# Explanation/Guide

### File Description and General Tips

This file contains the Secure Data Act affirmative. It includes three advantages and comprehensive backline evidence. When reading this affirmative, students can choose to read the Constitutional Privacy Advantage, the Tech Leadership Advantage, and/or the Cybersecurity Advantage. The negative’s case materials are located in the Secure Data Act negative file.

In response to negative case arguments, the affirmative can draw from the backline evidence in this file. For each case argument, the affirmative is provided with three cards in response. Due to time constraints, students should carefully choose which (if any) extension evidence to read in the 2AC. Instead of reading new cards to respond to each 1NC case argument, students are encouraged to write 2AC blocks that make analytical arguments drawing upon the relevant 1AC evidence. When necessary, these blocks should include evidence from the backline materials.

In response to negative off-case arguments, the affirmative can draw from the evidence in the relevant files. This file contains *only* case arguments.

### Explanation of the Plan

The plan prohibits federal intelligence agencies like NSA from requiring or compelling private companies to design or alter their commercial products for the purpose of facilitating domestic surveillance. In other words, it prevents agencies from working with companies to insert backdoors into commercial products or services. This is the major provision of the Secure Data Act, a legislative proposal that aims to protect the integrity of encryption tools. It is a response to revelations about NSA programs like BULLRUN and Sentry Raven and reports that NSA secretly paid RSA—a security company—to insert a backdoor in its industry-standard encryption products.

### Explanation of the Constitutional Privacy Advantage

The affirmative argues that government attempts to undermine encryption are unconstitutional because they violate First and Fourth Amendment rights to privacy. They argue that privacy is the foundation of freedom and that mass surveillance is inherently repressive because it stifles dissent and freedom of thought. The affirmative contends that violations of constitutional privacy rights should never be tolerated regardless of consequences because the Constitution establishes a series of collective pre-commitments. Constitutional rights can never be “balanced away” — even in the face of security threats — or they are emptied of their value as constraints on government action.

### Explanation of the Tech Leadership Advantage

The affirmative argues that NSA surveillance is undermining the global competitiveness of the U.S. tech industry because it is undermining international trust in American companies like Google, Apple, Microsoft, and Cisco. These companies are losing billions of dollars in revenue as their global market share shrinks. America’s overall tech leadership depends on the strength of these companies because they form the industrial base that produces innovative products and services upon which our national security depends. Without tech leadership, America will be unable to maintain its hegemony. The affirmative argues that this loss of leadership will create a dangerous power vacuum that exacerbates security threats and risks conflict.

### Explanation of the Cybersecurity Advantage

The affirmative argues that government attempts to undermine encryption tools jeopardizes global cybersecurity. When backdoors are inserted into encryption systems, they become vulnerable to exploitation by hackers, foreign intelligence agencies, and criminals. The affirmative contends that strong encryption is vital to prevent widespread cyber attacks like the ones the U.S. has recently suffered (OPM, Target, Sony, etc.). These attacks will only get worse and more frequent without strong encryption, threatening the electric grid and U.S. military installations. The affirmative argues that this kind of cyber attack would have devastating consequences and could even escalate to nuclear war.

## 1AC

### 1AC — Constitutional Privacy Advantage

#### Contention One: Constitutional Privacy

#### First, U.S. government attacks on encryption are an unconstitutional violation of privacy. Encryption is a basic human right.

Mukunth 15 — Vasudevan Mukunth, Science Editor at *The Wire*—a public interest news publication, holds a degree in Mechanical Engineering from the Birla Institute of Technology and Science a post-graduate degree from the Asian College of Journalism, 2015 (“A Call For a New Human Right, the Right to Encryption,” *The Wire*, June 2nd, Available Online at <http://thewire.in/2015/06/02/a-call-for-a-new-human-right-the-right-to-encryption/>, Accessed 06-24-2015)

DUAL\_EC\_DRBG is the name of a program that played an important role in the National Security Agency’s infiltration of communication protocols, which was revealed by whistleblower Edward Snowden. The program, at the time, drew the suspicion of many cryptographers who wondered why it was being used instead of the NIST’s more advanced standards. The answer arrived in December 2013: DUAL\_EC\_DRBG was a backdoor.

A backdoor is a vulnerability deliberately inserted into a piece of software to allow specific parties to decrypt it whenever they want to. When the NSA wasn’t forcibly getting companies to hand over private data, it was exploiting pre-inserted backdoors to enter and snoop around. Following 9/11, the Patriot Act made such acts lawful, validating the use of programs like DUAL\_EC\_DRBG that put user security and privacy at stake to defend the more arbitrarily defined questions of national security.

However, the use of such weakened encryption standards is a Trojan horse that lets in the weaknesses of those standards as well. When engineers attempt to use those standards for something so well-defined as the public interest, such weaknesses can undermine that definition. For example, one argument after Snowden’s revelations was to encrypt communications such that only the government could access them. This was quickly dismissed because it’s open knowledge among engineers that there are no safeguards that can be placed around such ‘special’ access that would deter anyone skilled enough to hack through it.

It’s against this ‘power draws power’ scenario that a new report from the UN Office of the High Commissioner for Human Rights (OHCHR) makes a strong case – one which the influential Electronic Frontier Foundation has called “groundbreaking”. It says, “requiring encryption back-door access, even if for legitimate purposes, threatens the privacy necessary to the unencumbered exercise of the right to freedom of expression.” Some may think this verges on needless doubt, but the report’s centre of mass rests on backdoors’ abilities to compromise individual identities in legal and technological environments that can’t fully protect those identities.

On June 1, those provisions of the Patriot Act that justified the interception of telephone calls expired and the US Senate was unable to keep them going. As Anuj Srivas argues, it is at best “mild reform” that has only plucked at the low-hanging fruit – reform that rested on individuals’ privacy being violated by unconstitutional means. The provisions will be succeeded by the USA Freedom Act, which sports some watered-down notions of accountability when organisations like the NSA trawl data.

According to the OHCHR report, however, what we really need are proactive measures. If decryption is at the heart of privacy violations, then strong encryption needs to be at the heart of privacy protection – i.e. encryption must be a human right. Axiomatically, as the report’s author, Special Rapporteur David Kaye writes, individuals rely on encryption and anonymity to “safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression.” On the same note, countries like the US that intentionally compromise products’ security, and the UK and India which constantly ask for companies to hand over the keys to their data to surveil their citizens, are now human rights violators.

By securing the importance of strong encryption and associating it with securing one’s identity, the hope is to insulate it from fallacies in the regulation of decryption – such as in the forms of the Patriot Act and the Freedom Act. Kaye argues, “Privacy interferences that limit the exercise of the freedoms of opinion and expression … must not in any event interfere with the right to hold opinions, and those that limit the freedom of expression must be provided by law and be necessary and proportionate to achieve one of a handful of legitimate objectives.”

This anastomosis in the debate can be better viewed as a wedge that was created around 1995. The FBI Director at the time, Louis Freeh, had said that the bureau was “in favor of strong encryption, robust encryption. The country needs it, industry needs it. We just want to make sure we have a trap door and key under some judge’s authority where we can get there if somebody is planning a crime.”

Then, in October 2014, then FBI Director James Comey made a similar statement: “It makes more sense to address any security risks by developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact.” In the intervening decades, however, awareness of the vulnerabilities of partial encryption has increased while the law has done little to provide recourse for the gaps in online protection. So, Comey’s arguments are more subversive than Freeh’s.

Kaye’s thesis is from a human rights perspective, but its conclusions apply to everyone – to journalists, lawyers, artists, scholars, anyone engaged in the exploration of controversial information and with a stake in securing their freedom of expression. In fact, a corollary of his thesis is that strong encryption will ensure unfettered access to the Internet. His report also urges Congress to pass the Secure Data Act, which would prevent the US government from forcibly inserting backdoors in software to suit its needs.

#### Second, constitutional privacy protections are the foundation of freedom. Mass surveillance is inherently repressive because it exposes individuals to inescapable, oppressive scrutiny.

Greenwald 14 — Glenn Greenwald, journalist who received the 2014 Pulitzer Prize for Public Service for his work with Edward Snowden to report on NSA surveillance, Founding Editor of *The Intercept*, former Columnist for the *Guardian* and *Salon*, recipient of the Park Center I.F. Stone Award for Independent Journalism, the Online Journalism Award for investigative work on the abusive detention conditions of Chelsea Manning, the George Polk Award for National Security Reporting, the Gannett Foundation Award for investigative journalism, the Gannett Foundation Watchdog Journalism Award, the Esso Premio for Excellence in Investigative Reporting in Brazil, and the Electronic Frontier Foundation’s Pioneer Award, holds a J.D. from New York University School of Law, 2014 (“The Harm of Surveillance,” *No Place To Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Published by Metropolitan Books, ISBN 9781627790734, p. 173-174)

Privacy is essential to human freedom and happiness for reasons that are rarely discussed but instinctively understood by most people, as evidenced by the lengths to which they go to protect their own. To begin with, people radically change their behavior when they know they are being watched. They will strive to do that which is expected of them. They want to avoid shame and condemnation. They do so by adhering tightly to accepted social practices, by staying within imposed boundaries, avoiding action that might be seen as deviant or abnormal.

The range of choices people consider when they believe that others are watching is therefore far more limited than what they might do when acting in a private realm. A denial of privacy operates to severely restrict one’s freedom of choice.

Several years ago, I attended the bat mitzvah of my best friend’s daughter. During the ceremony, the rabbi emphasized that “the central lesson” for the girl to learn was that she was “always being watched and judged.” He told her that God always knew what she was doing, every choice, every action, and even every thought, no matter how private. “You are never alone,” he said, which meant that she should always adhere to God’s will.

The rabbi’s point was clear: if you can never evade the watchful eyes of a supreme authority, there is no choice but to follow the dictates that authority imposes. You cannot even consider forging your own path beyond those rules: if you believe you are always being watched and judged, you are not really a free individual.

All oppressive authorities — political, religious, societal, parental — rely on this vital truth, using it as a principal tool to enforce orthodoxies, compel adherence, and quash dissent. It is in their interest to convey that nothing their subjects do will escape the knowledge of the authorities. Far more effectively than a police force, the deprivation of privacy will crush any temptation to deviate from rules and norms.

What is lost when the private realm is abolished are many of the [end page 173] attributes typically associated with quality of life. Most people have experienced how privacy enables liberation from constraint. And we’ve all, conversely, had the experience of engaging in private behavior when we thought we were alone — dancing, confessing, exploring sexual expression, sharing untested ideas — only to feel shame at having been seen by others.

Only when we believe that nobody else is watching us do we feel free — safe — to truly experiment, to test boundaries, to explore new ways of thinking and being, to explore what it means to be ourselves. What made the Internet so appealing was precisely that it afforded the ability to speak and act anonymously, which is so vital to individual exploration.

For that reason, it is in the realm of privacy where creativity, dissent, and challenges to orthodoxy germinate. A society in which everyone knows they can be watched by the state — where the private realm is effectively eliminated — is one in which those attributes are lost, at both the societal and the individual level.

Mass surveillance by the state is therefore inherently repressive, even in the unlikely case that it is not abused by vindictive officials to do things like gain private information about political opponents. Regardless of how surveillance is used or abused, the limits it imposes on freedom are intrinsic to its existence.

#### Third, constitutional safeguards against warrantless surveillance must be maintained *regardless of consequences*. “Weighing” privacy against security *nullifies* the Fourth Amendment.

Cole 6 — David Cole, Professor at Georgetown University Law Center, has litigated many significant constitutional cases in the Supreme Court, holds a J.D. from Yale Law School, 2007 (“How to Skip the Constitution,” *New York Review of Books*, November 16th, Available Online at <http://www.nybooks.com/articles/archives/2006/nov/16/how-to-skip-the-constitution/>, Accessed 06-28-2015)

Judge Posner is not troubled by any of these measures, at least as a constitutional matter. His theory of the Constitution is at once candid and cavalier. Rejecting popular conservative attacks on “judicial activism,” he argues that in view of the open-ended character of many of the document’s most important terms—“reasonable” searches and seizures, “due process of law,” “equal protection,” and even “liberty” itself—it is not objectionable but inevitable that constitutional law is made by judges. He dismisses the constitutional theories of textualism and originalism favored by many conservative judges and scholars as canards, arguing that neither the Constitution’s text nor the history of its framing gives much guidance in dealing with most of the hard questions of the day. Constitutional law, he maintains, “is intended to be a loose garment; if it binds too tightly, it will not be adaptable to changing circumstances.”

But Posner then goes on to treat the Constitution as essentially a license to open-ended “balancing” of interests by the political branches and the courts. His thinking is informed largely by an economist’s predilection for cost-benefit analysis and a philosophical enthusiasm for pragmatism. Posner’s reputation as a scholar rests not on his contributions to constitutional theory, but on his role as one of the founding fathers of the movement that applied economic analysis to law. His new book might just as well have been called “An Economist Looks at the Constitution.” In the end, constitutional interpretation for Posner is little more than a balancing act, and when the costs of a catastrophic terrorist attack are placed on the scale, he almost always feels they outweigh concerns about individual rights and liberties.

Consider, for example, his views on electronic surveillance. The Bush administration currently faces several dozen lawsuits challenging various aspects of its NSA spying program, which, according to the administration, involves the warrantless wiretapping of international phone calls and e-mails where one of the participants is thought to be connected with al-Qaeda or affiliated groups. That program, as I and many other constitutional scholars have argued, violates a provision in the Foreign Intelligence Surveillance Act (FISA) specifying that it is a crime for officials not to seek a warrant from the appropriate court before engaging in such wiretapping.1 The Bush administration seeks to justify this violation of law by invoking an inherent presidential power to ignore congressional legislation, echoing President Richard Nixon’s defense of his own decision to authorize warrantless wiretapping during the Vietnam War: “When the president does it, that means that it is not illegal.” Posner not only sees nothing wrong with the NSA program; he would also find constitutional a far more sweeping measure that subjected every phone call and e-mail in the nation, domestic as well as international, to initial computer screening for patterns of suspicious words, and then permitted intelligence agents to follow up on all communications that the computer treated as suspicious.

How does Posner reach the conclusion that the Constitution would permit such an Orwellian scheme, far more invasive than the Bush administration, if it is to be believed, has been willing to undertake so far? In a word, balancing. In Posner’s view, the costs to personal liberty of such a program are minimal, and are outweighed by the benefits to our security. Having a computer analyze one’s phone calls is no big deal, he claims, as long as we know it’s only looking for terrorists. He admits that there might be a danger of misuse of the information by the agents who follow up on the computer’s “suspects,” but he considers that risk minimal because he is confident that any such abuse would likely come to light and be widely criticized. (He fails to acknowledge that whistleblowing would be far less likely if he had his way and an Official Secrets Act were passed making it a crime to publish leaked government secrets.) As for the benefits of such surveillance, Posner surmises that such a program might sweep up sufficient data to permit intelligence agents to “connect the dots” and prevent a catastrophic attack. Even if it didn’t, he writes, it would at least have the salutary effect of discouraging terrorists from communicating by telephone and e-mail.

Every aspect of Posner’s analysis is open to question. He ignores that privacy is essential to political freedom: if everyone knows that their every electronic communication is subject to government monitoring, even by a computer, it would likely have a substantial chilling effect on communications that the government might conceivably find objectionable, not just terrorist planning, and not just criminal conduct. Moreover, Posner ignores the myriad ways in which the government can harass people without its ill intent ever coming to light. For example, the government can selectively prosecute minor infractions of the law, launch arbitrary tax investigations, and engage in blackmail, all methods perfected by FBI Director J. Edgar Hoover. Contrary to Posner’s claims, one cannot, as the FBI’s abuses showed, trust public scrutiny to forestall such tactics, even in the absence of an Official Secrets Act. Finally, it is far from clear that such a program would be effective—the sheer volume of “dots” generated would make connecting them virtually impossible. In any case, computer programs would be relatively easy to evade through the use of code words.

The real answer to Posner’s notion of balance, however, is not to show that a different balance can be struck, but to return to established Fourth Amendment jurisprudence, which has long required that searches must generally be justified by a showing of objective, specific suspicion approved by a judge who is willing to issue a specific warrant. The requirements that a warrant be issued and that it be based on “probable cause” are designed to protect privacy unless there are fairly strong grounds for official intrusion. The principal evil that the Fourth Amendment was drafted to avoid was the “general warrant,” which permitted government officials to search anyone’s home, without suspicion of specific individuals. Posner’s program is nothing less than a twenty-first-century version of exactly what the Fourth Amendment was designed to forbid. Through an open-ended and inevitably subjective balancing of privacy and security, he has managed to turn the Fourth Amendment on its head.

#### Fourth, *every* unconstitutional breach of privacy rights must be rejected to prevent total erosion of liberty.

Solove 11 — Daniel J. Solove, John Marshall Harlan Research Professor of Law at the George Washington University Law School, Founder of TeachPrivacy—a company that provides privacy and data security training programs to businesses, schools, healthcare institutions, and other organizations, Fellow at the Ponemon Institute and at the Yale Law School’s Information Society Project, Serves on the Advisory Boards of the Electronic Frontier Foundation, the Future of Privacy Forum, and the Law and Humanities Institute, holds a J.D. from Yale Law School, 2011 (“The Nothing-to-Hide Argument,” *Nothing to Hide: The False Tradeoff between Privacy and Security*, Published by Yale University Press, ISBN 9780300172317, p. 29-31)

Blood, Death, and Privacy

One of the difficulties with the nothing-to-hide argument is that it looks for a singular and visceral kind of injury. Ironically, this underlying [end page 29] conception of injury is sometimes shared by those advocating for greater privacy protections. For example, the law professor Ann Bartow argues that in order to have a real resonance, privacy problems must “negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease.” She urges that privacy needs more “dead bodies” and that privacy’s “lack of blood and death, or at least of broken bones and buckets of money, distances privacy harms from other [types of harm].”23

Bartow’s objection is actually consistent with the nothing-to-hide argument. Those advancing the nothing-to-hide argument have in mind a particular kind of appalling privacy harm, one where privacy is violated only when something deeply embarrassing or discrediting is revealed. Like Bartow, proponents of the nothing-to-hide argument demand a dead-bodies type of harm.

Bartow is certainly right that people respond much more strongly to blood and death than to more abstract concerns. But if this is the standard to recognize a problem, then few privacy problems will be recognized. Privacy is not a horror movie, most privacy problems don’t result in dead bodies, and demanding more palpable harms will be difficult in many cases.

In many instances, privacy is threatened not by a single egregious act but by the accretion of a slow series of relatively minor acts. In this respect, privacy problems resemble certain environmental harms which occur over time through a series of small acts by different actors. Although society is more likely to respond to a major oil spill, gradual pollution by a multitude of different actors often creates worse problems.

Privacy is rarely lost in one fell swoop. It is often eroded over time, little bits dissolving almost imperceptibly until we finally begin to notice how much is gone. When the government starts monitoring the phone numbers people call, many may shrug their shoulders and say, “Ah, it’s just numbers, that’s all.” Then the government might start monitoring some phone calls. “It’s just a few phone calls, nothing [end page 30] more,” people might declare. The government might install more video cameras in public places, to which some would respond, “So what? Some more cameras watching in a few more places. No big deal.” The increase in cameras might ultimately expand to a more elaborate network of video surveillance. Satellite surveillance might be added, as well as the tracking of people’s movements. The government might start analyzing people’s bank records. “It’s just my deposits and some of the bills I pay—no problem.” The government may then start combing through credit card records, then expand to Internet service provider (ISP) records, health records, employment records, and more. Each step may seem incremental, but after a while, the government will be watching and knowing everything about us.

“My life’s an open book,” people might say. “I’ve got nothing to hide.” But now the government has a massive dossier of everyone’s activities, interests, reading habits, finances, and health. What if the government leaks the information to the public? What if the government mistakenly determines that based on your pattern of activities, you’re likely to engage in a criminal act? What if it denies you the right to fly? What if the government thinks your financial transactions look odd—even if you’ve done nothing wrong—and freezes your accounts? What if the government doesn’t protect your information with adequate security, and an identity thief obtains it and uses it to defraud you? Even if you have nothing to hide, the government can cause you a lot of harm.

“But the government doesn’t want to hurt me,” some might argue. In many cases, this is true, but the government can also harm people inadvertently, due to errors or carelessness.

#### Finally, constitutional rights like privacy *can’t be “outweighed”* on the basis of cost-benefit analysis. This is especially important in the context of *terrorism*.

