takes place under the rule of law and with strict restrictions—have had remarkably little to say about the mass collection of the most sensitive sorts of data, and I spectulated about the reason for that silence: the privacy community is virtually silent. Look on the websites of the major privacy groups and you'll see almost nothing about this program. Don't look for breathless coverage of it on the The Intercept either. The reason? This giant surveillance program isn't being run by the United States government. It's being run against the U.S. government—by the Chinese government. And for some reason, even the grossest of privacy violations—in this case the pilfering of millions of background investigations and personnel records—just doesn't seem so bad when someone other than the United States is doing it. I didn't expect this piece to make me many friends, but I have been amused and a bit surprised by the harsh reactions from a number of privacy groups on Twitter. In particular, Harley Geiger of CDT and Chris Soghoian of the ACLU seemed to take particular umbrage---both issuing lengthy streams of tweets denouncing the piece. Neither made points that seem to me to warrant response. In the flurry of invective, however, there was one point that seemed to me substantial and worth addressing. That was made by the Cato Institute's Julian Sanchez, somewhat crudely, on Twitter, as well as by a correspondent by email: I didn't expect this piece to make me many friends, but I have been amused and a bit surprised by the harsh reactions from a number of privacy groups on Twitter. In particular, Harley Geiger of CDT and Chris Soghoian of the ACLU seemed to take particular umbrage---both issuing lengthy streams of tweets denouncing the piece. Neither made points that seem to me to warrant response. In the flurry of invective, however, there was one point that seemed to me substantial and worth addressing. That was made by the Cato Institute's Julian Sanchez, somewhat crudely, on Twitter, as well as by a correspondent by email: Is Sanchez right here? Should we understand the silence of privacy groups on this score as just reflecting the fact that there's no controversy, that everyone agrees the conduct is terrible? Sanchez goes on to point out that most advocacy work is directed at one's own government. So maybe the privacy groups are making a tactical judgment that it's better to focus on their own government and its policies than that a foreign authoritarian sovereign over which one has no influence. In this account, the issue is not so much a double standard as a hard-headed assessment of where one's energy is best spent. There are several reasons why I think this is not an adequate account of the behavior of the privacy groups in this instance, nd to the extent it does explain their behavior, why I think they are grossly misjudging the merits of the matter. For one thing, human rights groups comment all the time on the behavior of governments over which they have no influence. Glance at the front page of Human Rights Watch's home page and you won't see the implausibility of the group's influencing Russian or Angolan policy inhibiting HRW from talking about what governments are doing. Yes, it's true that democracies subject to human rights suasion tend to get more of it as a result of their responsiveness. But this does not explain the near-total silence on the part of the privacy groups about Chinese behavior on this score. Tilting at authoritarian windmills is part of what human rights advocacy is. Second and more importantly, privacy issues associated with giant international hacks are unlike other human rights issues in at least one fundamental sense. When China abuses due process or stifles free speech or tortures people, or harvests their organs, its victims are its own people. A U.S. advocacy group can reasonably take the position that, though terrible, this is not really that group's problem but a problem between the Chinese government and its people and civil society. Conversely, if you're a privacy group devoted to protecting the privacy of Americans, the OPM hack should be unthinkable to ignore. It is, after all, a far bigger threat to the interests you are pledged to protect than is any activity by your own government. You may have an argument for leaving Chinese domestic collection to Chinese civil libertarians to restrain, but to the extent you don't speak up against the bulk collection of the health records of kids of U.S. federal employees, you are tolerating an absurd double standard in which anyone can ride roughshod over Americans' privacy except the United States government.

## Circumvention Bad

### 1NC – relations and internet turn

#### Future circumventions tanks US relations with key countries & destroys internet hegemony

Greenwald 2014 (Glenn [Constitutional lawyer- patriot]; CONGRESS IS IRRELEVANT ON MASS SURVEILLANCE. HERE’S WHAT MATTERS INSTEAD; Nov 19; https://firstlook.org/theintercept/2014/11/19/irrelevance-u-s-congress-stopping-nsas-mass-surveillance/; kdf)

\*\*Chart omitted

2) Other countries taking action against U.S. hegemony over the internet. Most people who claim nothing has changed from the Snowden disclosures are viewing the world jingoistically, with the U.S. the only venue that matters. But the real action has long been in other countries, acting individually and jointly to prevent U.S. domination of the internet. Brazil is building a new undersea internet infrastructure specifically to avoid U.S. soil and thus NSA access. That same country punished Boeing by denying the U.S. contractor a long-expected $4.5 billion contract for fighter jets in protest over NSA spying. Another powerful country, Germany, has taken the lead with Brazil in pushing for international institutions and regulatory schemes to place real limits on NSA mass surveillance. U.S. diplomatic relations with numerous key countries have been severely hampered by revelations of mass surveillance. In July, Pew reported that “a new…survey finds widespread global opposition to U.S. eavesdropping and a decline in the view that the U.S. respects the personal freedoms of its people” and that, while the U.S. remains popular in many countries, particularly relative to others such as China, “in nearly all countries polled, majorities oppose monitoring by the U.S. government of emails and phone calls of foreign leaders or their citizens.” After just one year of Snowden reporting, there have been massive drops in the percentage of people who believe “the U.S. government respects personal freedom,” with the biggest drops coming in key countries that saw the most NSA reporting: All of that has significantly increased the costs for the U.S. to continue to subject the world, and the internet, to dragnets of mass surveillance. It has resulted in serious political, diplomatic, and structural impediments to ongoing spying programs. And it has meaningfully altered world opinion on all of these critical questions.

