# Explanation/Guide

### File Description and General Tips

This file contains the Secure Data Act negative. It includes 1NC frontlines against the affirmative’s three advantages and solvency as well as comprehensive backline evidence. When debating against this affirmative, students will need to prepare to answer the Constitutional Privacy Advantage, the Tech Leadership Advantage, and/or the Cybersecurity Advantage. The affirmative’s case materials are located in the Secure Data Act affirmative file. It includes explanations of the plan and each of the advantages.

When responding to the case, the negative is provided with a 1NC frontline for each contention. Two backline cards for each 1NC argument are also included; they can be used when extending case arguments in the 2NC and 1NR. Students should prepare 2NC/1NR blocks that extend the 1NC evidence as well as introduce additional evidence from the backline materials.

When debating against the SDA affirmative, the negative should also read one or more disadvantages. These materials are located in the separate DA files.

### Answering the Constitutional Privacy Advantage

In response to the Constitutional Privacy Advantage, the negative argues that encryption itself is unconstitutional because it prevents legitimate Fourth Amendment searches. To the extent that encryption backdoors nonetheless violate privacy, the negative argues that private companies are already violating privacy on a much greater scale than NSA. Moreover, the negative contends that privacy is relatively unimportant — especially in the face of a competing security interest. For that reason, the negative suggests that decision-makers should weigh privacy against security. When doing so, the negative argues that security should be prioritized.

### Answering the Tech Leadership Advantage

When answering the Tech Leadership Advantage, the negative argues that the U.S. technology sector is plagued by two more important problems than NSA surveillance: a lack of qualified STEM workers and high corporate taxes that drive businesses overseas. To the extent that NSA surveillance is hurting the industry, the negative argues that the passage of the USA Freedom Act was sufficient to restore international confidence in American companies. Finally, the negative contests the impact to the advantage by contesting whether “competitiveness” is a sound economic theory and by contending that the U.S. is not at risk of losing its global hegemony.

### Answering the Cybersecurity Advantage

In response to the Cybersecurity Advantage, the negative argues that a “Golden Key” system can provide law enforcement with exceptional access to encrypted data without jeopardizing cybersecurity. The negative also argues that a shortage of cyber workers is a much bigger threat to cybersecurity than encryption backdoors. Regardless, the negative contends that there is very little risk of a catastrophic cyber attack. In particular, the negative argues that a large attack against the electric grid is highly improbable and unlikely to have devastating consequences.

### Answering Solvency

The negative argues that the plan will be circumvented because there is no meaningful oversight of intelligence agencies like NSA. The FISA Court provides a rubber stamp to surveillance requests and Congressional Intelligence Committees have proven unwilling to reign in NSA. When making this argument, the negative should be cognizant of how it interacts with the disadvantage(s) that they have read. If NSA circumvents the plan, is there still a link to the disadvantage? Students should make sure that they have a clear and consistent story that ties together their circumvention arguments and disadvantage(s).

## 1NC

### 1NC — Constitutional Privacy Advantage

#### 1. Encryption Unconstitutional — it subverts legitimate Fourth Amendment searches.

Etzioni 15 — Amitai Etzioni, University Professor, Professor of International Affairs, and Director of the Institute for Communitarian Policy Studies at George Washington University, former Professor of Sociology at Columbia University, holds a Ph.D. in Sociology from the University of California-Berkeley, 2015 (“Ultimate Encryption,” May 11th, Available Online via SSRN at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605153>, Accessed 08-12-2015, p. 27-28)

In Conclusion

Civil libertarians object to the key new security measures that have been introduced in the wake of the 2001 attacks on the US homeland because they are not based on particularized, individualized suspicion recognized by a court. This is, they argue that these measures violate the constitutional requirement that separates [end page 27] legal from illegal searches. When the same libertarians then support moves by private companies that frustrate security measures that do meet this standard, in full, their position seems quite unreasonable.

Putting aside the question on what legal grounds one may ban UE, there is a major normative issue that is the subtext of the preceding deliberations. That is, there is a profound normative position that finds expression in the Fourth Amendment. Namely, that the government be curbed from searching people—unless there is a clear reason for it to proceed (and a mechanism is provided to determine what is reasonable). This amendment is often understood to protect individuals from an abusive, overreaching government, as we have known through much of human history and still see evidenced in many parts of the world—and, some hold, in the U.S. However, one should not overlook that the same text also fully recognized that the government may have fully legal and fully justified, legitimate reasons to conduct searches. Hence, when private parties develop, introduce, or promote technologies that make it impossible (or “only” very difficult) for the government to carry out searches courts ruled legitimate, these parties frustrate the essence of the 4th Amendment, even if technically they may not be required by law to cooperate. It is time for the law to catch up with what good judgment indicates: ban ultimate encryption.