Cole 7 — David Cole, Professor at Georgetown University Law Center, has litigated many significant constitutional cases in the Supreme Court, holds a J.D. from Yale Law School, 2007 (“Book Review: The Poverty of Posner's Pragmatism: Balancing Away Liberty After 9/11 (Review of Richard A. Posner’s *Not A Suicide Pact: The Constitution In A Time Of National Emergency*),” *Stanford Law Review* (59 Stan. L. Rev. 1735), April, Available Online to Subscribing Institutions via Lexis-Nexis)

II. The Disappearing Constitution

The general problem with Posner's approach is that it does away with the animating idea of the Constitution - namely, that it is a form of collective precommitment. The genius behind the Constitution is precisely the recognition that "pragmatic" cost-benefit decisions of the type Posner favors will often appear in the short term to favor actions that in the long term are contrary to our own best principles. Just as we may be tempted to smoke a cigarette tonight [\*1746] even though in the long term we are likely to suffer as a result, so we know collectively that in the short term we are likely to empower government to suppress unpopular speech, invade the privacy of "dangerous" minorities, and abuse suspected criminals, even though in the long term such actions undermine the values of free speech, equality, and privacy that are necessary to democracy and human flourishing. If we were always capable of rationally assessing the costs and benefits in such a way as to maximize our collective well-being, short-term and long-term, we might not need a Constitution. But knowing that societies, like individuals, will be tempted to act in ways that undermine their own best interests, we have precommitted to a set of constitutional constraints on pragmatic balancing. Posner's view that the Constitution must bend to the point of authorizing virtually any initiative that seems pragmatic to him reduces the Constitution to a precommitment to balance costs and benefits, and that is no precommitment at all.

Constitutional theory demands more than ad hoc balancing. n27 While the nature of competing interests means that at some level of generality, a balance must be struck, constitutional analysis is not an invitation to the freewheeling, all-things-considered balance of the economist. Instead, it requires an effort, guided by text, precedent, and history, to identify the higher principles that guide us as a society, principles so important that they trump democracy itself (not to mention efficiency). The judge's constitutional duty was perhaps best captured by Justice John Marshall Harlan, writing about the due process clause:

Due process has not been reduced to any formula; its content cannot be determined by reference to any code. The best that can be said is that through the course of this Court's decisions it has represented the balance which our Nation, built upon postulates of respect for the liberty of the individual, has struck between that liberty and the demands of organized society. If the supplying of content to this Constitutional concept has of necessity been a rational process, it certainly has not been one where judges have felt free to roam where unguided speculation might take them. The balance of which I speak is the balance struck by this country, having regard to what history teaches are the traditions from which it developed as well as the traditions from which it broke. That tradition is a living thing. A decision of this Court which radically departs from it could not long survive, while a decision which builds on what has survived is likely to be sound. No formula could serve as a substitute, in this area, for judgment and restraint. n28

Instead of looking to the Constitution and its jurisprudence as a reflection of our collective effort to determine the higher principles that should guide us, as Harlan suggests, Posner would start from scratch, assessing what is best from a pragmatic, open-ended balancing approach that he admits ultimately involves weighing imponderables.

 [\*1747] Posner insists that to declare a practice constitutional is not the same as saying that it is desirable as a policy matter: "Much that the government is permitted by the Constitution to do it should not do and can be forbidden to do by legislation or treaties" (p. 7). That is certainly true as a theoretical matter, at least where one's constitutional theory is not reducible to one's policy preferences. But Posner appears to view questions of constitutionality as simply a matter of weighing all the costs and benefits, which is surely the same utilitarian calculus the policymaker would use to determine whether a practice is desirable. Under Posner's approach, then, it is difficult to see why there would be any room between what is desirable and what is constitutional.

If constitutionalism is to have any bite, it must be distinct from mere policy preferences. In fact, our Constitution gives judges the authority to declare acts of democratically elected officials unconstitutional on the understanding that they will not simply engage in the same cost-benefit analyses that politicians and economists undertake. The very sources Judge Posner dismisses - text, precedent, tradition, and reason - as unhelpful in the face of the threat of catastrophic terrorism are absolutely essential to principled constitutional decision-making. It is true that text, precedent, tradition, and reason do not determine results in some mechanistic way. That is why we ask judges, not machines, to decide constitutional cases. But these sources are nonetheless critically important constraints on and guides to constitutional decision-making. They are what identify those principles that have been deemed fundamental - and therefore constitutional - over our collective history.

The Framers of the Constitution did not simply say "the government may engage in any practice whose benefits outweigh its costs," as Judge Posner would have it. Instead, they struggled to articulate a limited number of fundamental principles and enshrine them above the everyday pragmatic judgments of politicians. They foresaw what modern history has shown to be all too true - that while democracy is an important antidote to tyranny, it can also facilitate a particular kind of tyranny - the tyranny of the majority. Constitutional principles protect those who are likely to be the targets of such tyranny, such as terror suspects, religious and racial minorities, criminal defendants, enemy combatants, foreign nationals, and, especially in this day and age, Arabs and Muslims. Relegating such individuals to the mercy of the legislature denies the existence of that threat. The Constitution is about more than efficiency and more than democracy; it is a collective commitment to the equal worth and dignity of all human beings. To fail to see that is to miss the very point of constitutional law.

Posner's trump card is that because terrorism in the twenty-first century poses the risk of truly catastrophic harm, it renders constitutional precedent and history largely irrelevant. Everything has changed. We are in a new paradigm, in which, as Alberto Gonzales said of the Geneva Conventions, the old rules (apparently including even those enshrined in the Constitution) are now [\*1748] "quaint" or "obsolete." n29 But each new generation faces unforeseen challenges. The advent of modern weaponry changed war as we knew it. Communism backed by the Soviet Union posed a "new" threat of totalitarian takeover. The development of the nuclear bomb ushered in yet another new era. This is not to deny that there is a real threat that terrorists may get their hands on weapons of mass destruction, and that this threat must be taken very seriously. But it is to insist on what is a truly conservative point - that principles developed and applied over two centuries still have something important to say in guiding us as we address the threat of modern terrorism.

The corollary to Posner's pragmatic and utilitarian balancing approach to the Constitution is that judges should defer to the political branches on national security questions. Judges have no special expertise in national security, he argues, while the political branches do (p. 9). Decisions invalidating security measures as unconstitutional reduce our flexibility, for they are extremely difficult to change through the political process, and may cut off avenues of experimentation (p. 27). But the Constitution was meant to cut off certain avenues. Trying suspected terrorists without a jury, locking them up without access to a judge, convicting them without proving guilt beyond a reasonable doubt, searching them without probable cause or a warrant, and subjecting them to torture all might make terrorists' tasks more difficult (although, as I have argued elsewhere, many of these shortcuts actually help the terrorists and make us more vulnerable, because of the backlash they provoke). n30 But while the Constitution may not be a "suicide pact," neither is it a license to do anything our leaders think might improve our safety.

### 1AC — Tech Leadership Advantage

#### Contention Two: Tech Leadership

#### First, NSA surveillance is decimating the U.S. tech industry. The fallout will be large and long-term unless confidence in U.S. companies is restored.

Donohue 15 — Laura K. Donohue, Associate Professor of Law, Director of the Center on National Security and the Law, and Director of the Center on Privacy and Technology at Georgetown University, has held fellowships at Stanford Law School’s Center for Constitutional Law, Stanford University’s Center for International Security and Cooperation, and Harvard University’s John F. Kennedy School of Government, holds a Ph.D. in History from the University of Cambridge and a J.D. from Harvard Law School, 2015 (“High Technology, Consumer Privacy, and U.S. National Security,” Forthcoming Article in the *Business Law Review*, Available Online via SSRN at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2563573>, Accessed 08-08-2015, p. 3-6)

II. Economic Impact of NSA Programs

The NSA programs, and public awareness of them, have had an immediate and detrimental impact on the U.S. economy. They have cost U.S. companies billions of dollars in lost sales, even as companies have seen their market shares decline. American multinational corporations have had to develop new products and programs to offset the revelations and to build consumer confidence. At the same time, foreign entities have seen revenues increase. Beyond the immediate impact, the revelation of the programs, and the extent to which the NSA has penetrated foreign data flows, has undermined U.S. trade agreement negotiations. It has spurred data localization efforts around the world, and it has raised the spectre of the future role of the United States in Internet governance. Even if opportunistic, these shifts signal an immediate and long-term impact of the NSA programs, and public knowledge about them, on the U.S. economy.

A. Lost Revenues and Declining Market Share

Billions of dollars are on the line because of worldwide concern that the services provided by U.S. information technology companies are neither secure nor private.13 Perhaps nowhere is this more apparent than in cloud computing. [end page 3]

Previously, approximately 50% of the worldwide cloud computing revenues derived from the United States.14 The domestic market thrived: between 2008 and 2014, it more than tripled in value. 15 But within weeks of the Snowden leaks, reports had emerged that U.S. companies such as Dropbox, Amazon Web Services, and Microsoft’s Azure were losing business. 16 By December 2013, ten percent of the Cloud Security Alliance had cancelled U.S. cloud services projects as a result of the Snowden information.17 In January 2014 a survey of Canadian and British businesses found that one quarter of the respondents were moving their data outside the United States.18

The Information Technology and Innovation Foundation estimates that declining revenues of corporations that focus on cloud computing and data storage alone could reach $35 billion over the next three years.19 Other commentators, such as Forrester Research analyst James Staten, have put actual losses as high as $180 billion by 2016, unless something is done to restore confidence in data held by U.S. companies.20

The monetary impact of the NSA programs extends beyond cloud computing to the high technology industry. Cisco, Qualcomm, IBM, Microsoft, and Hewlett-Packard have all reported declining sales as a direct result of the NSA programs.21 Servint, a webhosting company based in Virginia, reported in June 2014 that its international clients had dropped by 50% since the leaks began.22 Also in June, the German government announced that because of Verizon’s complicity in the NSA program, it would end its contract with the company, which had previously [end page 4] provided services to a number of government departments.23 As a senior analyst at the Information Technology and Innovation Foundation explained, “It’s clear to every single tech company that this is affecting their bottom line.”24 The European commissioner for digital affairs, Neelie Kroes, predicts that the fallout for U.S. businesses in the EU alone will amount to billions of Euros.25

Not only are U.S. companies losing customers, but they have been forced to spend billions to add encryption features to their services. IBM has invested more than a billion dollars to build data centers in London, Hong Kong, Sydney, and elsewhere, in an effort to reassure consumers outside the United States that their information is protected from U.S. government surveillance. 26 Salesforce.com made a similar announcement in March 2014.27 Google moved to encrypt terms entered into its browser. 28 In June 2014 it took the additional step of releasing the source code for End-to-End, its newly-developed browser plugin that allows users to encrypt email prior to it being sent across the Internet.29 The following month Microsoft announced Transport Layer Security for inbound and outbound email, and Perfect Forward Secrecy encryption for access to OneDrive.30 Together with the establishment of a Transparency Center, where foreign governments could review source code to assure themselves of the integrity of Microsoft software, the company sought to put an end to both NSA back door surveillance and doubt about the integrity of Microsoft products. 31

Foreign technology companies, in turn, are seeing revenues increase. Runbox, for instance, an email service based in Norway and a direct competitor to Gmail and Yahoo, almost immediately made it publicly clear that it does not comply with foreign court requests for its customers’ personal information. 32 Its customer base increased 34% in the aftermath of the Snowden leaks. 33 Mateo Meier, CEO of Artmotion, Switzerland’s biggest offshore data hosting company, reported that within the first month of the leaks, the company saw a 45% rise in revenue.34 Because Switzerland is not a member of the EU, the only way to access data in a Swiss data center is through an official court order demonstrating guilt or liability; there are no exceptions for the United States.35 In April 2014, Brazil and the EU, which previously used U.S. firms to supply undersea cables for transoceanic [end page 5] communications, decided to build their own cables between Brazil and Portugal, using Spanish and Brazilian companies in the process. 36 OpenText, Canada’s largest software company, now guarantees customers that their data remains outside the United States. Deutsche Telekom, a cloud computing provider, is similarly gaining more customers.37 Numerous foreign companies are marketing their products as “NSA proof” or “safer alternatives” to those offered by U.S. firms, gaining market share in the process. 38

#### Second, this decline in the U.S. tech sector is crushing U.S. global tech leadership.

Castro and McQuinn 15 — Daniel Castro, Vice President of the Information Technology and Innovation Foundation—a nonprofit, non-partisan technology think tank, former IT Analyst at the Government Accountability Office, holds an M.S. in Information Security Technology and Management from Carnegie Mellon University and a B.S. in Foreign Service from Georgetown University, and Alan McQuinn, Research Assistant with the Information Technology and Innovation Foundation, holds a B.S. in Political Communications and Public Relations from the University of Texas-Austin, 2015 (“Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness,” Report by the Information Technology & Innovation Foundation, June, Available Online at <http://www2.itif.org/2015-beyond-usa-freedom-act.pdf?_ga=1.61741228.1234666382.1434075923>, Accessed 07-05-2015, p. 7)

Conclusion

When historians write about this period in U.S. history it could very well be that one of the themes will be how the United States lost its global technology leadership to other nations. And clearly one of the factors they would point to is the long-standing privileging of U.S. national security interests over U.S. industrial and commercial interests when it comes to U.S. foreign policy.

This has occurred over the last few years as the U.S. government has done relatively little to address the rising commercial challenge to U.S. technology companies, all the while putting intelligence gathering first and foremost. Indeed, policy decisions by the U.S. intelligence community have reverberated throughout the global economy. If the U.S. tech industry is to remain the leader in the global marketplace, then the U.S. government will need to set a new course that balances economic interests with national security interests. The cost of inaction is not only short-term economic losses for U.S. companies, but a wave of protectionist policies that will systematically weaken U.S. technology competiveness in years to come, with impacts on economic growth, jobs, trade balance, and national security through a weakened industrial base. Only by taking decisive steps to reform its digital surveillance activities will the U.S. government enable its tech industry to effectively compete in the global market.

#### Third, this jeopardizes national security. A strong U.S. tech sector is the lynchpin of U.S. global power.

Donohue 15 — Laura K. Donohue, Associate Professor of Law, Director of the Center on National Security and the Law, and Director of the Center on Privacy and Technology at Georgetown University, has held fellowships at Stanford Law School’s Center for Constitutional Law, Stanford University’s Center for International Security and Cooperation, and Harvard University’s John F. Kennedy School of Government, holds a Ph.D. in History from the University of Cambridge and a J.D. from Harvard Law School, 2015 (“High Technology, Consumer Privacy, and U.S. National Security,” Forthcoming Article in the *Business Law Review*, Available Online via SSRN at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2563573>, Accessed 08-08-2015, p. 14-15)

To the extent that the NSA programs, and public knowledge of them, has harmed the U.S. economy, they have harmed U.S. national security. The country’s economic strength is part of what enables the United States to respond to external and internal threats. The ability to defend the country against would-be aggressors requires resources—e.g., to build and equip a military force, to move troops, to [end page 14] respond to attacks in whatever form they may materialize. Many of the supplies needed to fend off overreaching by either states or non-state actors derive not from government production, but from the private sector. To the extent that a weak private sector emerges, the government’s ability to respond is harmed.

Beyond this, economic security allows the country the freedom to determine its international and domestic policies on the merits, not on need. Where the United States is in a strong economic position, it is less vulnerable in international negotiations, such as those related to trade. It is also in a politically superior position, where it can use its wealth to accomplish the desired ends.

A strong economy also ensures that citizens have their needs met, with sufficient income levels for housing, food, clothing, and education. This, in turn, generates social and political stability, which allows for the development of communities, which creates greater cohesion among citizens. It also contributes to the evolution of democratic deliberations, reinforcing the rule of law.

Economic security allows for growth and innovation, which is fed by education and opportunity. Innovation, in turn, allows the country to continue to adapt to the evolving environment and international context. There are further considerations. But these suffice to illustrate the importance of economic strength to U.S. national security writ large.

#### Fourth, U.S. leadership is vital to global stability. Relative decline opens a power vacuum that spurs conflict.

Goure 13 — Daniel Goure, President of The Lexington Institute—a nonprofit public-policy research organization, Adjunct Professor in Graduate Programs at the Center for Peace and Security Studies at Georgetown University, Adjunct Professor at the National Defense University, former Deputy Director of the International Security Program at the Center for Strategic and International Studies, has consulted for the Departments of State, Defense and Energy, has taught or lectured at the Johns Hopkins University, the Foreign Service Institute, the National War College, the Naval War College, the Air War College, and the Inter-American Defense College, holds Masters and Ph.D. degrees in International Relations and Russian Studies from Johns Hopkins University, 2013 (“How U.S. Military Power Holds the World Together,” *inFocus Quarterly*—the Jewish Policy Center's journal, Volume VII, Number 2, Summer, Available Online at http://www.jewishpolicycenter.org/4397/us-military-power, Accessed 08-17-2013)

The Centrality of U.S. Power

There are three fundamental problems with the argument in favor of abandoning America's security role in the world. The first problem is that the United States cannot withdraw without sucking the air out of the system. U.S. power and presence have been the central structural feature that holds the present international order together. It flavors the very air that fills the sphere that is the international system. Whether it is the size of the U.S. economy, its capacity for innovation, the role of the dollar as the world's reserve currency or the contribution of U.S. military power to the stability and peace of the global commons, the present world order has "Made in the USA" written all over it.

The international system is not a game of Jenga where the worst thing that can happen is that one's tower collapses. Start taking away the fundamental building blocks of the international order, particularly American military power, and the results are all but certain to be major instability, increased conflict rates, rapid proliferation of nuclear weapons, economic dislocation and, ultimately, serious and growing threats to security at home.

#### Finally, U.S. leadership resolves a myriad of catastrophic global impacts. The right policies will prevent decline.

Lieber 13 — Robert J. Lieber, Professor of Government and International Affairs at Georgetown University, has held fellowships from the Guggenheim, Rockefeller and Ford Foundations, the Council on Foreign Relations, and the Woodrow Wilson International Center for Scholars, holds a Ph.D. from the Department of Government at Harvard University, 2013 (“Against the Idea of American Decline,” *inFocus Quarterly*—the Jewish Policy Center's journal, Volume VII, Number 2, Summer, Available Online at http://www.jewishpolicycenter.org/4398/american-decline, Accessed 08-17-2013)

The stakes are immense, and not only for America itself. Since World War II, the United States has been the world's principal provider of collective goods. The leading international institutions of today and much of the existing international order have been a product of American leadership. Evidence from recent decades suggests that the alternative is not that some other institution or major power (the UN, the EU, China, India, Russia, or Japan) will take its place, but that none will. Some have argued that the effects of globalization are leading the world toward greater cooperation and even collective security. This may be a comforting view about the implications or even desirability of American disengagement, but practical experience suggests otherwise. In dealing with failed states, ethnic cleansing, human rights, the environment, trade liberalization, regional conflict, and nuclear proliferation, emerging powers such as the BRICS (Brazil, Russia, India, China, and South Africa) have been largely unhelpful, and others in Europe, Asia, Africa, or Latin America have more often than not lacked the will or capacity to act collectively on common tasks.

For the United States, the maintenance of its leading role matters greatly. The alternative would not only be a more disorderly and dangerous world in which its own economic and national security would be adversely affected, but also regional conflicts and the spread of nuclear weapons would be more likely. In addition, allies and those sharing common values, especially liberal democracy and the market economy, would increasingly be at risk. Ultimately, America's ability to avoid long-term decline—and the significant international retrenchment that would be a result of severely reduced resources—becomes a matter of policy and political will. There is nothing inevitable or fated about decline. Both past experience and national attributes matter greatly. Flexibility, adaptability, and the capacity for course correction provide the United States with a resilience that has proved invaluable in the past and is likely to do so in the future.

### 1AC — Cybersecurity Advantage

#### First, U.S. government attacks on encryption destroy cybersecurity.

Open Letter 15 — An Open Letter to President Obama co-signed by 36 civil society organizations (including the American Civil Liberties Union, Electronic Frontier Foundation, Electronic Privacy Information Center, and the Free Software Foundation), 48 technology companies and trade associations (including Apple, Facebook, Google, Microsoft, and Yahoo), and 58 security and policy experts (including Jacob Applebaum, Eric Burger, Joan Feigenbaum, and Bruce Schneier), the full list of signatories is available at the URL below, 2015 (Open Letter to Obama, May 19th, Available Online at https://static.newamerica.org/attachments/3138--113/Encryption\_Letter\_to\_Obama\_final\_051915.pdf, Accessed 06-29-2015, p. 1)

Strong encryption is the cornerstone of the modern information economy’s security. Encryption protects billions of people every day against countless threats—be they street criminals trying to steal our phones and laptops, computer criminals trying to defraud us, corporate spies trying to obtain our companies’ most valuable trade secrets, repressive governments trying to stifle dissent, or foreign intelligence agencies trying to compromise our and our allies’ most sensitive national security secrets.