#### Internet freedom is key to solve all impacts

Genachowski and Bollinger 2013(Julius [Chairman of the FCC] and Lee [President of Columbia U]; The plot to block internet freedom; Apr 16; www.foreignpolicy.com/articles/2013/04/16/plot\_block\_internet\_freedom?page=full; kdf)

The Internet has created an extraordinary new democratic forum for people around the world to express their opinions. It is revolutionizing global access to information: Today, more than 1 billion people worldwide have access to the Internet, and at current growth rates, 5 billion people -- about 70 percent of the world's population -- will be connected in five years. But this growth trajectory is not inevitable, and threats are mounting to the global spread of an open and truly "worldwide" web. The expansion of the open Internet must be allowed to continue: The mobile and social media revolutions are critical not only for democratic institutions' ability to solve the collective problems of a shrinking world, but also to a dynamic and innovative global economy that depends on financial transparency and the free flow of information. The threats to the open Internet were on stark display at last December's World Conference on International Telecommunications in Dubai, where the United States fought attempts by a number of countries -- including Russia, China, and Saudi Arabia -- to give a U.N. organization, the International Telecommunication Union (ITU), new regulatory authority over the Internet. Ultimately, over the objection of the United States and many others, 89 countries voted to approve a treaty that could strengthen the power of governments to control online content and deter broadband deployment. In Dubai, two deeply worrisome trends came to a head. First, we see that the Arab Spring and similar events have awakened nondemocratic governments to the danger that the Internet poses to their regimes. In Dubai, they pushed for a treaty that would give the ITU's imprimatur to governments' blocking or favoring of online content under the guise of preventing spam and increasing network security. Authoritarian countries' real goal is to legitimize content regulation, opening the door for governments to block any content they do not like, such as political speech. Second, the basic commercial model underlying the open Internet is also under threat. In particular, some proposals, like the one made last year by major European network operators, would change the ground rules for payments for transferring Internet content. One species of these proposals is called "sender pays" or "sending party pays." Since the beginning of the Internet, content creators -- individuals, news outlets, search engines, social media sites -- have been able to make their content available to Internet users without paying a fee to Internet service providers. A sender-pays rule would change that, empowering governments to require Internet content creators to pay a fee to connect with an end user in that country. Sender pays may look merely like a commercial issue, a different way to divide the pie. And proponents of sender pays and similar changes claim they would benefit Internet deployment and Internet users. But the opposite is true: If a country imposed a payment requirement, content creators would be less likely to serve that country. The loss of content would make the Internet less attractive and would lessen demand for the deployment of Internet infrastructure in that country. Repeat the process in a few more countries, and the growth of global connectivity -- as well as its attendant benefits for democracy -- would slow dramatically. So too would the benefits accruing to the global economy. Without continuing improvements in transparency and information sharing, the innovation that springs from new commercial ideas and creative breakthroughs is sure to be severely inhibited. To their credit, American Internet service providers have joined with the broader U.S. technology industry, civil society, and others in opposing these changes. Together, we were able to win the battle in Dubai over sender pays, but we have not yet won the war. Issues affecting global Internet openness, broadband deployment, and free speech will return in upcoming international forums, including an important meeting in Geneva in May, the World Telecommunication/ICT Policy Forum. The massive investment in wired and wireless broadband infrastructure in the United States demonstrates that preserving an open Internet is completely compatible with broadband deployment. According to a recent UBS report, annual wireless capital investment in the United States increased 40 percent from 2009 to 2012, while investment in the rest of the world has barely inched upward. And according to the Information Technology and Innovation Foundation, more fiber-optic cable was laid in the United States in 2011 and 2012 than in any year since 2000, and 15 percent more than in Europe. All Internet users lose something when some countries are cut off from the World Wide Web. Each person who is unable to connect to the Internet diminishes our own access to information. **We become less able to understand the world and formulate policies to respond to our shrinking planet**. Conversely, we gain a richer understanding of global events as more people connect around the world, and those societies nurturing nascent democracy movements become more familiar with America's traditions of free speech and pluralism. That's why we believe that the Internet should remain free of gatekeepers and that no entity -- public or private -- should be able to pick and choose the information web users can receive. That is a principle the United States adopted in the Federal Communications Commission's 2010 Open Internet Order. And it's why we are deeply concerned about arguments by some in the United States that broadband providers should be able to block, edit, or favor Internet traffic that travels over their networks, or adopt economic models similar to international sender pays. We must preserve the Internet as the most open and robust platform for the free exchange of information ever devised. Keeping the Internet open is perhaps the most important free speech issue of our time.