#### 2. Privacy Already Dead — tech companies are a greater threat than NSA.

Sterner 14 — Eric Sterner, Fellow at the George C. Marshall Institute, Faculty in the Graduate Department of Defense and Strategic Studies at Missouri State University, former Associate Deputy Administrator for Policy and Planning and Chief of Strategic Communications for NASA, former Senior Professional Staff Member of the House Armed Services Committee, holds an M.A. in Political Science from George Washington University and an M.A. in Security Policy Studies from George Washington University, 2014 (“The security vs. privacy debate is already over, and privacy lost,” *Washington Examiner*, March 10th, Available Online at <http://marshall.org/science-and-tech/the-security-vs-privacy-debate-is-already-over-and-privacy-lost/>, Accessed 08-07-2015)

When Edward Snowden leaked massive troves of information about the National Security Agency‘s collection of electronic information, he started a debate over the tradeoffs between security and privacy. At least that’s how President Obama framed it, arguing, “we have to make some important decisions about how to protect ourselves and sustain our leadership in the world, while upholding the civil liberties and privacy protections that our ideals and our Constitution require.”

Unfortunately, the security vs. privacy debate is largely over. As cybertechnologies pervaded our daily lives, we surrendered privacy, usually voluntarily. Consequently, framing the decisions before us as a contest between privacy and security is misguided; privacy died with the information age.

Information and communication technologies make life better. They improved economic productivity, efficiency, and economic growth. More personally, information digitization created opportunities to grow, relate to others, and generally realize one’s creative potential. Connected to the Internet, we create, post, and retrieve vast amounts of data, almost all of which is in the hands of third parties.

These benefits come at a price. In order for the applications we use to improve their performance and offer us ever better services, they require information about us. We give it to them. Facebook‘s 1 billion active users, for example, share roughly 5 billion items a day, not counting the data Facebook collects about them.

Consider Google‘s privacy policy. Google collects personal information, data about the services you use and how you use them, server logs (exactly the kind of thing the NSA was after), location information, data about the software you use, storage data and other identifying information that third parties may store on the hardware you use to access cyberspace. That is an awful lot of information when all you want to do is make a call, play a game or write a letter.

This is not to single Google out for praise or condemnation. Its policy is a standard for the industry. Most companies use that information to make our lives better. Surrendering data enables us to better exploit the Internet. When amalgamated, doctors can track public health risks, improve medical research, promote energy efficiency and more. Unsurprisingly, our adversaries use the technology too.

Not very long ago we considered all this information personal. But, as soon as we voluntarily shared it with others, the information stopped being truly private. Our behavior changed, but our expectations did not. So, when Snowden announced that “A child born today will grow up with no conception of privacy at all. They’ll never know what it means to have a private moment to themselves — an unrecorded, unanalyzed thought,” he was right. But the NSA had nothing to do with it.

#### 3. No Impact To Privacy — it’s just personal false advertising. There’s no harm to people with nothing to hide.

Posner 13 — Richard A. Posner, Senior Lecturer in Law at the University of Chicago, Judge on the United States Court of Appeals for the Seventh Circuit in Chicago, was named the most cited legal scholar of the 20th century by *The Journal of Legal Studies*, holds an LL.B. from Harvard University, 2013 (“Privacy is overrated,” *New York Daily News*, April 28th, Available Online at <http://www.nydailynews.com/opinion/privacy-overrated-article-1.1328656>, Accessed 04-16-2015)

There is a tendency to exaggerate the social value of privacy. I value my privacy as much as the next person, but there is a difference between what is valuable to an individual and what is valuable to society. Thirty-five years ago, when I was a law professor rather than a judge, I published an article called “The Right of Privacy,” in which I pointed out that “privacy” is really just a euphemism for concealment, for hiding specific things about ourselves from others.

We conceal aspects of our person, our conduct and our history that, if known, would make it more difficult for us to achieve our personal goals. We don’t want our arrest record to be made public; our medical history to be made public; our peccadilloes to be made public; and so on. We want to present sanitized versions of ourselves to the world. We market ourselves the way sellers of consumer products market their wares — highlighting the good, hiding the bad.