Encryption thereby protects us from innumerable criminal and national security threats. This protection would be undermined by the mandatory insertion of any new vulnerabilities into encrypted devices and services. Whether you call them “front doors” or “back doors”, introducing intentional vulnerabilities into secure products for the government’s use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government’s own experts.

#### Second, backdoors necessarily devastate cybersecurity — *inherent complexity* and *concentrated targets*.

Crypto Experts 15 — Harold Abelson, Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology, Fellow of The Institute of Electrical and Electronics Engineers, Founding Director of Creative Commons and the Free Software Foundation, holds a Ph.D. in Mathematics from the Massachusetts Institute of Technology, et al., with Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner, qualifications of these co-authors available upon request, 2015 (“Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications,” Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report (MIT-CSAIL-TR-2015-026), July 6th, Available Online at http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf, Accessed 07-20-2015, p. 2-3)

The goal of this report is to similarly analyze the newly proposed requirement of exceptional access to communications in today’s more complex, global information infrastructure. We find that it would pose far more grave security risks, imperil innovation, and raise thorny issues for human rights and international relations.

There are three general problems. First, providing exceptional access to communications would force a U-turn from the best practices now being deployed to make the Internet more secure. These practices include forward secrecy — where decryption keys are deleted immediately after use, so that stealing the encryption key used by a communications server would not compromise earlier or later communications. A related technique, authenticated encryption, uses the same temporary key to guarantee confidentiality and to verify that the message has not been forged or tampered with.

Second, building in exceptional access would substantially increase system complexity. Security researchers inside and outside government agree that complexity is the enemy of security — every new feature can interact with others to create vulnerabilities. To achieve widespread exceptional access, new technology features would have to be deployed and tested with literally hundreds of thousands of developers all around the world. This is a far more complex environment than the electronic surveillance now deployed in telecommunications and Internet access services, which tend to use similar technologies and are more likely to have the resources to manage vulnerabilities that may arise from new features. Features to permit law enforcement exceptional access across a wide range of Internet and mobile computing applications could be particularly problematic because their typical use would be surreptitious — making security testing difficult and less effective.

Third, exceptional access would create concentrated targets that could attract bad actors. Security credentials that unlock the data would have to be retained by the platform provider, law enforcement agencies, or some other trusted third party. If law enforcement’s keys guaranteed access to everything, an attacker who gained access to these keys would enjoy the same privilege. Moreover, law enforcement’s stated need for rapid access to data would make it impractical to store keys offline or split keys among multiple keyholders, as security engineers would normally do with extremely high-value credentials. Recent attacks on the United States Government Office of Personnel Management (OPM) show how much harm can arise when many organizations rely on a single institution that itself has security vulnerabilities. In the case of OPM, numerous federal agencies lost sensitive data because OPM had insecure infrastructure. If service providers implement exceptional [end page 2] access requirements incorrectly, the security of all of their users will be at risk.

#### Third, cyber attacks are *frequent* and *devastating*. Every attack increases the risk of widespread catastrophe.

Nolan 15 — Andrew Nolan, Legislative Attorney at the Congressional Research Service, former Trial Attorney at the United States Department of Justice, holds a J.D. from George Washington University, 2015 (“Cybersecurity and Information Sharing: Legal Challenges and Solutions,” CRS Report to Congress, March 16th, Available Online at <http://fas.org/sgp/crs/intel/R43941.pdf>, Accessed 07-05-2015, p. 1-3)

Introduction

Over the course of the last year, a host of cyberattacks1 have been perpetrated on a number of high profile American companies. In January 2014, Target announced that hackers, using malware,2 had digitally impersonated one of the retail giant’s contractors,3 stealing vast amounts of data—including the names, mailing addresses, phone numbers or email addresses for up to 70 million individuals and the credit card information of 40 million shoppers.4 Cyberattacks in February and March of 2014 potentially exposed contact and log-in information of eBay’s customers, prompting the online retailer to ask its more than 200 million users to change their passwords.5 In September, it was revealed that over the course of five months cyber-criminals tried to steal the credit card information of more than fifty million shoppers of the world’s largest home improvement retailer, Home Depot.6 One month later, J.P. Morgan Chase, the largest U.S. bank by assets, disclosed that contact information for about 76 million households was captured in a cyberattack earlier in the year.7 In perhaps the most infamous cyberattack of 2014, in late November, Sony Pictures Entertainment suffered a “significant system disruption” as a result of a “brazen cyber attack”8 that resulted in the leaking of the personal details of thousands of Sony employees.9 And in February of 2015, the health care provider Anthem Blue Cross Blue Shield [end page 1] disclosed that a “very sophisticated attack” obtained personal information relating to the company’s customers and employees.10

The high profile cyberattacks of 2014 and early 2015 appear to be indicative of a broader trend: the frequency and ferocity of cyberattacks are increasing,11 posing grave threats to the national interests of the United States. Indeed, the attacks on Target, eBay, Home Depot, J.P. Morgan-Chase, Sony Pictures, and Anthem were only a few of the many publicly disclosed cyberattacks perpetrated in 2014 and 2105.12 Experts suggest that hundreds of thousands of other entities may have suffered similar incidents during the same period,13 with one survey indicating that 43% of firms in the United States had experienced a data breach in the past year.14 Moreover, just as the cyberattacks of 2013—which included incidents involving companies like the New York Times, Facebook, Twitter, Apple, and Microsoft15—were eclipsed by those that occurred in 2014,16 the consensus view is that 2015 and beyond will witness more frequent and more sophisticated cyber incidents.17 To the extent that its expected rise outpaces any corresponding rise in the ability to defend against such attacks, the result could be troubling news for countless businesses that rely more and more on computers in all aspects of their operations, as the economic losses resulting from a single cyberattack can be extremely costly.18 And the resulting effects of a cyberattack can have effects beyond a single company’s bottom line. As “nations are becoming ever more dependent on information and information technology,”19 the threat posed by any one cyberattack [end page 2] can have “devastating collateral and cascading effects across a wide range of physical, economic and social systems.”20 With reports that foreign nations—such as Russia, China, Iran, and North Korea—may be using cyberspace as a new front to wage war,21 fears abound that a cyberattack could be used to shut down the nation’s electrical grid,22 hijack a commercial airliner,23 or even launch a nuclear weapon with a single keystroke.24 In short, the potential exists that the United States could suffer a “cyber Pearl Harbor,” an attack that would “cause physical destruction and loss of life”25 and expose—in the words of one prominent cybersecurity expert—“vulnerabilities of staggering proportions.”26

#### Fourth, cyber attacks risk electric grid shutdowns that collapse the military. This prompts nuclear retaliation.

Tilford 12 — Robert Tilford, Wichita Military Affairs Contributor for the *Examiner*, retired Private in the United States Army, Graduate of the U.S. Army Infantry School and U.S. Army Airborne School at Fort Benning, Georgia, quoting Chuck Grassley, Member of the United States Senate (R-IA), 2012 (“Cyber attackers could shut down the electric grid for the entire east coast,” *Examiner*, July 27th, Available Online at <http://www.examiner.com/article/cyber-attackers-could-easily-shut-down-the-electric-grid-for-the-entire-east-coa>, Accessed 08-09-2015)

In a speech before members of the United States Senate on July 26, 2012, Republican Chuck Grassley spoke about the need to protect the country from a devestating cyber attack.

He didn't mince words either:

“Cyber attackers could all too easily shut down the electric grid for the entire east coast, the west coast, and the middle part of our country”, said Senator Grassley on July 26, 2012.

“Any one attack could leave dozens of major cities and tens of millions of Americans without power. We know, because we were shown in a room here in the Capitol, how an attack could take place and what damage it would do, so we know this is not just make believe”, he said.

So what would a cyber attack look like anyway?

The Senator explained:

“Without ATMs or debit card readers, commerce would immediately grind to a halt. My daughter, who lives here in the DC area, lost power when the storm hit. They waited for a number of hours, and then they took all the food out of their freezer, they gave away what they could, and they threw the rest away. And that was the way it was all over. Their power was out for about a week, and it made it very difficult. They are fortunate enough to have a basement, and the heat wasn’t oppressive down there. Without refrigeration, food would rot on the shelves, the freezers would have to be emptied, and people could actually go hungry. Without gas pumps, transportation arteries would clog with abandoned vehicles. Without cell phones or computers, whole regions of the country would be cut off from communication and families would be unable to reach each other. Without air conditioning and without lifesaving technology and the service of hospitals and nursing homes, the elderly and sick would become much sicker and die. Most major hospitals have backup power, but it is only for a limited amount of time. It depends on how much fuel they can store, and that is very limited”, Senator Grassley said.

The devastation that the Senator describes is truly unimaginable.

To make matters worse a cyber attack that can take out a civilian power grid, for example could also cripple the U.S. military.

The senator notes that is that the same power grids that supply cities and towns, stores and gas stations, cell towers and heart monitors also power “every military base in our country.”

“Although bases would be prepared to weather a short power outage with backup diesel generators, within hours, not days, fuel supplies would run out”, he said.

Which means military command and control centers could go dark.

Radar systems that detect air threats to our country would shut down completely.

“Communication between commanders and their troops would also go silent. And many weapons systems would be left without either fuel or electric power”, said Senator Grassley.

“So in a few short hours or days, the mightiest military in the world would be left scrambling to maintain base functions”, he said.

We contacted the Pentagon and officials confirmed the threat of a cyber attack is something very real.

Top national security officials—including the Chairman of the Joint Chiefs, the Director of the National Security Agency, the Secretary of Defense, and the CIA Director— have said, “preventing a cyber attack and improving the nation’s electric grids is among the most urgent priorities of our country” (source: Congressional Record).

So how serious is the Pentagon taking all this?

Enough to start, or end a war over it, for sure (see video: Pentagon declares war on cyber attacks http://www.youtube.com/watch?v=\_kVQrp\_D0kY&feature=relmfu ).

A cyber attack today against the US could very well be seen as an “Act of War” and could be met with a “full scale” US military response.

That could include the use of “nuclear weapons”, if authorized by the President.

#### Finally, *only* strong encryption can protect cybersecurity. The plan is key.

Kehl et al. 15 — Danielle Kehl, Senior Policy Analyst at the Open Technology Institute at the New America Foundation, holds a B.A. in History from Yale University, with Andi Wilson, Policy Program Associate at the Open Technology Institute at the New America Foundation, holds a Master of Global Affairs degree from the Munk School at the University of Toronto, and Kevin Bankston, Policy Director at the Open Technology Institute at the New America Foundation, former Senior Counsel and Director of the Free Expression Project at the Center for Democracy & Technology, former Senior Staff Attorney at the Electronic Frontier Foundation, former Justice William Brennan First Amendment Fellow at the American Civil Liberties Union, holds a J.D. from the University of Southern California Law School, 2015 (“Doomed To Repeat History? Lessons From The Crypto Wars of the 1990s,” Report by the Open Technology Institute at the New America Foundation, June, Available Online at <https://static.newamerica.org/attachments/3407--125/Lessons%20From%20the%20Crypto%20Wars%20of%20the%201990s.882d6156dc194187a5fa51b14d55234f.pdf>, Accessed 07-06-2015, p. 19)

Strong Encryption Has Become A Bedrock Technology That Protects The Security Of The Internet

The evolution of the ecosystem for encrypted communications has also enhanced the protection of individual communications and improved cybersecurity. Today, strong encryption is an essential ingredient in the overall security of the modern network, and adopting technologies like HTTPS is increasingly considered an industry best-practice among major technology companies.177 Even the report of the President’s Review Group on Intelligence and Communications Technologies, the panel of experts appointed by President Barack Obama to review the NSA’s surveillance activities after the 2013 Snowden leaks, was unequivocal in its emphasis on the importance of strong encryption to protect data in transit and at rest. The Review Group wrote that:

Encryption is an essential basis for trust on the Internet; without such trust, valuable communications would not be possible. For the entire system to work, encryption software itself must be trustworthy. Users of encryption must be confident, and justifiably confident, that only those people they designate can decrypt their data…. Indeed, in light of the massive increase in cyber-crime and intellectual property theft on-line, the use of encryption should be greatly expanded to protect not only data in transit, but also data at rest on networks, in storage, and in the cloud.178

The report further recommended that the U.S. government should:

Promote security[] by (1) fully supporting and not undermining efforts to create encryption standards; (2) making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption; and (3) supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage.179

### 1AC — Plan

#### The United States federal government should prohibit federal agencies from requiring or compelling private entities to design or alter their commercial information technology products for the purpose of facilitating domestic surveillance.

### 1AC — Solvency

#### Contention Four: Solvency

#### First, the SDA is crucial to end the U.S.’s *war on encryption*. This solves privacy, tech competitiveness, and cybersecurity.

Wyden 14 — Ron Wyden, United States Senator (D-OR) who serves on the Senate Select Committee on Intelligence and who is known as “the internet’s Senator” for his leadership on technology issues, former Member of the United States House of Representatives, holds a J.D. from the University of Oregon School of Law, 2014 (“With hackers running rampant, why would we poke holes in data security?,” *Los Angeles Times*, December 14th, Available Online at <http://www.latimes.com/opinion/op-ed/la-oe-1215-wyden-backdoor-for-cell-phones-20141215-story.html>, Accessed 06-24-2015)

Hardly a week goes by without a new report of some massive data theft that has put financial information, trade secrets or government records into the hands of computer hackers.

The best defense against these attacks is clear: strong data encryption and more secure technology systems.

The leaders of U.S. intelligence agencies hold a different view. Most prominently, James Comey, the FBI director, is lobbying Congress to require that electronics manufacturers create intentional security holes — so-called back doors — that would enable the government to access data on every American's cellphone and computer, even if it is protected by encryption.

Unfortunately, there are no magic keys that can be used only by good guys for legitimate reasons. There is only strong security or weak security.

Americans are demanding strong security for their personal data. Comey and others are suggesting that security features shouldn't be too strong, because this could interfere with surveillance conducted for law enforcement or intelligence purposes. The problem with this logic is that building a back door into every cellphone, tablet, or laptop means deliberately creating weaknesses that hackers and foreign governments can exploit. Mandating back doors also removes the incentive for companies to develop more secure products at the time people need them most; if you're building a wall with a hole in it, how much are you going invest in locks and barbed wire? What these officials are proposing would be bad for personal data security and bad for business and must be opposed by Congress.

In Silicon Valley several weeks ago I convened a roundtable of executives from America's most innovative tech companies. They made it clear that widespread availability of data encryption technology is what consumers are demanding.

It is also good public policy. For years, officials of intelligence agencies like the NSA, as well as the Department of Justice, made misleading and outright inaccurate statements to Congress about data surveillance programs — not once, but repeatedly for over a decade. These agencies spied on huge numbers of law-abiding Americans, and their dragnet surveillance of Americans' data did not make our country safer.

Most Americans accept that there are times their government needs to rely on clandestine methods of intelligence gathering to protect national security and ensure public safety. But they also expect government agencies and officials to operate within the boundaries of the law, and they now know how egregiously intelligence agencies abused their trust.

This breach of trust is also hurting U.S. technology companies' bottom line, particularly when trying to sell services and devices in foreign markets. The president's own surveillance review group noted that concern about U.S. surveillance policies “can directly reduce the market share of U.S. companies.” One industry estimate suggests that lost market share will cost just the U.S. cloud computing sector $21 billion to $35 billion over the next three years.

Tech firms are now investing heavily in new systems, including encryption, to protect consumers from cyber attacks and rebuild the trust of their customers. As one participant at my roundtable put it, “I'd be shocked if anyone in the industry takes the foot off the pedal in terms of building security and encryption into their products.”

Built-in back doors have been tried elsewhere with disastrous results. In 2005, for example, Greece discovered that dozens of its senior government officials' phones had been under surveillance for nearly a year. The eavesdropper was never identified, but the vulnerability was clear: built-in wiretapping features intended to be accessible only to government agencies following a legal process.

Chinese hackers have proved how aggressively they will exploit any security vulnerability. A report last year by a leading cyber security company identified more than 100 intrusions in U.S. networks from a single cyber espionage unit in Shanghai. As another tech company leader told me, “Why would we leave a back door lying around?”

Why indeed. The U.S. House of Representatives recognized how dangerous this idea was and in June approved 293-123, a bipartisan amendment that would prohibit the government from mandating that technology companies build security weaknesses into any of their products. I introduced legislation in the Senate to accomplish the same goal, and will again at the start of the next session.

Technology is a tool that can be put to legitimate or illegitimate use. And advances in technology always pose a new challenge to law enforcement agencies. But curtailing innovation on data security is no solution, and certainly won't restore public trust in tech companies or government agencies. Instead we should give law enforcement and intelligence agencies the resources that they need to adapt, and give the public the data security they demand.

#### Finally, the plan effectively prevents law enforcement and intelligence agencies from weakening encryption. This is crucial to safeguard privacy, tech competitiveness, and cybersecurity.

McQuinn 14 — Alan McQuinn, Research Assistant with the Information Technology and Innovation Foundation, holds a B.S. in Political Communication from the University of Texas-Austin, 2014 (“The Secure Data Act could help law enforcement protect against cybercrime,” *The Hill*, December 19th, Available Online at <http://thehill.com/blogs/congress-blog/technology/227594-the-secure-data-act-could-help-law-enforcement-protect-against>, Accessed 06-24-2015)

Last Sunday, Sen. Ron Wyden (D-Ore.) wrote an op-ed describing the role that U.S. law enforcement should play in fostering stronger data encryption to make information technology (IT) systems more secure. This op-ed explains Wyden’s introduction of the the Secure Data Act, which would prohibit the government from mandating that U.S. companies build “backdoors” in their products for the purpose of surveillance. This legislation responds directly to recent comments by U.S. officials, most notably the Federal Bureau of Investigation (FBI) Director James Comey, chastising Apple and Google for creating encrypted devices to which law enforcement cannot gain access. Comey and others have argued that U.S. tech companies should design a way for law enforcement officials to access consumer data stored on those devices. In this environment, the Secure Data Act is a homerun for security and privacy and is a good step towards reasserting U.S. competitiveness in building secure systems for a global market.

By adopting its position on the issue the FBI is working against its own goal of preventing cybercrime as well as broader government efforts to improve cybersecurity. Just a few years ago, the Bureau was counseling people to better encrypt their data to safeguard it from hackers. Creating backdoor access for law enforcement fundamentally weakens IT systems because it creates a new pathway for malicious hackers, foreign governments, and other unauthorized parties to gain illicit access. Requiring backdoors is a step backwards for companies actively working to eliminate security vulnerabilities in their products. In this way, security is a lot like a ship at sea, the more holes you put in the system—government mandated or not—the faster it will sink. The better solution is to patch up all the holes in the system and work to prevent any new ones. Rather than decreasing security to suit its appetite for surveillance, the FBI should recognize that better security is needed to bolster U.S. defenses against online threats.

The Secure Data Act is an important step in that direction because it will stop U.S. law enforcement agencies from requiring companies to introduce vulnerabilities in their products. If this bill is enacted, law enforcement will be forced to use other means to solve crimes, such as by using metadata from cellular providers, call records, text messages, and even old-fashioned detective work. This will also allow U.S. tech companies, with the help of law enforcement, to continue to strengthen their systems, better detect intrusions, and identify emerging threats. Law enforcement, such as the recently announced U.S. Department of Justice Cybersecurity Unit—a unit designed solely to “deter, investigate, and prosecute cyber criminals,” should work in cooperation with the private sector to create a safer environment online. A change of course is also necessary to restore the ability of U.S. tech companies to compete globally, where mistrust has run rampant following the revelations of mass government surveillance.

With the 113th Congress at an end, Wyden has promised to reintroduce the Data Secure Act again in the next Congress. Congress should move expediently to advance Senator Wyden’s bill to promote security and privacy in U.S. devices and software. Furthermore, as Congress marks up the legislation and considers amendments, it should restrict not just government access to devices, but also government control of those devices. These efforts will move the efforts of our law enforcement agencies away from creating cyber vulnerabilities and allow electronics manufacturers to produce the most secure devices imaginable.