### Impact: Circumvention Turns Case

#### The plan will be used as a rouse to expand the power of intelligence groups – empirics

Groll 2015 (Elias [assistant editor at Foreign Policy]; Congress May Have Passed the Freedom Act, But Mass Surveillance Is Alive and Well; Jun 4; foreignpolicy.com/2015/06/04/congress-may-have-passed-the-freedom-act-but-mass-surveillance-is-alive-and-well/; kdf)

One useful way to think about the USA Freedom Act that President Barack Obama signed into law on Tuesday night is as a lightning-rod for the National Security Agency. By changing the way the NSA examines domestic phone records, the agency is now able to make the argument that it has undergone significant reforms in the aftermath of the Edward Snowden revelations. By giving up the authority to collect all American phone records, the agency has paid a small price — and gotten rid of a program that it had come to consider a burden, anyway — to keep its most important authorities intact. The full measure of those powers were on prominent display in the New York Times on Thursday, when the paper reported that the agency has expanded its “warrantless surveillance of Americans’ international Internet traffic to search for evidence of malicious computer hacking.” The NSA, the paper reported, has also partnered with the FBI to provide federal investigators with intelligence about computer intrusions carried out by foreign powers, according to documents provided by Snowden. There is no evidence of outright wrongdoing in Thursday’s reports, but they signal another expansion of the NSA’s authorities to collect data on the Internet. Sen. Patrick Leahy, the Vermont Democrat and ranking member of the Judiciary Committee, said Thursday’s report “underscores the critical importance of placing reasonable and commonsense limits on government surveillance in order to protect the privacy of Americans” and that “Congress should have an open, transparent and honest debate about how to protect both our national security and our privacy.” Jonathan Mayer, a cybersecurity researcher, told the Times that FBI use of NSA data to combat cybercrime threatens to conflate the latter’s intelligence gathering role with the former’s law enforcement mandate. “That’s a major policy decision about how to structure cybersecurity in the U.S. and not a conversation that has been had in public,” he said. In short, the Times report, which was published in conjunction with ProPublica, reveals that the NSA has directed some of its most powerful tools toward cracking down on state-sponsored hackers online. The agency now has the power to search the data streams it has access to for snippets of code and other identifying information to spot hackers and track their activities. It is doing so by relying on one of its most important tools: Its position atop the global Internet infrastructure. The NSA has risen to become the world’s most powerful intelligence agency in no small part because a huge amount of the world’s Internet traffic flows through the United States. Fiber optic cables carry large amounts of Internet data from one part of the world to another, and when that traffic arrives in the United States, the NSA is there to have a look at it. Section 702 of the FISA Amendments Act governs parts of the NSA’s relationship with U.S. telecommunications companies, and it is through such companies that the NSA is able to access enormous troves of data for terrorism and foreign intelligence purposes. Privacy activists are concerned that such collection activities potentially hoover up the communications of ordinary Americans, and Thursday’s revelation that the FBI is now allowed to partake of some data collected from telecom activities is likely to add to those concerns. According to the Times and ProPublica, the FBI’s access to such data — which is routed to a data center in Quantico, Virginia — is focused on foreign hackers trying to penetrate U.S. data systems. That’s a mission that’s central to the U.S. government’s obligations to combat cybercrime, but the contention of rights activists is that that effort has become far too reliant on the tools of mass data collection. Thursday’s reports signal just how far these activists have to go if they hope to rein in the NSA’s powers.

#### Empirically, the plan makes surveillance worse because it provides cover for circumvention

Vladeck 2015 (Stephen [Prof of Law @ American U]; Forget the Patriot Act-Here are the privacy violations you should be worried about; June 1; foreignpolicy.com/2015/06/01/section-215-patriot-act-expires-surveillance-continues-fisa-court-metadata/; kdf)

The Obama administration, along with a number of more moderate members of Congress, took more of a middle road, calling for the fairly modest reforms provided by the USA Freedom Act, which would replace the phone records program with a somewhat less open-ended (and somewhat better regulated) series of authorities for the government to obtain and review similar data — and which the House of Representatives overwhelmingly passed on May 13. But whatever the merits of the competing sides in this debate, the larger problem is that this conversation has missed the forest for a very small — and largely irrelevant — tree. In fact, from the perspective of individual privacy rights, the phone records program is much less problematic than the government’s other authorities to conduct mass surveillance under Executive Order 12333 and the 2008 FISA Amendments Act. And so, in focusing on how to “fix” Section 215, we’ve given short shrift to the far more significant problems raised by these other authorities — and, just as importantly, the broader lessons we should be taking away from the surveillance reform conversation that Snowden started.

### Impact: Internet Good – Warming

**The internet is key to cloud computing key which solves climate modeling**

**Boyce, 10**

[Eric, technical writer and user advocate for The Rackspace Cloud, September 14, 2010 <http://www.rackspacecloud.com/blog/2010/09/14/the-future-of-cloud-computing-the-big-25-in-the-next-25/>]

The promise of the cloud isn’t just about gaming and the ability to safely store all those photos that you wish you hadn’t ever taken. Many of **the most promising cloud-based applications** also **require massive computational power**. Searching a database of global DNA samples requires abundant, scalable processing power. Modeling protein folding is another example of how compute resources will be used. Protein folding is linked to many diseases including Alzheimer’s and cancer, and analyzing the folding process can lead to new treatments and cures, but it requires enormous compute power. Projects like Folding@home are using distributed computing to tackle these modeling tasks. **The cloud will offer a larger, faster, more scalable way to process data and thus benefit any heavy data manipulation task**. 6. Is it going to be hot tomorrow? Like protein folding modeling, **climate simulation and forecasting requires a large amount of data storage and processing.** Recently the German Climate Computing Center (DKRZ) **installed a climate calculating supercomputer that is capable of analyzing 60 petabytes of data (**roughly 13 million DVD’s) at over 158 teraflops (trillion calculations per second). In the next couple of decades, this level of computing power **will be widely available and will exist on remote hardware. Sophisticated climate models combined with never before seen compute power will provide better predictions of climate change and more rapid early warning systems**