I do not argue that all concealment is bad. There is nothing wrong with concealing wealth in order to avoid being targeted by thieves or concealing embarrassing personal facts, such as a deformity or being related to a notorious criminal, that would not cause a rational person to shun us but might complicate our social and business relations.

There may even be justification for allowing the concealment of facts that might, but should not, cause a person to be shunned. Laws that place a person’s arrest (as distinct from conviction) record behind a veil of secrecy are based on a belief that prospective employers would exaggerate the significance of such a record, not realizing, for example, that arrests are often based on mistakes by witnesses or police officers, or are for trivial infractions.

Privacy-protecting laws are paternalistic; they are based on a skepticism regarding whether people can make sensible evaluations of an arrest record or other private facts that enter the public domain.

Still, a good deal of privacy just facilitates the personal counterpart of the false advertising of goods and services, and by doing so, reduces the well-being of society as a whole.

I am not suggesting that privacy laws be repealed. I don’t think that they do much harm, and they do some good, as just indicated. But I don’t think they serve the public interest as well as civil libertarians contend, and so I don’t think that such laws confer social benefits comparable to those of methods of surveillance that are effective against criminal and especially terrorist assaults.

#### 4. Weigh Consequences — the Constitution is not a suicide pact.

Posner 6 — Richard A. Posner, Senior Lecturer in Law at the University of Chicago, Judge on the United States Court of Appeals for the Seventh Circuit in Chicago, was named the most cited legal scholar of the 20th century by *The Journal of Legal Studies*, holds an LL.B. from Harvard University, 2006 (“Wire Trap,” *New Republic*, February 6th, Available Online at http://www.newrepublic.com/article/104859/wire-trap, Accessed 04-16-2015)

The revelation by The New York Times that the National Security Agency (NSA) is conducting a secret program of electronic surveillance outside the framework of the Foreign Intelligence Surveillance Act (FISA) has sparked a hot debate in the press and in the blogosphere. But there is something odd about the debate: It is aridly legal. Civil libertarians contend that the program is illegal, even unconstitutional; some want President Bush impeached for breaking the law. The administration and its defenders have responded that the program is perfectly legal; if it does violate FISA (the administration denies that it does), then, to that extent, the law is unconstitutional. This legal debate is complex, even esoteric. But, apart from a handful of not very impressive anecdotes (did the NSA program really prevent the Brooklyn Bridge from being destroyed by blowtorches?), there has been little discussion of the program’s concrete value as a counter-terrorism measure or of the inroads it has or has not made on liberty or privacy.

Not only are these questions more important to most people than the legal questions; they are fundamental to those questions. Lawyers who are busily debating legality without first trying to assess the consequences of the program have put the cart before the horse. Law in the United States is not a Platonic abstraction but a flexible tool of social policy. In analyzing all but the simplest legal questions, one is well advised to begin by asking what social policies are at stake. Suppose the NSA program is vital to the nation’s defense, and its impingements on civil liberties are slight. That would not prove the program’s legality, because not every good thing is legal; law and policy are not perfectly aligned. But a conviction that the program had great merit would shape and hone the legal inquiry. We would search harder for grounds to affirm its legality, and, if our search were to fail, at least we would know how to change the law--or how to change the program to make it comply with the law--without destroying its effectiveness. Similarly, if the program’s contribution to national security were negligible--as we learn, also from the Times, that some FBI personnel are indiscreetly whispering--and it is undermining our civil liberties, this would push the legal analysis in the opposite direction.

Ronald Dworkin, the distinguished legal philosopher and constitutional theorist, wrote in The New York Review of Books in the aftermath of the September 11 attacks that “we cannot allow our Constitution and our shared sense of decency to become a suicide pact.” He would doubtless have said the same thing about FISA. If you approach legal issues in that spirit rather than in the spirit of ruat caelum fiat iusticia (let the heavens fall so long as justice is done), you will want to know how close to suicide a particular legal interpretation will bring you before you decide whether to embrace it. The legal critics of the surveillance program have not done this, and the defenders have for the most part been content to play on the critics’ turf.