## 2AC — Constitutional Privacy Advantage

### They Say: “Encryption Unconstitutional”

#### Encryption is vital to *First* and *Fourth* Amendment rights. Their argument turns the Constitution on its head.

Bankston 15 — Kevin Bankston, Policy Director of the Open Technology Institute at the New America Foundation, former Senior Counsel and the Director of the Free Expression Project at the Center for Democracy & Technology, former Fellow at the Stanford Law School’s Center for Internet & Society, former Senior Staff Attorney at the Electronic Frontier Foundation, former Justice William Brennan First Amendment Fellow at the American Civil Liberties Union, holds a J.D. from the University of Southern California Law School, 2015 (“OTI Policy Director Kevin Bankston Offers Ten Reasons Why Backdoor Mandates Are A Bad Idea,” Open Technology Institute at the New America Foundation, April 28th, Available Online at <https://www.newamerica.org/new-america/oti-policy-director-kevin-bankston-offers-ten-reasons-why-backdoor-mandates-are-a-bad-idea/>, Accessed 08-12-2015)

6. It would undermine — and turn on its head — the Fourth Amendment right to be secure in our papers and effects.

The Fourth Amendment gives individuals the right to be secure in their papers and effects, prohibiting unreasonable searches and seizures and requiring that any warrant authorizing such a government invasion be issued by a court based on a showing of probable cause. Recent Supreme Court cases like Riley v. California have argued that the need for vigorous enforcement of that right has become even more acute in the context of powerful digital technologies. The court did not pretend that requiring warrants for searches of cellphones seized incident to arrest did not risk diminishing law enforcement’s effectiveness — it simply recognized that allowing warrantless searches posed an even greater risk to our Fourth Amendment rights considering the scope of data available on those phones.

Encryption opponents would push in the other direction and flip our Fourth Amendment rights on their head, casting the Fourth Amendment as a right of the government — a right to dictate that the contours of the physical and digital worlds be redesigned to facilitate even easier surveillance. But as former computer crime prosecutor Marc Zwillinger recently put it, “I don’t believe that law enforcement has an absolute right to gain access to every way in which two people may choose to communicate… And I don’t think our Founding Fathers would think so, either. The fact that the Constitution offers a process for obtaining a search warrant where there is probable cause is not support for the notion that it should be illegal to make an unbreakable lock.” The law has never prohibited the creation of unbreakable locks, nor required us to hand our keys over to the government just in case it might need them for an investigation.

7. It would threaten First Amendment rights here and free expression around the world.

Repeated court challenges to export controls on encryption during the Crypto Wars illustrate how any attempt by the government to limit the distribution of encryption software code, which is itself speech, would raise serious First Amendment concerns. Similarly, a legal regime that forced individuals to hand over their private encryption keys to the government or to their communications providers for law enforcement purposes would also raise novel issues of compelled speech under the First Amendment. What’s more, a mandate against unbreakable encryption and in favor of backdoors for government could have even broader chilling effects. By contrast, encouraging the availability of strong encryption free of surveillance backdoors can enable free expression both in the United States and around the world, including by stymieing the censorship and surveillance efforts of governments with less respect for human rights than our own.

#### Encryption is the lynchpin of freedom of *opinion* and *expression*. Without it, intellectual privacy is impossible.

Fulton quoting Kaye 15 — Deirdre Fulton, Staff Writer for *Common Dreams*, quoting David Kaye, UN Special Rapporteur and author of a report about encryption released by the United Nations Office of the High Commissioner for Human Rights, 2015 (“No Backdoors: Online 'Zone of Privacy' is a Basic Human Right,” *Common Dreams*, May 29th, Available Online at <http://www.commondreams.org/news/2015/05/29/no-backdoors-online-zone-privacy-basic-human-right>, Accessed 06-29-2015)

Encryption and anonymity tools, which help protect individuals' private data and communications, are essential to basic human rights, according to a report released Friday by the United Nations Office of the High Commissioner for Human Rights.

Issued while U.S. lawmakers are engaged in heated debates over online privacy, data collection, and so-called 'back-door' surveillance methods, the document recommends holding proposed limits on encryption and anonymity to a strict standard: "If they interfere with the right to hold opinions, restrictions must not be adopted."

The report, written by UN Special Rapporteur David Kaye, is based on questionnaire responses submitted by 16 countries, opinions submitted by 30 non-government stakeholders, and statements made at a meeting of experts in Geneva in March.

The document reads, in part: "Encryption and anonymity, today’s leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression."

Kaye makes specific mention of tech tools such as Tor, a free software that directs Internet traffic through a free, worldwide, volunteer network consisting of more than 6,000 servers to conceal users' location and usage from anyone conducting online surveillance.

Such tools, the report continues, "create a zone of privacy to protect opinion and belief. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one’s gender, religion, ethnicity, national origin or sexuality."

Among its many recommendations for states and corporations, the document advises that governments "avoid all measures that weaken the security that individuals may enjoy online."

It cites "broadly intrusive measures" such as the back-doors that tech companies build into their products in order to facilitate law enforcement access to encrypted content. In the U.S., FBI Director James Comey and NSA chief Adm. Michael Rogers have both expressed support for backdoors and other restrictions on encryption.

The problem with all of those approaches is that they "inject a basic vulnerability into secure systems," Kaye told the Washington Post. "It results in insecurity for everyone even if intended to be for criminal law enforcement purposes."

#### Encryption is essential to privacy — it outweighs security.

Zdziarski 14 — Jonathan Zdziarski, considered one of the world’s foremost experts in iOS related digital forensics and security, Principal Software Engineer at Accessdata Group LLC, former Senior Forensic Scientist at Viaforensics, former Senior Research Scientist at Barracuda Networks, 2014 (“The Politics Behind iPhone Encryption and the FBI,” *Zdziarski's Blog of Things*—Jonathan Zdziarski’s blog, September 25th, Available Online at <http://www.zdziarski.com/blog/?p=3894>, Accessed 07-20-2015)

While perhaps a heartfelt utopian ideal, the fact is that demanding back doors for law enforcement is selfish. It’s selfish in that they want a backdoor to serve their own interests. Non law-enforcement types, such as Orin Kerr, a reporter who wrote a piece in the Washington Post supporting FBI backdoors (and then later changed his mind), are being selfish by demanding that others give up their privacy to make them feel safer. This is the absolute opposite of a society where law enforcement serves the public interest. What Kerr, and anyone supporting law enforcement back doors, really wants, is a society that caters to their fears at the expense of others’ privacy.

While we individually choose to trust the law enforcement we come in contact with, government only works if we inherently and collectively distrust it on a public level. Our public policies and standards should distrust those we have put in a position to watch over us. Freedom only works when the power is balanced toward the citizens; providing the government with the ability to choose to invade our 1st, 4th and 5th Amendment rights is only an invitation to lose control of our own freedom. Deep inside this argument is not one of public safety, but a massive power grab away from the people’s right to privacy. Whether everyone involved realizes that, it is privacy itself that is at stake.

Our founding fathers were aware that distrusting government was essential to freedom, and that’s why they used encryption. In fact, because of their own example in concealing correspondence, one can make an even stronger case supporting encryption as an instrument of free speech. The constitution is the highest law of the land – it’s above all other laws. Historically, our founding fathers guarded all instruments available that protect our freedom as beyond the law’s reach: The Press, Firearms, Assembly. These things provided information, teeth, and consensus. Modern encryption is just as essential to our freedom as a country as firearms, and are the teeth that guarantees our freedom of speech and freedom from fear to speak and communicate.

Encryption today still just as vital to free speech as it was in the 1700s, and to freedom itself. What’s at stake here is so much bigger than solving a crime. The excuse of making us safer has been beaten to death as a means to take away freedoms for hundreds of years. Don’t be so naive to think that this time, it’s any different.

### They Say: “Privacy Already Dead”

#### Government surveillance is a much greater threat because people can’t *opt-out*.

Fung 13 — Brian Fung, Technology Reporter for *The Washington Post*, former Technology Correspondent for *National Journal*, former Associate Editor at the *Atlantic*, holds an MSc in International Relations from the London School of Economics and a B.A. in Political Science from Middlebury College, 2013 (“Yes, there actually is a huge difference between government and corporate surveillance,” *The Washington Post*, November 4th, Available Online at <https://www.washingtonpost.com/news/the-switch/wp/2013/11/04/yes-there-actually-is-a-huge-difference-between-government-and-corporate-surveillance/>, Accessed 08-05-2015)

When it comes to your online privacy — or what little is left of it — businesses and governments act in some pretty similar ways. They track your credit card purchases. They mine your e-mail for information about you. They may even monitor your movements in the real world. Corporate and government surveillance also diverge in important ways. Companies are looking to make money off of you, while the government aims to prevent attacks that would halt that commercial activity (along with some other things).

But the biggest difference between the two has almost no relation to who's doing the surveillance and everything to do with your options in response. Last week, we asked you whether you'd changed your online behavior as a result of this year's extended national conversation about privacy — and if so, which form of snooping annoyed you more. Looking through the responses so far, this one caught my eye:

The government because I can't \*choose\* not to be spied on by them. The government also has the power to kill or imprison me which no private company has. I am a firm believer that our founding fathers created a system that respected individual privacy and to see it eroded by the federal government concerns me deeply. I am a strong believer in the 1st, 2nd, 4th and 5th amendments.

Putting aside the government's power to capture or kill, your inability to refuse the government is what distinguishes the NSA from even the nosiest companies on Earth. In a functioning marketplace, boycotting a company that you dislike — for whatever reason — is fairly easy. Diners who object to eating fake meat can stop frequenting Taco Bell. Internet users that don't like Google collecting their search terms can try duckduckgo, an anonymous search engine.

By contrast, it's nearly impossible to simply pick up your belongings and quit the United States. For most people, that would carry some significant costs — quitting your job, for instance, or disrupting your children's education, or leaving friends and family. Those costs can be high enough to outweigh the benefits of recovering some hard-to-measure modicum of privacy. Besides, leaving the country would ironically expose you to even greater risk of surveillance, since you'd no longer be covered by the legal protections granted to people (even foreign terror suspects) that arrive to U.S. shores.

There are still some ways to shield yourself from the NSA. To the best of our knowledge, the government has yet to crack the encryption protocols behind Tor, the online traffic anonymizing service. But Tor's users are also inherently the object of greater suspicion precisely because they're making efforts to cover their tracks.

In the business world, no single company owns a monopoly over your privacy. The same can't really be said about the government.

#### The government has unique powers to violate individuals’ privacy.

Harper 12 — Jim Harper, Director of Information Policy Studies at the Cato Institute, founding member of the Department of Homeland Security’s Data Privacy and Integrity Advisory Committee, holds a J.D. from the University of California-Hastings College of Law, 2012 (“Why Government is the Greater Threat to Privacy,” The Institute for Policy Innovation—a non-profit, non-partisan public policy think tank, November 2nd, Available Online at <http://www.ipi.org/ipi_issues/detail/why-government-is-the-greater-threat-to-privacy>, Accessed 08-05-2015)

Individuals enjoy privacy when they have the power to control information about themselves and when they have exercised that power consistent with their interests and values.

But while most of the debate about privacy has been focused on privacy with regard to private companies, government poses a much greater threat to privacy. In terms of privacy, the public sector and the private sector are worlds apart.

Because of governments’ unique powers, the issue of privacy from government is of a much more critical nature than privacy from companies. Governments can invade privacy by taking and using personal information against the will of individuals. Private companies cannot get information from people who refuse to share it. Moving beyond privacy, governments can knock down doors, audit people’s finances, break up families, and throw people in jail. A bright line should separate our contemplation of privacy from government and privacy in the private sector.

#### On balance, governments are a greater threat to privacy.

Harper 12 — Jim Harper, Director of Information Policy Studies at the Cato Institute, founding member of the Department of Homeland Security’s Data Privacy and Integrity Advisory Committee, holds a J.D. from the University of California-Hastings College of Law, 2012 (“Why Government is the Greater Threat to Privacy,” The Institute for Policy Innovation—a non-profit, non-partisan public policy think tank, November 2nd, Available Online at <http://www.ipi.org/ipi_issues/detail/why-government-is-the-greater-threat-to-privacy>, Accessed 08-05-2015)

Conclusion

Between government and the private sector, government is the clearest threat to privacy. Governments have the power to take information from people and use it in ways that are objectionable or harmful. This is a power that no business has: People can always turn away from businesses that do not satisfy their demands for privacy.

Privacy advocates and concerned citizens should be far more concerned about governments as potential abusers of privacy.

### They Say: “Nothing To Hide”

#### Privacy is vital to freedom. Posner’s argument breeds conformity and passivity.

Greenwald 14 — Glenn Greenwald, journalist who received the 2014 Pulitzer Prize for Public Service for his work with Edward Snowden to report on NSA surveillance, Founding Editor of *The Intercept*, former Columnist for the *Guardian* and *Salon*, recipient of the Park Center I.F. Stone Award for Independent Journalism, the Online Journalism Award for investigative work on the abusive detention conditions of Chelsea Manning, the George Polk Award for National Security Reporting, the Gannett Foundation Award for investigative journalism, the Gannett Foundation Watchdog Journalism Award, the Esso Premio for Excellence in Investigative Reporting in Brazil, and the Electronic Frontier Foundation’s Pioneer Award, holds a J.D. from New York University School of Law, 2014 (“What Bad, Shameful, Dirty Behavior is U.S. Judge Richard Posner Hiding? Demand to Know.,” *The Intercept*, December 8th, Available Online at <https://firstlook.org/theintercept/2014/12/08/bad-shameful-dirty-secrets-u-s-judge-richard-posner-hiding-demand-know/>, Accessed 06-28-2015)

Richard Posner has been a federal appellate judge for 34 years, having been nominated by President Reagan in 1981. At a conference last week in Washington, Posner said the NSA should have the unlimited ability to collect whatever communications and other information it wants: “If the NSA wants to vacuum all the trillions of bits of information that are crawling through the electronic worldwide networks, I think that’s fine.” The NSA should have “carte blanche” to collect what it wants because “privacy interests should really have very little weight when you’re talking about national security.”

His rationale? “I think privacy is actually overvalued,” the distinguished jurist pronounced. Privacy, he explained, is something people crave in order to prevent others from learning about the shameful and filthy things they do:

Much of what passes for the name of privacy is really just trying to conceal the disreputable parts of your conduct. Privacy is mainly about trying to improve your social and business opportunities by concealing the sorts of bad activities that would cause other people not to want to deal with you.

Unlike you and your need to hide your bad and dirty acts, Judge Posner has no need for privacy – or so he claims: “If someone drained my cell phone, they would find a picture of my cat, some phone numbers, some email addresses, some email text,” he said. “What’s the big deal?” He added: “Other people must have really exciting stuff. Do they narrate their adulteries, or something like that?”

I would like to propose a campaign inspired by Judge Posner’s claims (just by the way, one of his duties as a federal judge is to uphold the Fourth Amendment). In doing so, I’ll make the following observations:

First, note the bargain Judge Posner offers, the one that is implicitly at the heart of all surveillance advocacy: as long as you make yourself extremely boring and unthreatening – don’t exercise your political liberties, but instead, just take pictures of your cat, arrange Little League games, and exchange recipes – then you have nothing to worry about from surveillance. In other words, as long as you remain what Judge Posner is – an obedient servant of political and corporate power – then you have nothing to worry about from surveillance.

The converse, of course, is equally true: if you do anything unorthodox or challenging to those in power – if, for instance, you become a civil rights leader or an antiwar activist – then you are justifiably provoking surveillance aimed at you. That is the bargain at the heart of the anti-privacy case, which is why a surveillance state, by design, breeds conformity and passivity – which in turn is why all power centers crave it. Every time surveillance is discussed, someone says something to the effect of: “I’m not worried about being surveilled because I’ve chosen to do nothing that’d be interesting to the government or anyone else.” That self-imprisoning mindset, by itself, is as harmful as any abuse of surveillance power (in September, I gave a 15-minute TED talk specifically designed to address and refute the inane “nothing to hide” anti-privacy rationale Judge Posner offers here).

#### The ends don’t justify the means: even people with “nothing to hide” are harmed by surveillance.

Snowden 15 — Edward Snowden, NSA whistleblower, Member of the Board of Directors of the Freedom of the Press Foundation, former Central Intelligence Agency officer and National Security Agency contractor, 2015 (“Just days left to kill mass surveillance under Section 215 of the Patriot Act. We are Edward Snowden and the ACLU’s Jameel Jaffer. AUA.,” Reddit Ask Me Anything with Edward Snowden, May 21st, Available Online at <https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/crglgh2>, Accessed 06-16-2015)

Jameel is right, but I think the central issue is to point out that regardless of the results, the ends (preventing a crime) do not justify the means (violating the rights of the millions whose private records are unconstitutionally seized and analyzed).

Some might say "I don't care if they violate my privacy; I've got nothing to hide." Help them understand that they are misunderstanding the fundamental nature of human rights. Nobody needs to justify why they "need" a right: the burden of justification falls on the one seeking to infringe upon the right. But even if they did, you can't give away the rights of others because they're not useful to you. More simply, the majority cannot vote away the natural rights of the minority.

But even if they could, help them think for a moment about what they're saying. Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

A free press benefits more than just those who read the paper.

\* Jameel = Jameel Jaffer, Deputy Legal Director of the American Civil Liberties Union and Director of the ACLU's Center for Democracy

#### There is a substantial chilling effect — Wittes is wrong.

Masnick 14 — Mike Masnick, Founder and Chief Executive Officer of Floor64—a software company, Founder and Editor of *Techdirt*, 2014 (“Saying That You're Not Concerned Because The NSA Isn't Interested In You Is Obnoxious And Dangerous,” *Techdirt*, July 16th, Available Online at https://www.techdirt.com/articles/20140703/18113427778/saying-that-youre-not-concerned-because-nsa-isnt-interested-you-is-obnoxious-dangerous.shtml, Accessed 07-05-2015)

One of the more common responses we've seen to all of the revelations about all of that NSA surveillance, is the response that "Well, I don't think the NSA really cares about what I'm doing." A perfect example of that is long-time NSA defender Ben Wittes, who recently wrote about why he's not too worried that the NSA is spying on him at all, basically comparing it to the fact that he's confident that law enforcement isn't spying on him either:

As I type these words, I have to take on faith that the Washington D.C. police, the FBI, the DEA, and the Secret Service are not raiding my house. I also have to take on faith that federal and state law enforcement authorities are not tapping my various phones. I have no way of knowing they are not doing these things. They certainly have the technical capability to do them. And there’s historical reason to be concerned. Indeed, there is enough history of government abuse in the search and seizure realm that the Founders specifically regulated the area in the Bill of Rights. Yet I sit here remarkably confident that these things are not happening while my back is turned—and so do an enormous number of other Americans.

The reason is that the technical capability for a surveillance event to take place does not alone amount to the reality—or likelihood—of that event’s taking place....

For much the same reason as I am not rushing home to guard my house, I have a great deal of confidence that the National Security Agency is not spying on me. No doubt it has any number of capabilities to do so. No doubt those capabilities are awesome—in the wrong hands the tools of a police state. But there are laws and rules that protect me, and there are compliance mechanisms that ensure that the NSA follows those laws and rules. These systems are, to be sure, different from those that restrain the D.C. cops, but they are robust enough to reassure me.

Julian Sanchez has a blistering response to that, appropriately entitled Check Your Privilege, which highlights that while Wittes, a well-paid, white, DC-based policy think tank worker, may be confident of those things, plenty of other folks are not nearly so confident, and that the NSA has made it pretty clear that they shouldn't be so confident.

In a democracy, of course, the effects of surveillance are not restricted to its direct targets. Spying, like censorship, affects all of us to the extent it shapes who holds power and what ideas hold sway. Had the FBI succeeded in “neutralizing” Martin Luther King Jr. earlier in his career, it would hardly have been a matter of concern solely for King and his family—that was, after all, the whole point.

Instead of a couple wonks comfortably ensconced in D.C. institutions, let’s instead ask a peaceful Pakistani-American who protests our policy of targeted killings, perhaps in collaboration with activists abroad; we might encounter far less remarkable confidence. Or, if that seems like too much effort, we can just look to the survey of writers conducted by the PEN American Center, finding significant percentages of respondents self-censoring or altering their use of the Internet and social media in the wake of revelations about the scope of government surveillance. Or to the sworn declarations of 22 civil society groups in a lawsuit challenging bulk phone records collection, attesting to a conspicuous decline in telephonic contacts and members expressing increased anxiety about their association with controversial or unpopular organizations.

As Sanchez notes, it's not just whether or not any of us are direct targets, but the overall chilling effects of how the system is used. And, I should note, that while Wittes is confident that he's safe -- there are a growing number of folks who have good reason to believe that they are not immune from such surveillance. The recent revelation that Tor users are labeled as extremists who get extra-special scrutiny seems like a major concern. Similarly, the story from earlier this year that the NSA targeted the Pirate Bay and Wikileaks as part of some of its surveillance efforts is a major concern. In the process of doing journalism, I've communicated with folks associated with some of those and other similar organizations. In the past, I probably would have similarly noted that I doubted the NSA cared at all about what I was doing, but as each of these stories comes out, I am increasingly less sure. And, more importantly, even if the NSA is not at all concerned with what I happen to be doing, just the fact that I now have to think about what it means if they might be certainly creates a chilling effect, and makes me think twice over certain people I contact, and what I say to them.