**Key to warming adaptation**

**Pope, 10**

[ Vicky Pope is the head of climate science advice at the Met Office Hadley Centre, “ How science will shape climate adaptation plans,” 16 September 2010, <http://www.guardian.co.uk/environment/cif-green/2010/sep/16/science-climate-change-adaptation>]

Some would argue that **the demand for information on how climate change will affect our future outstrips the current capability of the science and climate models.** My view is that **as scientists**, we can provide useful information, but **we need to** be clear about its limitations and **strive to improve information** **for the future**. We need to be clear about the uncertainties in our projections while still extracting useful information for practical decision-making. I have been involved in developing climate models for the last 15 years and despite their limitations we are now able to assess the probability of different outcomes for the first time. That means **we can quantify the risk of** these **outcomes happening**. These projections – the UK climate projections published in 2009 - are already forming the backbone of adaptation decisions being made in the UK for 50 to 100 years ahead. A project commissioned by the Environment Agency to investigate the impact of climate change on the Thames estuary over the next 100 years concluded that current government predictions for sea level rise are realistic. A major outcome from the scientific analysis was that the worst-case scenarios for high water levels can be significantly reduced - from 4.2m to 2.7m – because we are able to rule out the more extreme sea level rise. As a result, massive investment in a tide-excluding estuary barrage is unlikely to be needed this century. This will be reviewed as more information becomes available, taking a flexible approach to adaptation. The energy industry, working with the Met Office, looked at the likely impact of climate change on its infrastructure. The project found that very few changes in design standards are required, although it did highlight a number of issues. For instance, transformers could suffer higher failure rates and efficiency of some types of thermal power station could be markedly reduced because of increasing temperatures. A particular concern highlighted by this report and reiterated in today's report from the Climate Change Committee - the independent body that advises government on its climate targets - is that little is known about how winds will change in the future - important because of the increasing role of wind power in the UK energy mix. Fortunately many people, from private industry to government, recognise the value of even incomplete information to help make decisions about the future. **Demand for climate information is increasing, particularly relating to changes in the short to medium term**. **More still needs to be done to refine the climate projections and make them more usable and accessible. This is especially true if we are to provide reliable projections for the next 10 to 30 years. The necessary science and modelling tools are being developed,** and the first tentative results are being produced. We need particularly to look at how we communicate complex and often conflicting results. In order to explain complex science to a lay audience, scientists and journalists are prone to progressively downplay the complexity. Conversely, in striving to adopt a more scientific approach and include the full range of uncertainty, we often give sceptics an easy route to undermine the science. All too often uncertainty in science offers a convenient excuse for delaying important decisions. However, in the case of climate change there is overwhelming evidence that the climate is changing — in part due to human activities — and that changes will accelerate if emissions continue unabated. In examining the uncertainty in the science we must take care to not throw away what we do know. Science has established that climate is changing. **Scientists** now **need to press on in developing the emerging tools that will be used to underpin sensible adaptation decisions which will determine our future.**

#### Warming is a threat magnifier, makes all impacts inevitable

**Pascual and Elkind 2010** (Carlos [US Ambassador to Mexico, Served as VP of foreign policy @ Brookings]; Jonathan [principal dep ass sec for policy and int energy @ DOE]; Energy Security; p 5; kdf)

Climate change is arguably the greatest challenge facing the human race.¶ It poses profound risks to the natural systems that sustain life on Earth and¶ consequently creates great challenges for human lives, national economies,¶ nations' security, and international governance. New scientific reports¶ emerging from one year to the next detail ever more alarming potential¶ impacts and risks.¶ It is increasingly common for analysts and policymakers to refer to¶ climate change as a threat multiplier, a destructive force that will exacerbate¶ existing social, environmental, economic, and humanitarian stresses.¶ The warming climate is predicted to bring about prolonged droughts¶ in already dry regions, flooding along coasts and even inland rivers, an¶ overall increase in severe weather events, rising seas, and the spread of¶ disease, to cite just a few examples. Such impacts may spark conflict in¶ weak states, lead to the displacement of millions of people, create environmental¶ refugees, and intensify competition over increasingly scarce¶ resources.¶ One of the great challenges of climate change is, indeed, the scope of¶ the phenomenon. The ongoing warming of the globe results chiefly from¶ one of the most ubiquitous of human practices, the conversion of fossil fuels¶ into energy through simple combustion. Halting and reversing climate¶ change, however, will require both unproven-perhaps even unimaginedtechnology¶ and sustained political commitment. We must change living¶ habits in all corners of the globe over the course of the next several decades.¶ We must resist the impulse to leave the problem for those who follow us¶ or to relax our efforts if we achieve a few years of promising progress. The¶ profound challenge will lie in the need for successive rounds of sustained¶ policymaking, successive waves of technological innovation, and ongoing¶ evolution of the ways in which we live our lives.