It's easy to claim that you're not worried when you're the one out there supporting those in power. It becomes a lot trickier when you're either criticizing those in power, or communicating with those who challenge the power structure. Suddenly, it's not so easy to sit on the sidelines and say "Meh, no one's going to care about me..." And that should be a major concern. The way we keep a strong democracy is by having people who are able and willing to challenge the status quo and those in power. And yes, the US is much more forgiving than many, many other countries to such people, but there are clear biases and clear cases where they are not at all accepting of such things. And the more of a chilling effect the government creates around those things, the more dangerous it becomes to stand up for what you believe in.

### They Say: “Weigh Consequences”

#### The Constitution enshrines fundamental principles as side constraints that guide cost-benefit analysis. Posner is wrong — those principles can’t be balanced away.

Cole 7 — David Cole, Professor at Georgetown University Law Center, has litigated many significant constitutional cases in the Supreme Court, holds a J.D. from Yale Law School, 2007 (“‘How to Skip the Constitution’: An Exchange,” *New York Review of Books*, January 11th, Available Online at <http://www.nybooks.com/articles/archives/2007/jan/11/how-to-skip-the-constitution-an-exchange/>, Accessed 06-28-2015)

More generally, Judge Posner shies away from his own constitutional theory when he says that to declare a practice constitutional is not the same as saying that it is desirable as a policy matter. That is certainly true as a theoretical matter, at least where one’s constitutional theory is not reducible to one’s policy preferences. But as my review points out, Posner views questions of constitutionality as simply a matter of weighing all the costs and benefits, which is surely the same utilitarian calculus the policymaker would use to determine whether a practice is desirable. Under Posner’s approach, then, it’s hard to see why there would be any room between what is desirable and what is constitutional.

Judge Posner accuses me, in effect, of subscribing to the same constitutionalism-as-policy approach that he uses by asserting, without evidentiary support, that my constitutional views simply track my own policy preferences; “the rest is rhetoric.” But I believe that there is a critical distinction between constitutionalism and mere policy preferences. In fact, our Constitution gives judges the authority to declare acts of democratically elected officials unconstitutional on the understanding that they do not simply engage in the same cost-benefit analyses that politicians and economists undertake.

My own view is that the very sources Judge Posner dismisses—text, precedent, tradition, and reason—are absolutely essential to principled constitutional decision-making. Posner suggests that because none of these elements necessarily provides a determinate answer to difficult questions, we may as well abandon them for his seat-of-the-pants, cost-benefit approach. It is true that text, precedent, tradition, and reason do not determine results in some mechanistic way. That is why we ask judges, not machines, to decide constitutional cases. But these sources are nonetheless critically important constraints on and guides to constitutional decision-making. They are what identify those principles that have been deemed fundamental—and therefore constitutional—over our collective history. That there are differences over principle in no way excludes the need for reasoned argument about them.

There is a reason the framers of the Constitution did not simply say “the government may engage in any practice whose benefits outweigh its costs,” as Judge Posner would have it, but instead struggled to articulate a limited number of fundamental principles and enshrine them above the everyday pragmatic judgments of politicians. They foresaw what modern history has shown to be all too true—that while democracy is an important antidote to tyranny, it can also facilitate a particular kind of tyranny—the tyranny of the majority. Constitutional principles protect those who are likely to be the targets of such tyranny, such as terror suspects, religious and racial minorities, criminal defendants, enemy combatants, foreign nationals, and, especially in this day and age, Arabs and Muslims. Relegating such individuals to the mercy of the legislature—whether it be Republican or Democratic—denies that threat. The Constitution is about more than efficiency, and more than democracy; it is a collective commitment to the equal worth and dignity of all human beings. To call that mere “rhetoric” is to miss the very point of constitutional law.

#### The neg’s impact comparison relies on *juking the stats*. “Balancing” liberty and security is a rigged game that *always* subjugates rights.

Sidhu 9 — Dawinder S. Sidhu, Visiting Researcher at the Georgetown University Law Center, former Fellow at the Center for Internet and Society at Stanford University, holds a J.D. from The George Washington University Law School and an M.A. in Government from Johns Hopkins University, 2009 (“Wartime America and the Wire: A Response to Posner's Post-9/11 Constitutional Framework,” *George Mason University Civil Rights Law Journal* (20 Geo. Mason U. Civ. Rts. L.J. 37), Fall, Available Online to Subscribing Institutions via Lexis-Nexis)

IV. Rigging the Game

"Juking the stats." n101

- Roland "Prez" Pryzbylewski, The Wire

In Not a Suicide Pact, Posner not only presents an unhelpful balancing scheme between liberty and security, a contest that is attended only by civil libertarians and hawkish security folks, but then also stacks the deck against the preservation of liberty such that security will invariably be dominant and liberty must consequently give way. n102 In particular, Posner posits that in times of war, greater weight is to be placed on security measures due to the heightened interest in protecting the homeland. He writes, "In times of danger, the weight of concerns for public safety increases relative to that of liberty concerns, and civil liberties are narrowed." n103 He continues, "[A] decline in [\*55] security causes the balance to shift against liberty," n104 and "the more endangered we feel, the more weight we place on the interest in safety." n105

Moreover, according to Posner, elevating security concerns above liberty interests may be necessary to ward off future terrorist activity. He speculates that "[a] minor curtailment of present civil liberties, to the extent that it reduces the probability of a terrorist attack, reduces the likelihood of a major future curtailment of those liberties." n106 Otherwise, "rooting out" the enemy "might be fatally inhibited if we felt constrained to strict observance of civil liberties." n107 From the government's point of view, Posner simply notes, "It is better to be safe than sorry." n108

Prez and others in The Wire often expressed their disappointment with the concept of "juking the stats." n109 This refers to a situation in which the powers that be—police commanders, high-level public school officials, or politicians—would manipulate perspectives or information to ultimately achieve a predetermined, preferred outcome. n110 It refers to the rigging of the system; it is result-oriented decisionmaking by those at the top of the power structure to the detriment [\*56] of those stakeholders with little or no bargaining ability. n111 For example, in an effort to appease the city's political leadership and the public to which the politicians were accountable, the high-level police officials implemented a strategy to increase the absolute number of arrests; in essence, they manufactured the impression that they were making a dent in city crime. n112 Although the number of arrests did increase, the arrests were of minor users and offenders; as such, police resources were drawn away from infiltrating the primary sources of the city's drug and related crime problems. n113 Even when the police furnished statistics that supported the suggestion that they were successful in addressing crime, in actuality the drug camp was unfazed and the public remained vulnerable to widespread drug trafficking and associated criminal activities. n114 The campaign, though successful on its face, was in truth ineffective and counterproductive.

Just as information could be "juked" to support a self-fulfilling outcome in The Wire, legal commentators recognize that the constitutional equation suggested by Posner is not objectively calibrated, but instead will yield only one pre-determined answer: Civil liberties must defer to security programs or policies. David Cole of the Georgetown University Law Center observed that "constitutional interpretation for Posner is little more than an all-things-considered balancing act—and when the potential costs of a catastrophic terrorist attack are placed on the scale, the concerns of constitutional rights and civil liberties are almost inevitably outweighed." n115 Two others criticize Posner's law and economics approach to security issues because his "method works largely through a cost-benefit analysis where equality and antisubordination never quite measure up to the concerns against [\*57] which they are being measured." n116 Similarly, another commentator writes that Posner's "method ... tilts in the favor of security more often than not." n117

In proposing that post-9/11 constitutional questions implicating the security of the nation be reduced to a balancing of purportedly competing interests, Posner offers a mechanism that is not only faulty in design, as both security and liberty can be simultaneously managed, but also troublesome in its application, as security invariably subjugates other constitutional interests, specifically individual rights. Accordingly, Posner's recommendation is consistent with the "rigging" exhibited and discredited in The Wire—giving the impression of an objective approach to produce a pre-determined outcome, but in essence depriving the people of a legitimate debate on the proper relationship between national security and individual rights.

#### Unconstitutional policies should be rejected regardless of consequences.

Carter 87 — Steven Carter, Professor of Law at Yale University, 1987 (“From Sick Chicken to Synar: The Evolution and Subsequent De-Evolution of the Separation of Powers,” *Brigham Young University Law Review*, Issue 3, Available Online at http://lawreview.byu.edu/archives/1987/3/car.pdf, Accessed 01-12-2013)

The Constitution, which is after all a species of law, is thus quite naturally viewed as a potential impediment to policy, a barrier that must be adjusted, through interpretation or amendment, more often than preservation of government under that Constitution is viewed as a desirable policy in itself. In this the modern student of policy is like the modern moral philosopher—and like a good number of constitutional theorists as well—in denigrating the value of preserving any particular process and exalting the desirable result. But constitutionalism assigns enormous importance to process, and consequently assigns costs, albeit perhaps intangible ones, to violating the constitutional process. For the constitutionalist, as for classical liberal democratic theory, the autonomy of the people themselves, not the achievement of some well-intentioned government policy, is the ultimate end for which the government exists. As a consequence, no violation of the means the people have approved for pursuit of policy—here, the means embodied in the structural provisions of the Constitution—can be justified through reference to the policy itself as the end**.**

### They Say: “Security Outweighs Privacy”

#### Weighing privacy against security *in the abstract* commits the all-or-nothing fallacy. Privacy outweighs security *in this case*.

Solove 11 — Daniel J. Solove, John Marshall Harlan Research Professor of Law at the George Washington University Law School, Founder of TeachPrivacy—a company that provides privacy and data security training programs to businesses, schools, healthcare institutions, and other organizations, Fellow at the Ponemon Institute and at the Yale Law School’s Information Society Project, Serves on the Advisory Boards of the Electronic Frontier Foundation, the Future of Privacy Forum, and the Law and Humanities Institute, holds a J.D. from Yale Law School, 2011 (“The All-or-Nothing Fallacy,” *Nothing to Hide: The False Tradeoff between Privacy and Security*, Published by Yale University Press, ISBN 9780300172317, p. 35-37)

The all-or-nothing fallacy causes tremendous distortion in the balance between privacy and security. In fact, I believe that many courts and commentators who balance security measures against privacy rights conduct the balance wrongly because of this fallacy. They cast the balance in terms of whether a particular government security measure should be barred. On one side of the scale they weigh the benefits of the security measure. On the other side they weigh privacy rights.

At first blush, this seems like a reasonable approach—balance the security measure against privacy. Yet it is quite wrong. Placing the security measure on the scale assumes that the entire security measure, all-or-nothing, is in the balance. It’s not. Protecting privacy seldom negates the security measure altogether. Rarely does judicial oversight or the application of the Fourth Amendment prohibit a government surveillance activity. Instead, the activity is allowed subject to oversight and sometimes a degree of limitation.

Most constitutional and statutory protections work this way. The Fourth Amendment, for example, allows all sorts of very invasive searches. Under the Fourth Amendment, the government can search your home. It can search your computer. It can do a full body-cavity search. It can search nearly anything and engage in nearly any kind of surveillance. How can this be so? Because the Fourth Amendment doesn’t protect privacy by stopping the government from searching; it works by requiring judicial oversight and mandating that the government justify its measures. So under the Fourth Amendment, the government can engage in highly invasive searches if it justifies the need to do so beforehand to a judge. [end page 35]

Like the Fourth Amendment, electronic-surveillance law allows for wiretapping, but limits the practice by mandating judicial supervision, minimizing the breadth of the wiretapping, and requiring law-enforcement officials to report back to the court to prevent abuses. Thus the protection of privacy might demand the imposition of oversight and regulation but need not entail scrapping an entire security measure.

When security is balanced against privacy, the entire security measure shouldn’t be weighed against the privacy harms it creates. Since protecting privacy involves imposing oversight and regulation on the initiative, the security side of the scale should gauge only the extent to which such oversight and regulation reduce the effectiveness of the security measure. If, say, judicial oversight and regulation designed to protect privacy result in delays and paperwork and limitations that make a security measure 10 percent less effective, it makes no sense to balance the entire security measure against privacy. Instead, the balance should be between privacy and the 10 percent decrease in the measure’s effectiveness.

Far too often, however, discussions of security and liberty fail to assess the balance this way. Polls frequently pose the question as an all-or-nothing tradeoff. A 2002 Pew Research poll asked American citizens:

Should the government be allowed to read e-mails and listen to phone calls to fight terrorism?3

A 2005 poll from Rasmussen Reports posed the question:

Should the National Security Agency be allowed to intercept telephone conversations between terrorism suspects in other countries and people living in the United States?4

Both these questions, however, neglect to account for warrants and court orders. Few would contend that the government shouldn’t be [end page 36] allowed to conduct a wide range of searches when it has a search warrant or court order. So the questions that should be posed are:

Should the government be allowed to read emails and listen to phone calls without a search warrant or the appropriate court order required by law to fight terrorism?

Should the National Security Agency be allowed to intercept telephone conversations between terrorism suspects in other countries and people living in the United States without a court order or judicial oversight?

The choice is not between a security measure and nothing, but between a security measure with oversight and regulation and a security measure at the sole discretion of executive officials. In many cases, oversight and regulation do not diminish a security measure substantially, so the cost of protecting privacy can be quite low. Unfortunately, the balance is rarely assessed properly. When the balance is measured under the all-or-nothing fallacy, the scale dips dramatically toward the security side. The costs of protecting privacy are falsely inflated, and the security measure is accorded too much weight.

#### Sacrificing privacy for the sake of security negates the Constitution. In this context, giving up privacy means giving up *the rule of law*.

Rotenberg 7 — Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, Adjunct Professor at the Georgetown University Law Center, Fellow of the American Bar Foundation, has testified before Congress more than 60 times including for the 9/11 Commission, holds a J.D. from Stanford Law School, 2007 (“Privacy vs. Security? Privacy.,” *The Huffington Post* — from a public debate hosted by The Miller Center for Public Affairs at the University of Virginia, November 13th, Available Online at <http://www.huffingtonpost.com/marc-rotenberg/privacy-vs-security-priva_b_71806.html>, Accessed 08-07-2015)

But Benjamin Franklin warned long ago that such a strategy would fail. The correct balance is not a metaphysical tradeoff between security and privacy. The correct balance -- really a counter-balance - is between the powers of government and the means of oversight that are established.

This is the point made clear by the 9-11 Commission. It is the oversight of government and the rights of the individuals that we are being asked to sacrifice, and no where is the cost more clear than with privacy.

In the modern era, the right of privacy represents a vast array of rights that include clear legal standards, government accountability, judicial oversight, the design of techniques that are minimally intrusive and the respect for the dignity and autonomy of individuals.

The choice that we are being asked to make is not simply whether to reduce our expectation of privacy, but whether to reduce the rule of law, whether to diminish the role of the judiciary, whether to cast a shroud of secrecy over the decisions made by government.

In other words, we are being asked to become something other than the strong America that could promote innovation and safeguard privacy that could protect the country and its Constitutional traditions. We are being asked to become a weak nation that accepts surveillance without accountability that cannot defend both security and freedom.

That is a position we must reject. If we agree to reduce our expectation of privacy, we will erode our Constitutional democracy.

#### Privacy *is* a security interest. Without it, society is unbearably oppressive.

Solove 11 — Daniel J. Solove, John Marshall Harlan Research Professor of Law at the George Washington University Law School, Founder of TeachPrivacy—a company that provides privacy and data security training programs to businesses, schools, healthcare institutions, and other organizations, Fellow at the Ponemon Institute and at the Yale Law School’s Information Society Project, Serves on the Advisory Boards of the Electronic Frontier Foundation, the Future of Privacy Forum, and the Law and Humanities Institute, holds a J.D. from Yale Law School, 2011 (“Why Privacy Isn’t Merely an Individual Right,” *Nothing to Hide: The False Tradeoff between Privacy and Security*, Published by Yale University Press, ISBN 9780300172317, p. 49-50)

In contrast, the philosopher John Dewey proposed an alternative theory about the relationship between individual and society. For Dewey, the good of individual and the good of society are often interrelated rather than antagonistic: “We cannot think of ourselves save as to some extent social beings. Hence we cannot separate the idea of ourselves and our own good from our idea of others and of their good.”7 Dewey contended that the value of protecting individual rights emerges from their contribution to society. In other words, individual [end page 49] rights are not trumps but are protections by society from its intrusiveness. Society makes space for the individual because of the social benefits this space provides. Therefore, Dewey argues, rights should be valued based on “the contribution they make to the welfare of the community.” Otherwise, in any kind of utilitarian calculus, individual rights wouldn’t be valuable enough to outweigh most social interests, and it would be impossible to justify individual rights. Dewey argued that we must insist upon a “social basis and social justification” for civil liberties.8

Like Dewey, I contend the value of protecting the individual is a social one. Society involves a great deal of friction, and we are constantly clashing with one another. Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be oppressive. When protecting individual rights, we as a society decide to hold back in order to receive the benefits of creating free zones for individuals to flourish.

As the legal theorist Robert Post has argued, privacy is not merely a set of restraints on society’s rules and norms. Instead, privacy constitutes a society’s attempt to promote civility.9 Society protects privacy as a means of enforcing order in the community. Privacy isn’t the trumpeting of the individual against society’s interests but the protection of the individual based on society’s own norms and values. Privacy isn’t simply a way to extricate individuals from social control; it is itself a form of social control that emerges from a society’s norms. It is not an external restraint on society but an internal dimension of society. Therefore, privacy has a social value. When the law protects the individual, it does so not just for the individual’s sake but for the sake of society. Privacy thus shouldn’t be weighed as an individual right against the greater social good. Privacy issues involve balancing societal interests on both sides of the scale.10

## 2AC — Tech Leadership Advantage

### They Say: “Alternate Causality – STEM”

#### There is no STEM shortage — consensus of studies.

Camarota 14 — Steven Camarota, Director of Research for the Center for Immigration Studies, holds a Ph.D. in Public Policy Analysis from the University of Virginia, 2014 (“What STEM Shortage?,” *National Review*, May 20th, Available Online at <http://www.nationalreview.com/article/378334/what-stem-shortage-steven-camarota>, Accessed 08-09-2015)

The idea that we need to allow in more workers with science, technology, engineering, and math (“STEM”) background is an article of faith among American business and political elite.

But in a new report, my Center for Immigration Studies colleague Karen Zeigler and I analyze the latest government data and find what other researchers have found: The country has well more than twice as many workers with STEM degrees as there are STEM jobs. Also consistent with other research, we find only modest levels of wage growth for such workers for more than a decade. Both employment and wage data indicate that such workers are not in short supply.

Reports by the Economic Policy Institute (EPI), the RAND Corporation, the Urban Institute, and the National Research Council have all found no evidence that STEM workers are in short supply. PBS even published an opinion piece based on the EPI study entitled, “The Bogus High-Tech Worker Shortage: How Guest Workers Lower U.S. Wages.” This is PBS, mind you, which is as likely to publish something skeptical of immigration as it is to publish something skeptical of taxpayer subsidies for the Corporation for Public Broadcasting.

RAND’s analysis looked backward in time and found, “Despite recurring concerns about potential shortages of STEM personnel . . . we did not find evidence that such shortages have existed at least since 1990, nor that they are on the horizon.”

#### The scholarly evidence is overwhelmingly on our side.

Teitelbaum 14 — Michael S. Teitelbaum, Senior Research Associate with the Labor and Worklife Program at Harvard Law School, former Vice President and Program Director at the Alfred P. Sloan Foundation, former faculty member at Princeton University and Oxford University, former Vice Chair and Acting Chair of the U.S. Commission on International Migration, holds a D.Phil. in Demography from Oxford University, 2014 (“The Myth of the Science and Engineering Shortage,” *The Atlantic*, March 19th, Available Online at <http://www.theatlantic.com/education/archive/2014/03/the-myth-of-the-science-and-engineering-shortage/284359/>, Accessed 08-09-2015)

A compelling body of research is now available, from many leading academic researchers and from respected research organizations such as the National Bureau of Economic Research, the RAND Corporation, and the Urban Institute. No one has been able to find any evidence indicating current widespread labor market shortages or hiring difficulties in science and engineering occupations that require bachelors degrees or higher, although some are forecasting high growth in occupations that require post-high school training but not a bachelors degree. All have concluded that U.S. higher education produces far more science and engineering graduates annually than there are S&E job openings—the only disagreement is whether it is 100 percent or 200 percent more. Were there to be a genuine shortage at present, there would be evidence of employers raising wage offers to attract the scientists and engineers they want. But the evidence points in the other direction: Most studies report that real wages in many—but not all—science and engineering occupations have been flat or slow-growing, and unemployment as high or higher than in many comparably-skilled occupations.

#### The U.S. has a STEM worker surplus, not a shortage.

Bruenig 13 — Matt Bruenig, Economics and Politics Writer for *PolicyShop*—the Demos blog, 2013 (“The STEM-Shortage Myth,” *The American Prospect*, April 25th, Available Online at <http://prospect.org/article/stem-shortage-myth>, Accessed 08-09-2015)

The Economic Policy Institute published a report yesterday on the supposed shortage of professionals in science, technology, engineering, and math (STEM). You've probably heard of the crisis by now. America is not producing enough STEM degrees. This will be the death of innovation and global competitiveness. We must reorient higher education to convert more liberal arts students into STEM students. And so on.

The problem with this alleged crisis is that it is not real. As the EPI report lays bare, the common wisdom about our STEM problem is mistaken: We are not facing a shortage of STEM-qualified workers. In fact, we appear to have a considerable STEM surplus. Only half of students graduating with a STEM degree are able to find STEM jobs. Beyond that, if there was an actual shortage of STEM workers, basic supply and demand would predict that the wages of STEM workers would be on the rise. Instead, wages in STEM fields have not budged in over a decade. Stagnant wages and low rates of STEM job placement strongly suggest we actually have an abundance of STEM-qualified workers.

### They Say: “Alternate Causality – Taxes”

#### Tech companies move cash overseas to avoid U.S. taxes.

Sullivan 13 — Mark Sullivan, Senior Editor of *TechHive*, 2013 (“How much tax do big tech companies pay?,” *TechHive*, April 13th, Available Online at <http://www.techhive.com/article/2034137/how-much-tax-do-big-tech-companies-pay-.html>, Accessed 08-10-2015)

Large U.S. tech companies should pay income taxes of about 35 percent on the profits they make (above $18.3 million) from business done in the United States. So says the tax code.

It rarely works out that way. Instead, many U.S. companies routinely park large chunks of their income overseas to avoid paying federal income taxes on it. And the SEC apparently looks the other way when companies obscure the true mix of their domestic-versus-overseas profit in their regulatory filings.

Ultimately, only the IRS knows how much these companies actually pay, and it’s not sharing the information with people like you and me.

Tech-sector companies have been especially adept at moving cash assets around the globe, and at muddying the waters as to precisely where their profits came from.

Under federal law, U.S. companies may permanently “defer” paying taxes on income transferred to foreign subsidiaries. Those monies may be subject to taxation by the country where they’ve been parked, but tax rates in popular tax haven countries like Bermuda are extremely low or even nonexistent.

Bloomberg reported in December that Google avoided paying $2 billion in global income taxes by moving $10 billion in revenue to Bermuda, which has no corporate income tax.

The fact that the tax rate on tech companies’ global income is less than the statutory rate of 35 percent in the United States suggests that shifting income overseas can reduce companies’ overall tax burden considerably, and often dramatically.

#### All the major tech companies do it — high tax rates are circumvented.

Bort 13 — Julie Bort, Editor of Enterprise Computing at *Business Insider*, 2013 (“Look At The Humongous Amounts Of Money US Tech Companies Stash Overseas To Avoid Taxes,” *Business Insider*, August 13th, Available Online at <http://www.businessinsider.com/tech-companies-hoard-cash-overseas-to-avoid-taxes-2013-8?op=1>, Accessed 08-10-2015)

U.S. companies are stockpiling really huge amounts of cash in offshore accounts.

But, it turns out, the two most vocal proponents concerning the tax rules that incentivize companies to avoid moving cash into the U.S., Cisco and Apple, aren't even the ones with the biggest stashes.

Microsoft's pile of foreign cash is way bigger.

A lot of the money sitting overseas was earned overseas, but some of it is put there through accounting methods to avoid U.S. taxes, a situation that Congress has recently been investigating. If these companies want to spend that money in the U.S. to make an acquisition or hire a bunch of new employees, Uncle Sam wants to take a 35% cut.

Cisco's CEO John Chambers and Apple's CEO Tim Cook have been trying to get Congress to change the rules, asking for a lower tax rate or even no taxes at all.

Chambers even went so far as to threaten not to make any more U.S. acquisitions or hire any more U.S. employees unless the rule is changed. He didn't make good on that. Last month, Cisco bought Maryland-based Sourcefire for $2.7 billion.

But Cisco and Apple clearly aren't the only ones with a lot at stake. Bloomberg on Tuesday published a list of the 25 companies with the biggest overseas tax hoards.

All of the top 10 are tech companies:

1. Microsoft, $76.4 billion

2. IBM, $44.4 billion

3. Cisco Systems, $41.3 billion

4. Apple, $40.4 billion

5. Hewlett-Packard, $33.4 billion

6. Google, $33.3 billion

7. Oracle, $26.2 billion

8. Dell, $19.0 billion

9. Intel, $17.5 billion

10. Qualcomm, $16.4 billion

#### Effective tax rates on tech companies are already very low.

Pyke 15 — Alan Pyke, Deputy Economic Policy Editor for *Think Progress*, former blogger and researcher with a focus on economic policy and political advertising at Media Matters for America, American Bridge 21st Century Foundation, and PoliticalCorrection.org, 2015 (“Corporate Tax Rates Aren’t The Reason American Companies Flee To Tax Havens,” *Think Progress*, February 9th, Available Online at <http://thinkprogress.org/economy/2015/02/09/3620741/inversion-mergers-not-about-tax-rate/>, Accessed 08-10-2015)

Cutting the corporate tax rate in the U.S. would do little to discourage companies from moving overseas to dodge American taxes, according to a new Reuters analysis of the half-dozen largest companies to launch so-called inversion mergers last year.

The list of six companies includes both Medtronic and Burger King, household names whose inversion plans drew significant press attention to the growth of the business practice in recent years. An inversion allows an American company to merge with a foreign entity then set the corporate headquarters of the merged firm in that other company’s home country, shifting the U.S. firm’s tax residence overseas without requiring any actual realignment of where and how the company does business. The maneuver is entirely legal and “mainly driven by efforts to shift profits out of the U.S. and to access overseas earnings at little or not cost in U.S. tax,” Reuters explains.

While proponents of a corporate tax cut or repatriation tax holiday often argue that companies undertake these elaborate schemes specifically because of the 35 percent statutory income tax rate that corporations face in the U.S. But that argument ignores the often huge gap between that on-paper tax rate and the effective rate that companies actually pay. Reuters reports that Medtronic, Burger King, and four other large companies plotting inversions actually paid an average federal tax rate of 20.3 percent from 2011 to 2013. That finding corresponds with other research on effective corporate tax rates, such as a 2014 report from Citizens for Tax Justice that found an effective tax rate of just below 20 percent for the 288 largest profitable companies in America.

Some analyses have found that a significant number of profitable companies even pay zero percent income tax rates in the U.S. thanks to creative accounting. Complex international corporate structures have let giant tech companies like Apple and Google protect hundreds of billions of dollars in revenue from taxation, and there is so much money to be made from gaming the rules of the international business tax system that even an old-guard manufacturer like Caterpillar decided to spend $50 million setting up a scheme to route profits through Switzerland and away from Internal Revenue Service hands. About $2 trillion in U.S. corporate profits is currently stashed offshore under one or another such scheme, and the Wall Street firms that help set up inversion mergers made about a billion dollars facilitating the deals in recent years.

If American companies are expatriating even though they already manage to avoid roughly half of the statutory tax burden they face, that suggests that cutting statutory rates would not produce a surge of patriotism from these firms. Burger King took significant heat from customers over its tax inversion merger with Canadian brand Tim Horton’s, but is pressing ahead anyway because the financial returns from the deal are too good to pass up.

### They Say: “Status Quo Solves”

#### The Freedom Act wasn’t enough — the plan is needed.

Castro and McQuinn 15 — Daniel Castro, Vice President of the Information Technology and Innovation Foundation—a nonprofit, non-partisan technology think tank, former IT Analyst at the Government Accountability Office, holds an M.S. in Information Security Technology and Management from Carnegie Mellon University and a B.S. in Foreign Service from Georgetown University, and Alan McQuinn, Research Assistant with the Information Technology and Innovation Foundation, holds a B.S. in Political Communications and Public Relations from the University of Texas-Austin, 2015 (“Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness,” Report by the Information Technology & Innovation Foundation, June, Available Online at <http://www2.itif.org/2015-beyond-usa-freedom-act.pdf?_ga=1.61741228.1234666382.1434075923>, Accessed 07-05-2015, p. 1)

Almost two years ago, ITIF described how revelations about pervasive digital surveillance by the U.S. intelligence community could severely harm the competitiveness of the United States if foreign customers turned away from U.S.-made technology and services.1 Since then, U.S. policymakers have failed to take sufficient action to address these surveillance concerns; in some cases, they have even fanned the flames of discontent by championing weak information security practices.2 In addition, other countries have used anger over U.S. government surveillance as a cover for implementing a new wave of protectionist policies specifically targeting information technology. The combined result is a set of policies both at home and abroad that sacrifices robust competitiveness of the U.S. tech sector for vague and unconvincing promises of improved national security.

ITIF estimated in 2013 that even a modest drop in the expected foreign market share for cloud computing stemming from concerns about U.S. surveillance could cost the United States between $21.5 billion and $35 billion by 2016.3 Since then, it has become clear that the U.S. tech industry as a whole, not just the cloud computing sector, has underperformed as a result of the Snowden revelations. Therefore, the economic impact of U.S. surveillance practices will likely far exceed ITIF’s initial $35 billion estimate. This report catalogues a wide range of specific examples of the economic harm that has been done to U.S. businesses. In short, foreign customers are shunning U.S. companies. The policy implication of this is clear: Now that Congress has reformed how the National Security Agency (NSA) collects bulk domestic phone records and allowed private firms—rather than the government—to collect and store approved data, it is time to address other controversial digital surveillance activities by the U.S. intelligence community.4

#### The Freedom Act didn’t go far enough — our evidence cites tech companies.

Volz 14 — Dustin Volz, Staff Correspondent covering tech policy for *National Journal*, holds a Master of Mass Communication, a B.A. in Journalism, and a B.A. in History from Arizona State University, 2014 (“Google, Facebook Warn NSA Bill Wouldn't Stop Mass Surveillance,” *National Journal*, May 21st, Available Online at <http://www.nationaljournal.com/tech/google-facebook-warn-nsa-bill-wouldn-t-stop-mass-surveillance-20140521>, Accessed 08-10-2015)

A day before the House will vote on a major bill designed to rein in government surveillance, a group of blue-chip tech firms are warning that the measure falls far short of what is advertised.

The Reform Government Surveillance coalition—whose members include Google, Facebook, Microsoft, AOL, Apple, Twitter, LinkedIn, DropBox, and Yahoo—issued a statement Wednesday announcing it was pulling its support of the USA Freedom Act. The legislation would take the storage of phone records out of government hands and keep them with phone companies.

But newly amended language in the bill has "moved in the wrong direction" of true surveillance reforms, the tech companies said.

"The latest draft opens up an unacceptable loophole that could enable the bulk collection of Internet users' data," the coalition said. "While it makes important progress, we cannot support this bill as currently drafted and urge Congress to close this loophole to ensure meaningful reform."

The loophole referred to is the Freedom Act's definition of a "specific selection term," which underwent changes in the newest version of the bill released this week. Earlier drafts, including the one passed two weeks ago by the House Judiciary and Intelligence committees, defined selectors as "a person, account or entity." But the new language—which adds words like "address and "device" and the non-limiting term "such as"—is seen as more broad.

Also on Wednesday, the Computer & Communications Industry Association, whose members additionally include Pandora, Samsung, Sprint and others, said it would "not support consideration or passage of the USA Freedom Act in its current form."

Several privacy groups have already revolted against the bill, citing similar concerns with the new language. Harley Geiger, senior counsel with the Center for Democracy & Technology, said the bill would allow for "an unacceptable level of surveillance." While the language could impose some limits on infinitely vast bulk collection of phone records, Geiger said, it could still potentially allow collection on areas as large as area codes or cities.

#### The Freedom Act was a net-negative because it extended unconstitutional programs.

Marthews 14 —Alex Marthews, National Chair at Restore The Fourth—a 501(c)(4) nonprofit that seeks to strengthen the Fourth Amendment to the United States Constitution and end programs that violate it, holds a Masters in Public Policy from the University of California-Berkeley and a B.A. in English from the University of Cambridge, 2014 (“We Need Real Surveillance Reform, Not The House's ‘USA Freedom Act’,” *Restore The Fourth*, May 27th, Available Online at http://restorethe4th.com/blog/we-need-real-surveillance-reform-not-the-houses-usa-freedom-act/, Accessed 06-19-2015)

Last week, the House of Representatives passed the bill called The USA Freedom Act, 303 votes to 121. Following a series of amendments, the bill as it passed in the end contained much weaker reforms than even the very modest ones it originally proposed. The Chair of the Judiciary Committee's manager's amendment removed two-thirds of its substantive reforms; the Chair of the Intelligence Committee and the White House worked hard to remove as much as possible of what remained, leaving a shell that will still permit mass surveillance.

The Fourth Amendment is clear: Mass surveillance is unconstitutional. A government search is unreasonable, and therefore unconstitutional, if it is not authorized beforehand by a warrant issued by a judge, on the basis of "probable cause" of involvement in an actual crime, supported by an "oath or affirmation, and particularly describing" the "persons or things to be seized."

That's what ought to happen. This bill, on the other hand, would allow government searches of millions of innocent people's data and movements, not based on probable cause or even reasonable suspicion of their personal involvement in a crime, but simply on any "selection term" vaguely associated with a target of surveillance.

The "selection term" could be as broad as the government likes, covering, for example, everyone born in Hawaii, or everyone with the middle name Hussein. The argument for this “reform” that supporters are touting is that this is better than the current government practice of collecting everything with no selection term at all. While that's true, it misses the larger point. The standard is individualized probable cause warrants, not “whatever is most convenient for the NSA.” A standard that can be redefined at will is marginally – if at all – better than having none.

As a terrible coda, the bill's last section extends out the sunset of crucial parts of the abusive PATRIOT Act from 2015 all the way through till 2017. Apparently, fourteen years of "emergency" privacy-violating legislation is still not enough to defeat the people who attacked us on 9/11, and we need sixteen. Given this extension, were this bill as it currently exists to be signed into law, it would be a net negative for the Fourth Amendment.

The only merit in the bill having passed is that it provides something with which the Senate's superior version of the USA Freedom Act can be reconciled in conference. We urge the Senate, and especially the Judiciary Committee, to fight hard for the Fourth Amendment in the next few months by advancing as strong a bill as possible – much stronger than this one. The USA Freedom Act, in its original form, was popular enough in the House to have passed unamended, had it been allowed to come to the floor. In the Senate, the same may well be true, and our next steps on Capitol Hill will be to work to make that happen.

When we look back in a generation at the era of our out-of-control surveillance state, we will wonder why we didn't take the Fourth Amendment as seriously as our Founders took it. We will feel shame that we were willing to sell our Bill of Rights in an attempt to thwart the same terrorists said to be attacking it. The sooner we replace this act with actual reform, the sooner our out-of-control surveillance state will finally be a thing to look back on.

### They Say: “No Competitiveness Impact”

#### Competitiveness is real and necessary for economic growth — Krugman is wrong.

Ezell 11 — Stephen Ezell, Senior Analyst with the Information Technology and Innovation Foundation—a non-partisan research and educational institute and think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity, former head of the Global Service Innovation Consortium at Peer Insight—an innovation research and consulting firm, holds a B.S. from the School of Foreign Service at Georgetown University with an Honors Certificate from Georgetown’s Landegger International Business Diplomacy program, 2011 (“Krugman Flat Wrong that Competitiveness is a Myth,” *The Innovation Files*, January 25th, Available Online at http://www.innovationfiles.org/krugman-flat-wrong-that-competitiveness-is-a-myth/, Accessed 08-11-2013)

In a Sunday op-ed in the New York Times, “The Competition Myth,” Paul Krugman argues that “competitiveness” is a myth, a bad metaphor, a fundamentally misleading goal, and that it doesn’t make “any sense to view our current woes as stemming from a lack of competitiveness.” About this, Krugman is absolutely, dead-on, 100 percent wrong. For the reality is that the perilous state of the American economy has everything to do with faltering U.S. competitiveness—and more than that—much to do with the abject refusal of neoclassical economists like Krugman himself to recognize that competitiveness is an issue, that countries compete, and that U.S. economic policy should be directly designed to bolster the competitiveness of U.S. organizations and industries.

Krugman’s like the young boy who finds himself losing a race with his buddies and who stops and yells, “I’m not racing!” Better to simply pretend that you aren’t racing than to lose. For if you can convince yourself that you aren’t in a race, you sure sleep better at night than if you admitted you were in a competition and were losing…That is, until you wake up one morning having lost ten million manufacturing jobs, have 10% unemployment, and have a horrifically bad trade balance. Moreover, when you refuse to even believe that you’re in a race, it’s a sure sign that you’re going to lose, as evidenced by the fact that the United States ranks 40th of out of 40 countries and regions in improving its innovation competitiveness over the past decade, as ITIF’s Atlantic Century report found.

#### Government policies are needed to support innovation and global competitiveness — Krugman is wrong.

Ezell 11 — Stephen Ezell, Senior Analyst with the Information Technology and Innovation Foundation—a non-partisan research and educational institute and think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity, former head of the Global Service Innovation Consortium at Peer Insight—an innovation research and consulting firm, holds a B.S. from the School of Foreign Service at Georgetown University with an Honors Certificate from Georgetown’s Landegger International Business Diplomacy program, 2011 (“Krugman Flat Wrong that Competitiveness is a Myth,” *The Innovation Files*, January 25th, Available Online at http://www.innovationfiles.org/krugman-flat-wrong-that-competitiveness-is-a-myth/, Accessed 08-11-2013)

Krugman’s misguided perspective on competitiveness dates back to a 1994 Foreign Affairs article he wrote, “Competitiveness, A Dangerous Obsession,” in which he made the utterly astounding contention that, “The notion that nations compete is incorrect…countries are not to any important degree in competition with each other.” Like many U.S. elites, Krugman simply refuses to recognize that the U.S. is in global economic—and innovation—competition with other nations. This view remains readily apparent in the NYT article, where Krugman contends that “we’re in a mess because we had a financial crisis, not because American companies have lost their ability to compete with foreign rivals.” Krugman goes on, “But isn’t it at least somewhat useful to think of our nation as if it were America Inc., competing in the global marketplace? No.” So again, only companies compete with one another; and it’s not helpful to think of the U.S. as competing. Moreover, our companies are competing fine…so the problem must be a financial crisis (caused by a few malfeasant firms in the financial sector).

But the reality is that countries do compete and seek to win in the highest-value-added sectors of economic activity. In fact, Krugman dramatically underestimates the impact that countries’ strategies—whether fair and consistent with global rules or not—can have in shifting comparative advantage in critical technology-based sectors their way. There are two aspects to this competition worth discussing.

First, an increasingly globalized economy means that countries have become price takers—not price makers—on international markets. In other words, companies now shop the world for the best locations to situate their globally mobile innovation activity, such as where to locate R&D facilities or build new factories. These companies look for which countries offer the best pools of talent (skilled scientists and engineers and a highly educated, highly skilled populace); which have the most attractive tax laws in terms of low corporate tax rates and generous and stable R&D tax credits; which have the most robust physical and digital infrastructures, the latter especially in terms of fixed and mobile broadband, electric smart grids, or intelligent transportation systems; which have the best high-skill immigration policies; the deepest pools of capital; the best funding for R&D; the easiest place to start a business; etc.. Collectively, these attributes constitute a nation’s innovation ecosystem, and governments play a legitimate and crucial role in shaping their nation’s innovation ecosystem. In fact, it is these innovation ecosystems on which countries increasingly compete. As Greg Tassey, a Senior Economist at the Department of Commerce National Institute of Standards and Technology argues, “Competition among governments has become a critical factor in determining which economies win and which lose in the increasingly intense process of creative destruction.”

But Krugman refuses to see this because “only companies compete.” This raises a consequent challenge again explained by Tassey: “Another underlying problem is that U.S. firms are attempting to compete largely as independent entities against a growing number of national economies in Europe and Asia in which government, industry, and a broad infrastructure (technical, education, economic, and information) are evolving into increasingly effective technology-based ecosystems.” Or as Wayne Johnson, Hewlett Packard’s Director of Worldwide Strategic University Customer Relations, said at a 2008 conference, “We in the United States find ourselves in competition not only with individuals, companies, and private institutions, but also with governments and mixed government-private collaborations.” In other words, the United States has a collection of players (businesses) running around competing against other players (nations) that are well equipped, well coached, and running specific plays.