### Impact: Internet good – Extinction (Eagleman)

#### A free internet is vital to combating every existential threat

**Eagleman, 10** - American neuroscientist and writer at Baylor College of Medicine, where he directs the Laboratory for Perception and Action and the Initiative on Neuroscience and Law (David, “Six ways the internet will save civilization” Wired, 9/10, <http://www.wired.co.uk/magazine/archive/2010/12/start/apocalypse-no>

Many great civilisations have fallen, leaving nothing but cracked ruins and scattered genetics. Usually this results from: natural disasters, resource depletion, economic meltdown, disease, poor information flow and corruption. But we’re luckier than our predecessors because we command a technology that no one else possessed: a rapid communication network that finds its highest expression in the internet. I propose that there are six ways in which the net has vastly reduced the threat of societal collapse. Epidemics can be deflected by telepresence One of our more dire prospects for collapse is an infectious-disease epidemic. Viral and bacterial epidemics precipitated the fall of the Golden Age of Athens, the Roman Empire and most of the empires of the Native Americans. The internet can be our key to survival because the ability to work telepresently can inhibit microbial transmission by reducing human-to-human contact. In the face of an otherwise devastating epidemic, businesses can keep supply chains running with the maximum number of employees working from home. This can reduce host density below the tipping point required for an epidemic. If we are well prepared when an epidemic arrives, we can fluidly shift into a self-quarantined society in which microbes fail due to host scarcity. Whatever the social ills of isolation, they are worse for the microbes than for us. The internet will predict natural disasters We are witnessing the downfall of slow central control in the media: news stories are increasingly becoming user-generated nets of up-to-the-minute information. During the recent California wildfires, locals went to the TV stations to learn whether their neighbourhoods were in danger. But the news stations appeared most concerned with the fate of celebrity mansions, so Californians changed their tack: they uploaded geotagged mobile-phone pictures, updated Facebook statuses and tweeted. The balance tipped: the internet carried news about the fire more quickly and accurately than any news station could. In this grass-roots, decentralised scheme, there were embedded reporters on every block, and the news shockwave kept ahead of the fire. This head start could provide the extra hours that save us. If the Pompeiians had had the internet in 79AD, they could have easily marched 10km to safety, well ahead of the pyroclastic flow from Mount Vesuvius. If the Indian Ocean had the Pacific’s networked tsunami-warning system, South-East Asia would look quite different today. Discoveries are retained and shared Historically, critical information has required constant rediscovery. Collections of learning -- from the library at Alexandria to the entire Minoan civilisation -- have fallen to the bonfires of invaders or the wrecking ball of natural disaster. Knowledge is hard won but easily lost. And information that survives often does not spread. Consider smallpox inoculation: this was under way in India, China and Africa centuries before it made its way to Europe. By the time the idea reached North America, native civilisations who needed it had already collapsed. The net solved the problem. New discoveries catch on immediately; information spreads widely. In this way, societies can optimally ratchet up, using the latest bricks of knowledge in their fortification against risk. Tyranny is mitigated Censorship of ideas was a familiar spectre in the last century, with state-approved news outlets ruling the press, airwaves and copying machines in the USSR, Romania, Cuba, China, Iraq and elsewhere. In many cases, such as Lysenko’s agricultural despotism in the USSR, it directly contributed to the collapse of the nation. Historically, a more successful strategy has been to confront free speech with free speech -- and the internet allows this in a natural way. It democratises the flow of information by offering access to the newspapers of the world, the photographers of every nation, the bloggers of every political stripe. Some posts are full of doctoring and dishonesty whereas others strive for independence and impartiality -- but all are available to us to sift through. Given the attempts by some governments to build firewalls, it’s clear that this benefit of the net requires constant vigilance. Human capital is vastly increased Crowdsourcing brings people together to solve problems. Yet far fewer than one per cent of the world’s population is involved. We need expand human capital. Most of the world not have access to the education afforded a small minority. For every Albert Einstein, Yo-Yo Ma or Barack Obama who has educational opportunities, uncountable others do not. This squandering of talent translates into reduced economic output and a smaller pool of problem solvers. The net opens the gates education to anyone with a computer. A motivated teen anywhere on the planet can walk through the world’s knowledge -- from the webs of Wikipedia to the curriculum of MIT’s OpenCourseWare. The new human capital will serve us well when we confront existential threats we’ve never imagined before. Energy expenditure is reduced Societal collapse can often be understood in terms of an energy budget: when energy spend outweighs energy return, collapse ensues. This has taken the form of deforestation or soil erosion; currently, the worry involves fossil-fuel depletion. The internet addresses the energy problem with a natural ease. Consider the massive energy savings inherent in the shift from paper to electrons -- as seen in the transition from the post to email. Ecommerce reduces the need to drive long distances to purchase products. Delivery trucks are more eco-friendly than individuals driving around, not least because of tight packaging and optimisation algorithms for driving routes. Of course, there are energy costs to the banks of computers that underpin the internet -- but these costs are less than the wood, coal and oil that would be expended for the same quantity of information flow. The tangle of events that triggers societal collapse can be complex, and there are several threats the net does not address. But vast, networked communication can be an antidote to several of the most deadly diseases threatening civilisation. The next time your coworker laments internet addiction, the banality of tweeting or the decline of face-to-face conversation, you may want to suggest that the net may just be the technology that saves us.

####

# Affirmative

### Reform Solves

#### Reform will snowball

Patel 6/25/2015 (Faiza [co-director of the Brennan Center’s Liberty and National Security Program]; When will surveillance reform stop being just 'cool'?; www.brennancenter.org/blog/when-will-surveillance-reform-stop-being-just-‘cool’; kdf)

Last week, former National Security Agency Director Michael Hayden declared that he was “cool” with the recently enacted USA Freedom Act, which reined in government bulk collection of Americans’ phone records. His characterization of that program as “little” is no doubt accurate. Information from the archive of documents released by NSA whistleblower Edward Snowden has revealed many other programs that pose equal or greater risks to Americans’ privacy. But Hayden is too quick to assume that the phone records program will be the only reform. The passage of the USA Freedom Act is the first curtailment of intelligence authorities since the 9/11 attacks and should mark the beginning — not the end — of reform. It’s no surprise that Congress chose to tackle the phone record program first. It is relatively straightforward for people to understand, and its goal of amassing a vast database of information about Americans is patently difficult to square with our constitutional values. Two review boards found it to be of minimal counterterrorism value, and a federal appeals court declared it illegal. Even the intelligence community and the president were amenable to reform. But Congress is well aware that this reform is insufficient. Many of the votes against the act in the House and Senate came from lawmakers who believe it didn’t go far enough.