#### High tech competitiveness is key to U.S. leadership.

Segal 4 — Adam Segal, Maurice R. Greenberg Senior Fellow in China Studies at the Council on Foreign Relations, 2004 (“Is America Losing Its Edge?; Innovation in a Globalized World,” *Foreign Affairs*, January-February, Available Online to Subscribing Institutions via Lexis-Nexis)

The United States' global primacy depends in large part on its ability to develop new technologies and industries faster than anyone else. For the last five decades, U.S. scientific innovation and technological entrepreneurship have ensured the country's economic prosperity and military power. It was Americans who invented and commercialized the semiconductor, the personal computer, and the Internet; other countries merely followed the U.S. lead.

Today, however, this technological edge—so long taken for granted—may be slipping, and the most serious challenge is coming from Asia. Through competitive tax policies, increased investment in research and development(R&D), and preferential policies for science and technology (S&T) personnel, Asian governments are improving the quality of their science and ensuring the exploitation of future innovations. The percentage of patents issued to and science journal articles published by scientists in China, Singapore, South Korea, and Taiwan is rising. Indian companies are quickly becoming the second-largest producers of application services in the world, developing, supplying, and managing database and other types of software for clients around the world. South Korea has rapidly eaten away at the U.S. advantage in the manufacture of computer chips and telecommunications software. And even China has made impressive gains in advanced technologies such as lasers, biotechnology, and advanced materials used in semiconductors, aerospace, and many other types of manufacturing.

Although the United States' technical dominance remains solid, the globalization of research and development is exerting considerable pressures on the American system. Indeed, as the United States is learning, globalization cuts both ways: it is both a potent catalyst of U.S. technological innovation and a significant threat to it. The United States will never be able to prevent rivals from developing new technologies; it can remain dominant only by continuing to innovate faster than everyone else. But this won't be easy; to keep its privileged position in the world, the United States must get better at fostering technological entrepreneurship at home.

### They Say: “No U.S. Leadership Impact”

#### Strong *relative* growth is crucial to maintain U.S. military power.

Manzi 11 — Jim Manzi, Senior Fellow at the Manhattan Institute, Chief Executive Officer of Applied Predictive Technologies—an applied artificial intelligence software company, holds a B.S. in Mathematics from the Massachusetts Institute of Technology, 2011 (“On Not Ceding ‘Competitiveness’ to the Left,” *National Review Online*, September 16th, Available Online at http://www.nationalreview.com/corner/277406/not-ceding-competitiveness-left-jim-manzi, Accessed 08-11-2013)

An idiosyncrasy of contemporary American political debate is that concern with “competitiveness” is so often associated with the Democratic party, and is often used as a code word for industrial policy and a host of social engineering initiatives. I think it is a mistake for the right to concede this territory.

You link to a quote from Paul Krugman, supposedly discrediting the idea of national competitiveness:

International trade, unlike competition among businesses for a limited market, is not a zero-sum game in which one nation’s gain is another’s loss. It is [a] positive-sum game, which is why the word “competitiveness” can be dangerously misleading when applied to international trade.

But this doesn’t make a lot of sense to me. Sure, some product markets are somewhat limited, but competition between companies as a whole is not generally “zero-sum” either — hence, economic growth.

International trade can make both parties better off than they would be without the exchange. But there are still relative winners and losers. Some societies are populated by lots of people with high-wage jobs, nice houses, and good schools, and other societies are populated by lots of people hustling for tips from vacationers from the first kind of society. Over time, people who spend their working hours generating goods or services that they can sell for a big margin versus the costs of the required inputs will tend to live in the first kind of society. Nothing is forever in this world, but I want America to remain in that camp for a very long time.

In the most important sense, competitiveness is relative productivity. And relative productivity is likely to matter a lot, because it will materially influence future absolute wealth by affecting the flow of global technology and innovation. But relative productivity and the wealth wealth it produces also matter in and of themselves. First, they will impact the global prestige and success of the Western idea of the open society which we value independently of its economic benefits — people naturally look to economically successful societies for lessons and inspiration. Second, maintenance of a very large GDP per capita gap between the West and the rest of the world will be essential to maintaining relative Western aggregate GDP, and therefore, long-run military power.

In sum, we want the rest of the world to get richer, but we want to stay much richer than they get.

#### Maintaining strong economic growth is vital to prevent great power conflict — *relative* growth is key.

Goldstein 7 — Avery Goldstein, David M. Knott Professor of Global Politics and International Relations at the University of Pennsylvania, Associate Director of the Christopher H. Browne Center for International Politics, Senior Fellow at the Foreign Policy Research Institute, holds a Ph.D. from the University of California-Berkeley, 2007 (“Power transitions, institutions, and China's rise in East Asia: Theoretical expectations and evidence,” *Journal of Strategic Studies*, Volume 30, Number 4-5, August-October, Available Online to Subscribing Institutions via Taylor & Francis Online, p. 647-648)

Two closely related, though distinct, theoretical arguments focus explicitly on the consequences for international politics of a shift in power between a dominant state and a rising power. In War and Change in World Politics, Robert Gilpin suggested that peace prevails when a dominant state’s capabilities enable it to ‘govern’ an international order that it has shaped. Over time, however, as economic and technological diffusion proceeds during eras of peace and development, other states are empowered. Moreover, the burdens of international governance drain and distract the reigning hegemon, and challengers eventually emerge who seek to rewrite the rules of governance. As the power advantage of the erstwhile hegemon ebbs, it may become desperate enough to resort to the ultima ratio of international politics, force, to forestall the increasingly urgent demands of a rising challenger. Or as the power of the challenger rises, it may be tempted to press its case with threats to use force. It is the rise and fall of the great powers that creates the circumstances under which major wars, what Gilpin labels ‘hegemonic wars’, break out.13

Gilpin’s argument logically encourages pessimism about the implications of a rising China. It leads to the expectation that international trade, investment, and technology transfer will result in a steady diffusion of American economic power, benefiting the rapidly developing states of the world, including China. As the US simultaneously scurries to put out the many brushfires that threaten its far-flung global interests (i.e., the classic problem of overextension), it will be unable to devote sufficient resources to maintain or restore its former advantage over emerging competitors like China. While the erosion of the once clear American advantage plays itself out, the US will find it ever more difficult to preserve the order in Asia that it created during its era of preponderance. The expectation is an increase in the likelihood for the use of force – either by a Chinese challenger able to field a stronger military in support of its demands for greater influence over international arrangements in Asia, or by a besieged American hegemon desperate to head off further decline. Among the trends that alarm [end page 647] those who would look at Asia through the lens of Gilpin’s theory are China’s expanding share of world trade and wealth (much of it resulting from the gains made possible by the international economic order a dominant US established); its acquisition of technology in key sectors that have both civilian and military applications (e.g., information, communications, and electronics linked with the ‘revolution in military affairs’); and an expanding military burden for the US (as it copes with the challenges of its global war on terrorism and especially its struggle in Iraq) that limits the resources it can devote to preserving its interests in East Asia.14

Although similar to Gilpin’s work insofar as it emphasizes the importance of shifts in the capabilities of a dominant state and a rising challenger, the power-transition theory A. F. K. Organski and Jacek Kugler present in The War Ledger focuses more closely on the allegedly dangerous phenomenon of ‘crossover’– the point at which a dissatisfied challenger is about to overtake the established leading state.15 In such cases, when the power gap narrows, the dominant state becomes increasingly desperate to forestall, and the challenger becomes increasingly determined to realize the transition to a new international order whose contours it will define.

#### U.S. relative decline creates a power vacuum that risks war.

Friedberg and Schoenfeld 8 — Aaron Friedberg, Professor of Politics and International Relations at the Woodrow Wilson School at Princeton University, and Gabriel Schoenfeld, Senior Editor of Commentary and Visiting Scholar at the Witherspoon Institute—an independent research center in Princeton, NJ, 2008 (“The Dangers of a Diminished America,” *Wall Street Journal*, October 21st, Available Online at http://online.wsj.com/article/SB122455074012352571.html, Accessed 11-11-2008)

If America now tries to pull back from the world stage, it will leave a dangerous power vacuum. The stabilizing effects of our presence in Asia, our continuing commitment to Europe, and our position as defender of last resort for Middle East energy sources and supply lines could all be placed at risk.

In such a scenario there are shades of the 1930s, when global trade and finance ground nearly to a halt, the peaceful democracies failed to cooperate, and aggressive powers led by the remorseless fanatics who rose up on the crest of economic disaster exploited their divisions. Today we run the risk that rogue states may choose to become ever more reckless with their nuclear toys, just at our moment of maximum vulnerability.

The aftershocks of the financial crisis will almost certainly rock our principal strategic competitors even harder than they will rock us. The dramatic free fall of the Russian stock market has demonstrated the fragility of a state whose economic performance hinges on high oil prices, now driven down by the global slowdown. China is perhaps even more fragile, its economic growth depending heavily on foreign investment and access to foreign markets. Both will now be constricted, inflicting economic pain and perhaps even sparking unrest in a country where political legitimacy rests on progress in the long march to prosperity.

None of this is good news if the authoritarian leaders of these countries seek to divert attention from internal travails with external adventures.

As for our democratic friends, the present crisis comes when many European nations are struggling to deal with decades of anemic growth, sclerotic governance and an impending demographic crisis. Despite its past dynamism, Japan faces similar challenges. India is still in the early stages of its emergence as a world economic and geopolitical power.

What does this all mean? There is no substitute for America on the world stage. The choice we have before us is between the potentially disastrous effects of disengagement and the stiff price tag of continued American leadership.

## 2AC — Cybersecurity Advantage

### They Say: “Golden Key Solves”

#### A Golden Key is mathematically impossible — *experts*.

Geller 15 — Eric Geller, Deputy Morning Editor at *The Daily Dot*—the “hometown newspaper of the Internet,” 2015 (“The rise of the new Crypto War,” *The Daily Dot*, July 10th, Available Online at <http://www.dailydot.com/politics/encryption-crypto-war-james-comey-fbi-privacy/>, Accessed 07-20-2015)

To researchers who have spent their careers studying code, the FBI’s belief that it can shut down the development of strong cryptography is ludicrous. Code, after all, is just math.

“This all requires an idea that people just won’t innovate in areas where the government doesn’t like them to,” said Cohn. “And that’s really never been the case.”

Hall said, “You’re basically trying to prevent people from doing certain kinds of math.”

Philip Zimmerman, the inventor of the widely used PGP encryption scheme, neatly summed up the problem with government encryption limits when he told a 1996 Senate subcommittee hearing, “Trying to stop this is like trying to legislate the tides and the weather.”

The mathematical nature of encryption is both a reassurance that it cannot be banned and a reminder that it cannot be massaged to fit an agenda—even agendas ostensibly meant to save lives. Software engineers simply cannot build backdoors that do what the FBI wants without serious security vulnerabilities, owing to the fundamental mathematical nature of cryptography. It is no more possible for the FBI to design a secure backdoor than it is for the National Weather Service to stop a hurricane in its tracks.

“No amount of presto change-o is going to change the math,” Cohn said. “Some people say time is on their side; I think that math is on our side when it comes to crypto.”

\* Cohn = Cindy Cohn, Executive Director and former Legal Director and General Counsel of the Electronic Frontier Foundation, holds a J.D. from the University of Michigan Law School; Hall = Joseph Hall, chief technologist at the Center for Democracy & Technology

#### Creating a “law enforcement-only” backdoor is *technically* impossible.

Schneier 15 — Bruce Schneier, Chief Technology Officer for Counterpane Internet Security, Fellow at the Berkman Center for Internet and Society at Harvard Law School, Program Fellow at the New America Foundation's Open Technology Institute, Board Member of the Electronic Frontier Foundation, Advisory Board Member of the Electronic Privacy Information Center, interviewed by Rob Price, 2015 (“Bruce Schneier: David Cameron's proposed encryption ban would 'destroy the internet',” *Business Insider*, July 6th, Available Online at <http://www.businessinsider.com/bruce-schneier-david-cameron-proposed-encryption-ban-destroy-the-internet-2015-7>, Accessed 07-20-2015)

BI: Is there really no way to keep users' data secure while providing backdoors to law enforcement?

BS: Yes, there really is no way.

Think of it like this. Technically, there is no such thing as a "backdoor to law enforcement." Backdoor access is a technical requirement, and limiting access to law enforcement is a policy requirement. As an engineer, I cannot design a system that works differently in the presence of a particular badge or a signed piece of paper. I have two options. I can design a secure system that has no backdoor access, meaning neither criminals nor foreign intelligence agencies nor domestic police can get at the data. Or I can design a system that has backdoor access, meaning they all can. Once I have designed this less-secure system with backdoor access, I have to install some sort of policy overlay to try to ensure that only the police can get at the backdoor and only when they are authorized. I can design and build procedures and other measures intended to prevent those bad guys from getting access, but anyone who has followed all of the high-profile hacking over the past few years knows how futile that would be.

There is an important principle here: we have one world and one Internet. Protecting communications means protecting them from everybody. Making communications vulnerable to one group means making them vulnerable to all. There just isn't any way around that.

#### Prefer our evidence — we cite the world’s leading experts. They cite people who don’t understand math.

Crypto Experts 15 — Harold Abelson, Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology, Fellow of The Institute of Electrical and Electronics Engineers, Founding Director of Creative Commons and the Free Software Foundation, holds a Ph.D. in Mathematics from the Massachusetts Institute of Technology, et al., with Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner, qualifications of these co-authors available upon request, 2015 (“Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications,” Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report (MIT-CSAIL-TR-2015-026), July 6th, Available Online at http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf, Accessed 07-20-2015, p. 1)

Political and law enforcement leaders in the United States and the United Kingdom have called for Internet systems to be redesigned to ensure government access to information — even encrypted information. They argue that the growing use of encryption will neutralize their investigative capabilities. They propose that data storage and communications systems must be designed for exceptional access by law enforcement agencies. These proposals are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm.

As computer scientists with extensive security and systems experience, we believe that law enforcement has failed to account for the risks inherent in exceptional access systems. Based on our considerable expertise in real-world applications, we know that such risks lurk in the technical details. In this report we examine whether it is technically and operationally feasible to meet law enforcement’s call for exceptional access without causing large-scale security vulnerabilities. We take no issue here with law enforcement’s desire to execute lawful surveillance orders when they meet the requirements of human rights and the rule of law. Our strong recommendation is that anyone proposing regulations should first present concrete technical requirements, which industry, academics, and the public can analyze for technical weaknesses and for hidden costs.

### They Say: “Alternate Causality – Workforce”

#### The workforce shortage will resolve itself — it’s overblown.

Halzack 14 — Sarah Halzack, Reporter for *The Washington Post*, 2014 (“Shortage of cybersecurity workers is a problem that will solve itself, study says,” *Washington Post*, June 27th, Available Online at <https://www.washingtonpost.com/business/capitalbusiness/an-argument-that-the-shortage-of-cyber-workers-is-a-problem-that-will-solve-itself/2014/06/27/dbab364a-fe00-11e3-8176-f2c941cf35f1_story.html>, Accessed 08-12-2015)

Talk to any recruiter in the Washington region and they will tell you cybersecurity jobs are among the most difficult for them to fill. Workers with the right skills are relatively hard to come by, and in a labor market dominated by the federal government and its contractors, they are in especially high demand.

Companies, universities and government entities are all focused on finding ways to close the gap: Educational partnerships. Hackathon competitions. Internal corporate training programs. A regional task force.

But the Rand Corp. argues in a study released last week that this problem — which has prompted so much action — will solve itself.

Study authors Martin C. Libicki, David Senty and Julia Pollak examined existing studies on the cybersecurity workforce; interviewed government agencies, defense contractors and security firms; and looked at labor economics research to try to get a handle on the nature and scope of the cybersecurity worker shortage.

Based on that compendium of information, they predict that the high levels of compensation in this industry will be enough to lure more workers to its ranks. As the supply of these skilled workers increases over the long term, the pay packages will begin to be less eye-popping.

The report forecasts that cyber­security pay will not dip below where it was in 2007, when a rash of high-profile Internet attacks made this field seem more essential.

But the authors do predict that pay will cool off from where it is now.

The authors say that this balance “may take some time to achieve,” and they are careful to state that, indeed, demand for cyber professionals is intense right now.

“Our assessment does not refute this position — good cybersecurity professionals are in high demand — but it suggests that these fears be tempered, that many forces are at work to fix the situation, and that the case for additional effort beyond that is not particularly strong,” they write.

#### Attacks on encryption make the U.S. vulnerable to cyber attacks — it’s the comparatively largest factor.

Snowden 15 — Edward Snowden, NSA whistleblower, Member of the Board of Directors of the Freedom of the Press Foundation, former Central Intelligence Agency officer and National Security Agency contractor, interviewed by James Bamford, author and journalist who specializes in U.S. intelligence agencies including the National Security Agency, former Distinguished Visiting Professor at the University of California-Berkeley, 2015 (“Exclusive: Edward Snowden on Cyber Warfare,” *Nova Next*, January 8th, Available Online at http://www.pbs.org/wgbh/nova/next/military/snowden-transcript/, Accessed 08-12-2015)

The community of technical experts who really manage the internet, who built the internet and maintain it, are becoming increasingly concerned about the activities of agencies like the NSA or Cyber Command, because what we see is that defense is becoming less of a priority than offense. There are programs we’ve read about in the press over the last year, such as the NSA paying RSA $10 million to use an insecure encryption standard by default in their products. That’s making us more vulnerable not just to the snooping of our domestic agencies, but also foreign agencies.

We saw another program called Bullrun which subverted the—which subverts—it continues to subvert similar encryption standards that are used for the majority of e-commerce all over the world. You can’t go to your bank and trust that communication if those standards have been weakened, if those standards are vulnerable. And this is resulting in a paradigm where these agencies wield tremendous power over the internet at the price of making the rest of their nation incredibly vulnerable to the same kind of exploitative attacks, to the same sort of mechanisms of cyber-attack.

And that means while we may have a real advantage when it comes to eavesdropping on the military in Syria or trade negotiations over the price of shrimp in Indonesia—which is an actually real anecdote—or even monitoring the climate change conference, it means it results. It means we end up living in an America where we no longer have a National Security Agency. We have a national surveillance agency. And until we reform our laws and until we fix the excesses of these old policies that we inherited in the post-9/11 era, we’re not going to be able to put the security back in the NSA.

#### Encryption is vital to *every aspect* of cybersecurity.

Schneier 15 — Bruce Schneier, Chief Technology Officer for Counterpane Internet Security, Fellow at the Berkman Center for Internet and Society at Harvard Law School, Program Fellow at the New America Foundation's Open Technology Institute, Board Member of the Electronic Frontier Foundation, Advisory Board Member of the Electronic Privacy Information Center, interviewed by Rob Price, 2015 (“Bruce Schneier: David Cameron's proposed encryption ban would 'destroy the internet',” *Business Insider*, July 6th, Available Online at <http://www.businessinsider.com/bruce-schneier-david-cameron-proposed-encryption-ban-destroy-the-internet-2015-7>, Accessed 07-20-2015)

BI: Are there any less obvious ways in which encryption helps people on a day-to-day basis?

BS: Encryption secures everything we do on the Internet. It secures our commerce. It secures our communications. It secures our critical infrastructure. It secures our persons from criminal attack, and it secures our countries from nation-state attack. In many countries, it helps journalists, dissidents, and human rights workers stay alive. In a world of pretty bad computer security, it is the one thing that works well.

### They Say: “No Cyber Impact”

#### Cybersecurity is the most pressing threat to national security — official threat assessment.

Fadilpasic 15 — Sead Fadilpasic, freelance journalist and Contributor to *IT Pro Portal*, 2015 (“US identifies cyber attacks as biggest national threat,” *IT Pro Portal*, February 27th, Available Online at <http://www.itproportal.com/2015/02/27/us-identifies-cyber-attacks-biggest-national-threat/>, Accessed 08-12-2015)

Forget school shootings, bomb threats, planes flying into buildings, tsunamis and hurricanes – cyber attacks are the biggest threat to the US.

National intelligence director James Clapper says attacks by politically and criminally motivated actors are the biggest threat to US national security.

“Cyber threats to US national and economic security are increasing in frequency, scale, sophistication and severity of impact,” he said in the latest annual threat assessment delivered to Congress (PDF).

#### Cybersecurity is a huge threat to national security — it *outweighs* terrorism.

CSM 14 — Christian Science Monitor, 2014 (“Feds hacked: Is cybersecurity a bigger threat than terrorism?,” Byline Harry Bruinius, November 10th, Available Online at <http://www.csmonitor.com/USA/2014/1110/Feds-hacked-Is-cybersecurity-a-bigger-threat-than-terrorism-video>, Accessed 07-06-2015)

While the terrestrial fears of terrorism and Ebola have dominated headlines, American leaders are fretting about what may be even more serious virtual threats​ to the nation’s security.

This year, hundreds of millions of private records have been exposed in an unprecedented number of cyberattacks on both US businesses and the federal government.

On Monday, just as President Obama arrived in Beijing to being a week-long summit with regional leaders, Chinese hackers are suspected to have breached the computer networks of the US Postal Service, leaving the personal data of more than 800,00 employees and customers compromised, The Washington Post reports.

The data breach, which began as far back as January and lasted through mid-August, potentially exposed 500,000 postal employees’ most sensitive personal information, including names, dates of birth, and Social Security numbers, the Postal Service said in a statement Monday. The data of customers who used the Postal Service’s call center from January to August may have also been exposed.

"The FBI is working with the United States Postal Service to determine the nature and scope of this incident," the federal law enforcement agency said in a statement Monday. Neither the FBI nor the Postal Service, however, confirmed it was the work of Chinese hackers.

The breach did not expose customer payment or credit card information, the Postal Service said, but hackers did gain access to its computer networks at least as far back as January. The FBI informed the Postal Service of the hack in mid-September.

“It is an unfortunate fact of life these days that every organization connected to the Internet is a constant target for cyber intrusion activity,” said Postmaster General Patrick Donahoe in a statement. “The United States Postal Service is no different. Fortunately, we have seen no evidence of malicious use of the compromised data and we are taking steps to help our employees protect against any potential misuse of their data.”

But the reported breach comes as both intelligence officials and cybersecurity experts say computer hackers now pose a greater threat to national security than terrorists.

Since 2006, cyber-intruders have gained access to the private data of nearly 90 million people in federal networks, the Associated Press reported in a major investigation published Monday.

Hackers have also accessed 255 million customer records in retail networks during this time, 212 million customer records in financial and insurance industry servers​,​ as well as 13 million ​records of those in ​educational institutions, the AP reported.

“The increasing number of cyber-attacks in both the public and private sectors is unprecedented and poses a clear and present danger to our nation’s security,” wrote Rep. Elijah Cummings (D) of Maryland, ranking member of the House Committee on Oversight and Government Reform, in a letter to Postmaster General Donahoe on Monday.

#### The cybersecurity costs of weakened encryption are massive and outweigh terrorism.

Doctorow 14 — Cory Doctorow, journalist and science fiction author, Co-Editor of *Boing Boing*, Fellow at the Electronic Frontier Foundation, former Canadian Fulbright Chair for Public Diplomacy at the Center on Public Diplomacy at the University of Southern California, recipient of the Electronic Frontier Foundation’s Pioneer Award, 2014 (“A World of Control and Surveillance,” *Information Doesn't Want to Be Free: Laws for the Internet Age*, Published by McSweeney’s, ISBN 9781940450285, p. 125-126)

The Edward Snowden leaks left much of the world in shock. Even the most paranoid security freaks were astounded to learn about the scope of the surveillance apparatus that had been built by the NSA, along with its allies in the "Five Eyes" countries (the UK, Canada, New Zealand, and Australia).

The nontechnical world was most shocked by the revelation that the NSA was snaffling up such unthinkable mountains of everyday communications. In some countries, the NSA is actively recording every single cell-phone conversation, putting millions of indisputably innocent people under surveillance without even a hint of suspicion.

But in the tech world, the real showstopper was the news that the NSA and the UK's spy agency, the GCHQ, had been spending $250 million a year on two programs of network and computer sabotage — BULLRUN, in the USA, and EDGEHILL, in the UK. Under these programs, technology companies are bribed, blackmailed, or tricked into introducing deliberate flaws into their products, so that spies can break into them and violate their users' privacy. The NSA even sabotaged U.S. government agencies, such as the National Institute for Standards and Technology (NIST), a rock-ribbed expert body that produces straightforward engineering standards to make sure that our digital infrastructure doesn't fall over. NIST was forced to recall one of its cryptographic standards after it became apparent that the NSA had infiltrated its process and deliberately weakened the standard — an act akin to deliberately ensuring that the standard for electrical wiring was faulty, so that you could start house fires in the homes of people you wanted to smoke out during armed standoffs.

The sabotage shocked so many technology experts because they understood that there was no such thing as a security flaw that could be [end page 125] exploited by "the good guys" alone. If you weaken the world's computer security — the security of our planes and nuclear reactors, our artificial hearts and our thermostats, and, yes, our phones and our laptops, devices that are privy to our every secret — then no amount of gains in the War on Terror will balance out the costs we'll all pay in vulnerability to crooks, creeps, spooks, thugs, perverts, voyeurs, and anyone else who independently discovers these deliberate flaws and turns them against targets of opportunity.

### They Say: “No Grid Collapse”

#### The grid is extremely vulnerable to a cyber attack — expert consensus.

Roberts 14 — Paul F. Roberts, Correspondent for *Passcode*—the *Christian Science Monitor* technology policy blog, Founder and Editor in Chief of *The Security Ledger*—an independent security website that explores the intersection of cyber security with the Internet of Things, 2014 (“If cyberwar erupts, America's electric grid is a prime target,” *Passcode*—a *Christian Science Monitor* blog, December 23rd, Available Online at <http://www.csmonitor.com/World/Passcode/2014/1223/If-cyberwar-erupts-America-s-electric-grid-is-a-prime-target>, Accessed 08-12-2015)

Even as the Obama administration seeks to tamp down talk of computer wars and retaliation, experts agree that, when cyberwar does reach our shores, the most likely targets won't be Hollywood movie studios. Instead, it may be the critical infrastructure – the systems that keep our society and economy humming.

In fact, in just the past three months, senior US government officials have warned of computer attacks on the nation’s critical infrastructure with growing urgency. Attacks are not just possible, they are already happening, they say.

First came an alert in October from the Department of Homeland Security’s Industrial Control System Computer Emergency Response Team (ICS-CERT). It warned critical infrastructure operators about malicious software known as BlackEnergy used in attacks on industrial control systems.

Then, on Nov. 20, the government’s most senior cyber warrior, the National Security Agency's chief Adm. Michael Rogers, told Congress that the government was aware of wide-spread and concerted efforts by nation-state actors to use malicious software and online attacks to infiltrate, study, and – potentially – cripple US critical infrastructure, including the nation’s electric grid.

"There are those industrial control systems that can shut down and forestall our ability to operate … basic infrastructure, whether it’s generating power across this nation, whether it’s moving water and fuel,” Admiral Rogers told the House Select Intelligence Committee.

At the top of the list of targets for a crippling hack: North America's vast and vulnerable electrical grid.

Rogers, who also serves as the head of US Cyber Command, gave a dire assessment of the security of the US grid to an audience of energy company executives in October. In that speech, Rogers said that the power infrastructure was not designed to stand up to today's attacks. "Power ... is one of the segments that concerns me the most," he said, according to a report by CNN, which obtained a transcript of the speech.

For security experts who have been working within the power sector, however, the dire warnings are not news. They would not have been news last year, or the year before. In fact, Rogers’ dim assessment of the US power sector’s readiness to face and withstand a cyberattack has been shared and articulated within the power industry for seven years.

#### A devastating cyber attack on the grid is likely.

Gertz 14 — Bill Gertz, National Security Columnist for *The Washington Times*, Senior Editor at *The Washington Free Beacon*, former Guest Lecturer at the FBI National Academy, the Central Intelligence Agency, the National Defense University, and the Brookings Institution, 2014 (“Inside the Ring: U.S. power grid defenseless from physical and cyber attacks,” *The Washington Times*, April 16th, Available Online at <http://www.washingtontimes.com/news/2014/apr/16/inside-the-ring-us-power-grid-defenseless-from-att/?page=all>, Accessed 08-12-2015)

The U.S. electrical power grid is vulnerable to cyber and physical attacks that could cause devastating disruptions throughout the country, federal and industry officials told Congress recently.

Gerry Cauley, president of the North American Electric Reliability Corp., said that several — if not all — other critical U.S. infrastructures depend on electricity, and that he is “deeply concerned” about attacks, extreme weather and equipment failures causing power outages.

“I am most concerned about coordinated physical and cyber attacks intended to disable elements of the power grid or deny electricity to specific targets, such as government or business centers, military installations, or other infrastructures,” Mr. Cauley told the Senate Energy and Natural Resources Committee last Thursday.

Mr. Cauley said the April 2013 attack on a California electrical power substation by unidentified gunmen did not result in power outages, but highlighted the vulnerability of the country’s three-sector power grid.

The incident at the Metcalf substation in Northern California “demonstrates that attacks are possible and have the potential to cause significant damage to assets and disrupt customer service,” he said.

Cheryl A. LaFleur, acting chairman of the Federal Energy Regulatory Commission who testified at the Senate hearing, said the Metcalf attack led federal authorities to conduct a 13-city campaign to warn utilities about the need for better security.

Ms. LaFleur said cyber threats to electrical infrastructure are “fast-changing,” as she called for better information-sharing about threats between government and industry.

Sue Kelly, head of the American Public Power Association of more than 2,000 U.S. electric utilities, testified about the growing danger of cyberattacks against the power grid.

“The threat of cyberattack is relatively new compared to long-known physical threats, but an attack with operational consequences could occur and cause disruptions in the flow of power if malicious actors are able to hack into the data and control systems used to operate our electric generation and transmission infrastructure,” Ms. Kelly said.

To date, security measures have prevented a successful cyberattack on the bulk electric system, she said.

An Energy Department-sponsored study published last fall said the U.S. power grid is vulnerable to catastrophic disruption by nation states like China and North Korea, terrorist groups like al Qaeda, and non-state criminals.

The 269-page study “Electric Sector Failure Scenarios and Impact Analyses” was published in September by the National Electric Sector Cybersecurity Organization Resource, a non-government group of industry and security specialists.

A malicious software cyberattack on the power grid’s Distributed Energy Resource Management System (DERMS), which manages requests and commands for the power system, would damage transformers that are costly and difficult to replace.

Cyberattacks against computers that distribute electrical power over wide areas could be jammed or disrupted through wireless signals.

And cyber attackers could cause widespread power outages or cascading power failures by gaining access to distribution systems and equipment via remote hacking.

“After gaining the required access, the threat agent manufactures an artificial cascade through sequential tripping of select critical feeders and components, causing automated tripping of generation sources due to power and voltage fluctuations,” the report said. “A blackout of varying degree and potential equipment damage ensues.”

According to the report, nation state threats to the grid include China, North Korea and Cuba. Among the cyber terrorist threats listed: al Qaeda and the Afghan Taliban, the Pakistani group Lashkar-e-Taibi, and the Palestinian group Hamas. Domestic threats include “lone wolf” extremists, ecoterrorists among Earth First and Greenpeace, U.S. separatist groups, and militias and hate groups, the report said.

#### Many actors have the motivation and capability to attack the grid.

Harris 14 — Shane Harris, Senior Staff Writer covering intelligence and cyber security at *Foreign Policy*, received the Gerald R. Ford Prize for Distinguished Reporting on National Defense, 2014 (“U.S. Electrical Grid Vulnerable to Cyberthreats and Physical Attack, Study Finds,” *The Complex*—a *Foreign Policy* blog, July 15th, Available Online at <http://foreignpolicy.com/2014/07/15/u-s-electrical-grid-vulnerable-to-cyberthreats-and-physical-attack-study-finds/>, Accessed 08-12-2015)

The United States’ electrical grid is vulnerable to disruptive attacks by computer hackers that could shut off power to vital sectors of the economy and key public utilities, giving potential adversaries a new way of hitting the United States, according to a new study by a Washington think tank.

The report by the nonpartisan Center for the Study of the Presidency and Congress comes as lawmakers on Capitol Hill consider legislation that would beef up cybersecurity standards for critical infrastructure like the power grid while also encouraging the government and private sector to share more information about cyberthreats and thwarted attacks. That legislation has been in the works for years but has been blocked by business interests that see mandatory security standards as an improper attempt by Washington to dictate how companies manage privately owned facilities in industries ranging from telecommunications to the financial and transportation sectors.

Cyberattacks on the power grid have long been seen as a kind of doomsday scenario that could cripple large swaths of the U.S. economy and society, leading to lengthy power outages and wide-scale panic. The new report identifies a range of potential cyberattackers that have both the motive and the capability to take down portions of the power grid, from countries like China and Russia to terrorist organizations and organized criminals.

"For countries like Iran and North Korea, grid vulnerabilities serve as targets for attacks aimed at disruption or asymmetric effects in terms of national, economic, and civil security," the report’s authors write, referring to the idea that a country that will always be outmatched militarily by the United States will look for unconventional ways to attack. Cyberweapons, which can include malicious programs written by individual hackers, offer just such a relatively cheap and easier way of hitting the United States.

## 2AC — Solvency

### They Say: “Plan Gets Circumvented”

#### The plan won’t be circumvented — SDA prohibits requiring *or compelling* backdoors. No lawyering.

Sensenbrenner et al. 15 — Jim Sensenbrenner, Member of the United States House of Representatives (R-WI), with Thomas Massie, Member of the United States House of Representatives (R-KY), and Zoe Lofgren, Member of the United States House of Representatives (D-CA), 2015 (“Sensenbrenner, Massie & Lofgren Introduce Secure Data Act,” Press Release, February 4th, Available Online at <https://lofgren.house.gov/news/documentsingle.aspx?DocumentID=397873>, Accessed 06-30-2015)

Bipartisan lawmakers today reintroduced the Secure Data Act to protect Americans’ privacy and data security by prohibiting surveillance agencies from requiring or compelling surveillance “backdoors” in products and services.

A similar amendment to the Department of Defense Appropriations Act last year passed the House of Representatives by an overwhelming 293-123 vote. This amendment was not included in the CRomnibus.

U.S. Reps. Jim Sensenbrenner (R- Wis.), Thomas Massie (R- Ky.), and Zoe Lofgren (D-Calif.), sponsors of the Secure Data Act of 2015, issued the following statement:

“Congress has allowed the Administration’s surveillance authorities to go unchecked by failing to enact adequate reform. Last Congress, the Massie-Sensenbrenner-Lofgren amendment garnered support from an overwhelming bi-partisan majority in the House as a provision to the Defense Appropriations bill, but unfortunately, was not included in the CRomnibus. With threats to our homeland ever prevalent, we should not tie the hands of the intelligence community. But unwarranted, backdoor surveillance is indefensible. The Secure Data Act is an important step in rebuilding public trust in our intelligence agencies and striking the appropriate balance between national security and civil liberty.”

It has been widely reported that US intelligence and law enforcement agencies have requested or required individuals and organizations build a “backdoor” into their product or service to assist in unwarranted electronic surveillance.

However, on more than one occurrence, major security flaws have been found in these “backdoors” that put the data security of every person and business using the internet at risk. For example, a software testing firm found serious backdoor vulnerabilities in wiretapping software for law enforcement made by Israeli software firm NICE Systems in 2013 that allowed hackers to completely compromise their system and listen to intercepted phone calls. If a backdoor is created for law enforcement and intelligence surveillance, past experience has shown it’s only a matter of time before hackers exploit it too.

These "backdoors" can also be detrimental to American jobs. Other countries buy less American hardware and software and favor their domestic suppliers in order to avoid compromised American products.

The Secure Data Act fixes this by prohibiting any agency from requesting or compelling backdoors in services and products to assist with electronic surveillance.

#### The plan establishes a clear policy that protects encryption. This is sufficient to restore trust in U.S. companies.

Kehl et al. 14 — Danielle Kehl, Senior Policy Analyst at the Open Technology Institute at the New America Foundation, holds a B.A. in History from Yale University, with Kevin Bankston, Policy Director at the Open Technology Institute at the New America Foundation, former Senior Counsel and Director of the Free Expression Project at the Center for Democracy & Technology, former Senior Staff Attorney at the Electronic Frontier Foundation, former Justice William Brennan First Amendment Fellow at the American Civil Liberties Union, holds a J.D. from the University of Southern California Law School, Robyn Greene, Policy Counsel specializing in surveillance and cybersecurity at the Open Technology Institute at the New America Foundation, holds a J.D. from Hofstra University School of Law, and Robert Morgus, Program Associate with the Cybersecurity Initiative and International Security Program at the New America Foundation, 2014 (“Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity,” Report by the Open Technology Institute of the New America Foundation, July, Available Online at <https://static.newamerica.org/attachments/184-surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-and-cybersecurity/Surveilance_Costs_Final.pdf>, Accessed 07-05-2015, p. 40-41)

The U.S. government should not require or request that new surveillance capabilities or security vulnerabilities be built into communications technologies and services, even if these are intended only to facilitate lawful surveillance. There is a great deal of evidence that backdoors fundamentally weaken the security of hardware and software, regardless of whether only the NSA purportedly knows about said vulnerabilities, as some of the documents suggest. A policy statement from the Internet Engineering Task Force in 2000 emphasized that “adding a requirement for wiretapping will make affected protocol designs considerably more complex. Experience has shown that complexity almost inevitably jeopardizes the security of communications.”355 More recently, a May 2013 paper from the Center for Democracy and Technology on the risks of wiretap modifications to endpoints concludes that “deployment of an intercept capability in... communications services, systems and applications poses serious security risks.”356 The authors add that “on balance mandating that endpoint software vendors build intercept functionality into their products will be much more costly to personal, economic and governmental security overall than the risks associated with not being able to wiretap all communications.”357 While NSA programs such as SIGINT Enabling—much like proposals from domestic law enforcement agencies to update the Communications Assistance for Law Enforcement Act (CALEA) to require digital wiretapping capabilities in modern Internet-based communications services358—may aim to [end page 40] promote national security and law enforcement by ensuring that federal agencies have the ability to intercept Internet communications, they do so at a huge cost to online security overall.

Because of the associated security risks, the U.S. government should not mandate or request the creation of surveillance backdoors in products, whether through legislation, court order, or the leveraging industry relationships to convince companies to voluntarily insert vulnerabilities. As Bellovin et al. explain, complying with these types of requirements would also hinder innovation and impose a “tax” on software development in addition to creating a whole new class of vulnerabilities in hardware and software that undermines the overall security of the products.359 An amendment offered to the NDAA for Fiscal Year 2015 (H.R. 4435) by Representatives Zoe Lofgren (D-CA) and Rush Holt (D-NJ) would have prohibited inserting these kinds of vulnerabilities outright.360 The Lofgren-Holt proposal aimed to prevent “the funding of any intelligence agency, intelligence program, or intelligence related activity that mandates or requests that a device manufacturer, software developer, or standards organization build in a backdoor to circumvent the encryption or privacy protections of its products, unless there is statutory authority to make such a mandate or request.”361 Although that measure was not adopted as part of the NDAA, a similar amendment sponsored by Lofgren along with Representatives Jim Sensenbrenner (D-WI) and Thomas Massie (R-KY), did make it into the House-approved version of the NDAA—with the support of Internet companies and privacy organizations362—passing on an overwhelming vote of 293 to 123.363 Like Representative Grayson’s amendment on NSA’s consultations with NIST around encryption, it remains to be seen whether this amendment will end up in the final appropriations bill that the President signs. Nonetheless, these legislative efforts are a heartening sign and are consistent with recommendations from the President’s Review Group that the U.S. government should not attempt to deliberately weaken the security of commercial encryption products. Such mandated vulnerabilities, whether required under statute or by court order or inserted simply by request, unduly threaten innovation in secure Internet technologies while introducing security flaws that may be exploited by a variety of bad actors. A clear policy against such vulnerability mandates is necessary to restore international trust in U.S. companies and technologies.

#### The problem is the law, not NSA compliance. The plan solves.

Jaffer 13 — Jameel Jaffer, ACLU Deputy Legal Director and Director of the ACLU Center for Democracy, 2013 (“’There Have Been Some Compliance Incidents’: NSA Violates Surveillance Rules Multiple Times a Day,” ACLU Blog, August 16th, Available Online at <https://www.aclu.org/blog/there-have-been-some-compliance-incidents-nsa-violates-surveillance-rules-multiple-times-day?redirect=blog/national-security/nsa-privacy-violations-even-more-frequent-we-imagined>, Accessed 06-05-2015)

One final note: The NSA's noncompliance incidents are a big deal, but we shouldn't let them become a distraction. The far bigger problem is with the law itself, which gives the NSA almost unchecked authority to monitor Americans' international calls and emails. The problem arises, in other words, not just from the NSA's non-compliance with the law, but from its compliance with it.