### Surveillance Bad

#### Government surveillance is unique and invites tyranny

Robertson 2015 (James [served on the FISC from 2002 to 2005, resigning the day after warrantless wiretaps were exposed]; Forward of What went wrong with the FISA court; https://www.brennancenter.org/sites/default/files/analysis/What\_Went\_%20Wrong\_With\_The\_FISA\_Court.pdf; kdf)

Many people are surprised to learn that there is no “right to privacy” in the Constitution. Privacy is more of a cultural construct than a legal one in this country, and we are aiding and abetting its steady erosion with our dependence on the Internet, our credit cards and smartphones, our flirtation with social media, and our capitulation to commercial exploitation of Big Data. In a sense, we are all under surveillance, all the time — our whereabouts, activities, and transactions reduced to metadata and available to anyone who can break the code — and we have brought it upon ourselves. Surveillance by the government, however, is another matter. Distrust or at least wariness of a government that collects data about us lies deep in the amygdala of our civic consciousness. This administration may be operating lawfully and with full regard to our rights and privileges, but what about that one? Have we been reading too many novels, or is there a real threat of tyranny? Here, of course, is where the Constitution comes in, with the Fourth Amendment’s guarantee of “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” I have no criticism of the FISA Court. I know and deeply respect every one of its presiding judges for the last 30 years, and I am well acquainted with many of the other FISA judges who have served. They are, every one of them, careful and scrupulous custodians of the extraordinary and sensitive power entrusted to them. The staff that supports the FISA Court, the Justice Department lawyers who appear before the FISA Court, and the FBI, CIA and NSA personnel who present applications to the FISA Court are superb, dedicated professionals. What I do criticize is the mission creep of the statute all of those people are implementing.

### No Circumvention

#### Circumvention won’t happen if surveillance is prohibited

Ackerman, 15 --- American national security reporter and blogger, national security editor for the Guardian (6/1/2015, Spencer, The Guardian, “Fears NSA will seek to undermine surveillance reform; Privacy advocates are wary of covert legal acrobatics from the NSA similar to those deployed post-9/11 to circumvent congressional authority,” Lexis, JMP)

Despite that recent history, veteran intelligence attorneys reacted with scorn to the idea that NSA lawyers will undermine surveillance reform. Robert Litt, the senior lawyer for director of national intelligence, James Clapper, said during a public appearance last month that creating a banned bulk surveillance program was " not going to happen ".

"The whole notion that NSA is just evilly determined to read the law in a fashion contrary to its intent is bullshit, of the sort that the Guardian and the left - but I repeat myself - have fallen in love with. The interpretation of 215 that supported the bulk collection program was creative but not beyond reason, and it was upheld by many judges," said the former NSA general counsel Stewart Baker, referring to Section 215 of the Patriot Act.

This is the section that permits US law enforcement and surveillance agencies to collect business records and expired at midnight, almost two years after the whistleblower Edward Snowden revealed to the Guardian that the Patriot Act was secretly being used to justify the collection of phone records from millions of Americans.

With one exception, the judges that upheld the interpretation sat on the non-adversarial Fisa court, a body that approves nearly all government surveillance requests and modifies about a quarter of them substantially. The exception was reversed by the second circuit court of appeals.

Baker, speaking before the Senate voted, predicted: "I don't think anyone at NSA is going to invest in looking for ways to defy congressional intent if USA Freedom is adopted."

### AT: Internet Freedom Impacts

#### Zero chance of solving internet freedom

Morozov 15 [Evgeny Morozov, Who’s the true enemy of internet freedom - China, Russia, or the US?, The Guardian, http://www.theguardian.com/commentisfree/2015/jan/04/internet-freedom-china-russia-us-google-microsoft-digital-sovereignty]

Given that Russia and China are not known for their commitment to freedoms of expression and assembly, it is tempting to view their quest for information sovereignty as yet another stab at censorship and control. In fact, even when the far more benign government of Brazil toyed with the idea of forcing American companies to store user data locally – an idea it eventually abandoned – it was widely accused of draconian overreach. However, Russia, China and Brazil are simply responding to the extremely aggressive tactics adopted by none other than the US. In typical fashion, though, America is completely oblivious to its own actions, believing that there is such a thing as a neutral, cosmopolitan internet and that any efforts to move away from it would result in its “Balkanisation”. But for many countries, this is not Balkanisation at all, merely de-Americanisation. US companies have been playing an ambiguous role in this project. On the one hand, they build efficient and highly functional infrastructure that locks in other countries, creating long-term dependencies that are very messy and costly to undo. They are the true vehicles for whatever is left of America’s global modernisation agenda. On the other hand, the companies cannot be seen as mere proxies for the American empire. Especially after the Edward Snowden revelations clearly demonstrated the cosy alliances between America’s business and state interests, these companies need to constantly assert their independence – occasionally by taking their own government to court – even if, in reality, most of their interests perfectly align with those of Washington. This explains why Silicon Valley has been so vocal in demanding that the Obama administration do something about internet privacy and surveillance: if internet companies were seen as compromised parties here, their business would collapse. Just look at the misfortunes of Verizon in 2014: uncertain of the extent of data-sharing between Verizon and the NSA, the German government ditched its contract with the US company in favour of Deutsche Telekom. A German government spokesman said at the time: “The federal government wants to win back more technological sovereignty, and therefore prefers to work with German companies.” However, to grasp the full extent of America’s hypocrisy on the issue of information sovereignty, one needs to look no further than the ongoing squabble between Microsoft and the US government. It concerns some email content – relevant to an investigation – stored on Microsoft’s servers in Ireland. American prosecutors insist that they can obtain such content from Microsoft simply by serving it a warrant – as if it makes no difference that the email is stored in a foreign country. In order to obtain it, Washington would normally need to go through a complex legal process involving bilateral treaties between the governments involved. But now it wants to sidestep that completely and treat the handling of such data as a purely local issue with no international implications. The data resides in cyberspace – and cyberspace knows no borders! The government’s reasoning here is that the storage issue is irrelevant; what is relevant is where the content is accessed – and it can be accessed by Microsoft’s employees in the US. Microsoft and other tech giants are now fighting the US government in courts, with little success so far, while the Irish government and a handful of European politicians are backing Microsoft. In short, the US government insists that it should have access to data regardless of where it is stored as long as it is handled by US companies. Just imagine the outcry if the Chinese government were to demand access to any data that passes through devices manufactured by Chinese companies – Xiaomi, say, or Lenovo – regardless of whether their users are in London or New York or Tokyo. Note the crucial difference: Russia and China want to be able to access data generated by their citizens on their own soil, whereas the US wants to access data generated by anybody anywhere as long as American companies handle it. In opposing the efforts of other countries to reclaim a modicum of technological sovereignty, Washington is likely to run into a problem it has already encountered while promoting its nebulous “internet freedom” agenda: its actions speak louder than its words. Rhetorically, it is very hard to oppose government-run digital surveillance and online spin in Russia, China or Iran, when the US government probably does more of it than all of these countries combined. Whatever motivates the desire of Russia and China to exert more control over their digital properties – and only the naive would believe that they are not motivated by concerns over domestic unrest – their actions are proportional to the aggressive efforts of Washington to exploit the fact that so much of the world’s communications infrastructure is run by Silicon Valley. One’s man internet freedom is another man’s internet imperial.

#### Squo solves—net neutrality

Garside March 3, 2015 (Juliette; Net neutrality is like free speech – and the internet needs rules, says FCC boss; www.theguardian.com/technology/2015/mar/03/net-neutrality-free-speech-fcc-tom-wheeler; kdf)

The US’s top media regulator hit back at critics of new net neutrality rules voted into law last week, comparing them to the first amendment and saying neither government nor private companies had the right to restrict the openness of the internet. The Federal Communications Commission chairman, Tom Wheeler, was speaking in Barcelona at Mobile World Congress, the world’s largest telecoms trade show, just as European governments are meeting to thrash out their own principles for keeping the internet open. “This is no more regulating the internet than the first amendment regulates free speech in our country,” Wheeler said. “If the internet is the most powerful and pervasive platform in the history of the planet, can it exist without a referee? There needs to be a referee with a yardstick, and that is the structure we have put in place. A set of rules that say activity should be just and reasonable, and somebody who can raise the flag if they aren’t.” Telecoms companies across Europe and America have railed against Wheeler’s reforms, saying they will discourage investment in better cable and wireless networks and simply benefit bandwidth-hungry services like Netflix and YouTube, which do not normally pay for their content to be carried across the internet. In the US, Verizon and AT&T, the two largest mobile operators, have said they will try to reverse the new rules in the courts. Meanwhile, Wheeler told conference attendees in Barcelona: “Those who were opposed to the open internet rules like to say this is Depression-era monopoly regulation. We built our model for net neutrality on the regulatory model that has been wildly successful in the US for mobile.” The FCC rules will treat telecoms companies in a similar way to utilities such as electricity. Internet service providers will be explicitly prohibited from blocking, throttling or prioritising internet traffic for commercial reasons. Where complaints are raised, the FCC will decide on a case-by-case basis whether what network owners are doing is “fair and just”. The FCC has said it would not intervene areas such as pricing, network unbundling and technical operating requirements. The European parliament is in the midst of negotiations with member states and network operators over final net neutrality rules, which could be published later this spring. A source at one of Europe’s largest mobile carriers said the fear was that Europe would introduce similar rules, only to find itself out of step when the FCC is forced to back down by a legal challenge or a change of president.

#### Internet not key to growth

Lowrey 2011 (Annie; Freaks, geeks, and the GDP; Mar 8; www.slate.com/articles/business/moneybox/2011/03/freaks\_geeks\_and\_gdp.html; kdf)

If you have attended any economists' cocktail parties in the past month or so—lucky you!—then you have probably heard chatter about Tyler Cowen's e-book, The Great Stagnation. The book seeks to explain why in the United States median wages have grown only slowly since the 1970s and have actually declined in the past decade. Cowen points to an innovation problem: Through the 1970s, the country had plenty of "low-hanging fruit" to juice GDP growth. In the past 40 years, coming up with whiz-bang, life-changing innovations—penicillin, free universal kindergarten, toilets, planes, cars—has proved harder, pulling down growth rates across the industrialized world. But wait! you might say. In the 1970s, American businesses started pumping out amazing, life-changing computing technologies. We got graphing calculators, data-processing systems, modern finance, GPS, silicon chips, ATMs, cell phones, and a host of other innovations. Has the Internet, the most revolutionary communications technology advance since Gutenberg rolled out the printing press, done nothing for GDP growth? The answer, economists broadly agree, is: Sorry, but no—at least, not nearly as much as you would expect. A quarter century ago, with new technologies starting to saturate American homes and businesses, economists looked around and expected to find computer-fueled growth everywhere. But signs of increased productivity or bolstered growth were few and far between. Sure, computers and the Web transformed thousands of businesses and hundreds of industries. But overall, things looked much the same. The GDP growth rate did not tick up significantly, nor did productivity. As economist Robert Solow put it in 1987: "You can see the computer age everywhere but in the productivity statistics." An overlapping set of theories emerged to explain the phenomenon, often termed the "productivity paradox." Perhaps the new technologies advantaged some firms and industries and disadvantaged others, leaving little net gain. Perhaps computer systems were not yet easy enough to use to reduce the amount of effort workers need to exert to perform a given task. Economists also wondered whether it might just take some time—perhaps a lot of time—for the gains to show up. In the past, information technologies tended to need to incubate before they produced gains in economic growth. Consider the case of Gutenberg's printing press. Though the technology radically transformed how people recorded and transmitted news and information, economists have failed to find evidence it sped up per-capita income or GDP growth in the 15th and 16th centuries. At one point, some economists thought that an Internet-driven golden age might have finally arrived in the late 1990s. Between 1995 and 1999, productivity growth rates actually exceeded those during the boom from 1913 to 1972—perhaps meaning the Web and computing had finally brought about a "New Economy." But that high-growth period faded quickly. And some studies found the gains during those years were not as impressive or widespread as initially thought. Robert Gordon, a professor of economics at Northwestern, for instance, has found that computers and the Internet mostly helped boost productivity in durable goods manufacturing—that is, the production of things like computers and semiconductors. "Our central theme is that computers and the Internet do not measure up to the Great Inventions of the late nineteenth and early twentieth century, and in this do not merit the label of Industrial Revolution," he wrote. Gordon's work leads to another theory, one espoused by Cowen himself. Perhaps the Internet is just not as revolutionary as we think it is. Sure, people might derive endless pleasure from it—its tendency to improve people's quality of life is undeniable. And sure, it might have revolutionized how we find, buy, and sell goods and services. But that still does not necessarily mean it is as transformative of an economy as, say, railroads were. That is in part because the Internet and computers tend to push costs toward zero, and have the capacity to reduce the need for labor. You are, of course, currently reading this article for free on a Web site supported not by subscriptions, but by advertising. You probably read a lot of news articles online, every day, and you probably pay nothing for them. Because of the decline in subscriptions, increased competition for advertising dollars, and other Web-driven dynamics, journalism profits and employment have dwindled in the past decade. (That Cowen writes a freely distributed blog and published his ideas in a $4 e-book rather than a $25 glossy airport hardcover should not go unnoted here.) Moreover, the Web- and computer-dependent technology sector itself does not employ that many people. And it does not look set to add workers: The Bureau of Labor Statistics estimates that employment in information technology, for instance, will be lower in 2018 than it was in 1998. That the Internet has not produced an economic boom might be hard to believe, Cowen admits. "We have a collective historical memory that technological progress brings a big and predictable stream of revenue growth across most of the economy," he writes. "When it comes to the web, those assumptions are turning out to be wrong or misleading. The revenue-intensive sectors of our economy have been slowing down and the big technological gains are coming in revenue-deficient sectors." But revenue is not always the end-all, be-all—even in economics. That brings us to a final explanation: Maybe it is not the growth that is deficient. Maybe it is the yardstick that is deficient. MIT professor Erik Brynjolfsson \* explains the idea using the example of the music industry. "Because you and I stopped buying CDs, the music industry has shrunk, according to revenues and GDP. But we're not listening to less music. There's more music consumed than before." The improved choice and variety and availability of music must be worth something to us—even if it is not easy to put into numbers. "On paper, the way GDP is calculated, the music industry is disappearing, but in reality it's not disappearing. It is disappearing in revenue. It is not disappearing in terms of what you should care about, which is music." As more of our lives are lived online, he wonders whether this might become a bigger problem. "If everybody focuses on the part of the economy that produces dollars, they would be increasingly missing what people actually consume and enjoy. The disconnect becomes bigger and bigger." But providing an alternative measure of what we produce or consume based on the value people derive from Wikipedia or Pandora proves an extraordinary challenge—indeed, no economist has ever really done it. Brynjolfsson says it is possible, perhaps, by adding up various "consumer surpluses," measures of how much consumers would be willing to pay for a given good or service, versus how much they do pay. (You might pony up $10 for a CD, but why would you if it is free?) That might give a rough sense of the dollar value of what the Internet tends to provide for nothing—and give us an alternative sense of the value of our technologies to us, if not their ability to produce growth or revenue for us. Of course, if our most radical and life-altering technologies are not improving incomes or productivity or growth, then we still have problems. Quality-of-life improvements do not put dinner on the table or pay for Social Security benefits. Still, even Cowen does not see all doom and gloom ahead, with incomes stagnating endlessly as we do more and more online and bleed more and more jobs and money. Who knows what awesome technologies might be just around the bend?