#### 5. Security Outweighs Privacy — without security, privacy is meaningless.

Himma 7 — Kenneth Einar Himma, Associate Professor of Philosophy at Seattle Pacific University, holds a Ph.D. in Philosophy from the University of Washington and a J.D. from the University of Washington Law School, 2007 (“Privacy Versus Security: Why Privacy is Not an Absolute Value or Right,” *San Diego Law Review* (44 San Diego L. Rev. 857), Fall, Available Online to Subscribing Institutions via Lexis-Nexis)

XIII. Security as a Prerequisite for the Meaningful Exercise of Privacy Rights

The last argument I wish to make in this essay will be brief because it is extremely well known and has been made in a variety of academic and nonacademic contexts. The basic point here is that no right not involving [\*919] security can be meaningfully exercised in the absence of efficacious protection of security. The right to property means nothing if the law fails to protect against threats to life and bodily security. Likewise, the right to privacy has little value if one feels constrained to remain in one's home because it is so unsafe to venture away that one significantly risks death or grievous bodily injury.

This is not merely a matter of describing common subjective preferences; this is rather an objective fact about privacy and security interests. If security interests are not adequately protected, citizens will simply not have much by way of privacy interests to protect. While it is true, of course, that people have privacy interests in what goes on inside the confines of their home, they also have legitimate privacy interests in a variety of public contexts that cannot be meaningfully exercised if one is afraid to venture out into those contexts because of significant threats to individual and collective security — such as would be the case if terrorist attacks became highly probable in those contexts.

It is true, of course, that to say that X is a prerequisite for exercising a particular right Y does not obviously entail that X is morally more important than Y, but this is a reasonable conclusion to draw. If it is true that Y is meaningless in the absence of X, then it seems clear that X deserves, as a moral matter, more stringent protection than Y does. Since privacy interests lack significance in the absence of adequate protection of security interests, it seems reasonable to infer that security interests deserve, as a moral matter, more stringent protection than privacy interests.

### 1NC — Tech Leadership Advantage

#### 1. Alternate Causality — STEM worker shortages hamstring the U.S. tech sector.

Tech CEOs 13 — An Open Letter by more than 100 chief executives of major tech companies and trade associations, 2013 (Open Letter to President Obama, Speaker Boehner, Senator Reid, Senator McConnell, and Representative Pelosi, March 14th, Available Online at <https://www.scribd.com/doc/130388692/Tech-CEO-letter>, Accessed 08-09-2015)

One of the biggest economic challenges facing our nation is the need for more qualified, highly-skilled professionals, domestic and foreign, who can create jobs and immediately contribute to and improve our economy. As leaders of technology companies from around the country, we want to thank you for your sincere efforts in addressing high skilled immigration and we urge that you and your colleagues enact reform legislation this year.

As you know, the United States has a long history of welcoming talented, hard-working people to our shores. Immigrant entrepreneurs have gone on to found thousands of companies with household names like eBay, Google, PayPal and Yahoo! to name just a few. These companies provide jobs, drive economic growth and generate tax revenue at all levels of government.

Yet because our current immigration system is outdated and inefficient, many high-skilled immigrants who want to stay in America are forced to leave because they are unable to obtain permanent visas. Some do not bother to come in the first place. This is often due to visa shortages, long waits for green cards, and lack of mobility. We believe that numerical levels and categories for high-skilled nonimmigrant and immigrant visas should be responsive to market needs and, where appropriate, include mechanisms to fluctuate based on objective standards. In addition, spouses and children should not be counted against the cap of high-skilled immigrant visas. There should not be a marriage or family penalty.

According to the U.S. Bureau of Labor Statistics, there are tens of thousands of unfilled jobs requiring highly skilled individuals. Five high-tech companies alone – IBM, Intel, Microsoft, Oracle and [end page 1] Qualcomm – have combined 10,000 openings in the United States. Each one of these jobs has the potential to create many others, directly and indirectly. Bipartisan legislation currently introduced in the Senate, such as The Immigration Innovation Act of 2013, and bi-partisan legislation focused on addressing the needs of entrepreneurs and start ups such as the Startup Visa Act and Startup Act 3.0, will encourage innovation here in the U.S. by allowing American companies and entrepreneurs to have access to the talented workers they need while simultaneously investing in STEM education here in the U.S. We know what it will take to keep America in a position of global leadership. We know that when America is leading, our economic growth follows to the benefit of our nation’s workforce.

#### 2. Alternate Causality — high taxes hurt the U.S. tech industry.

BDO 15 — BDO, a worldwide professional services network of public accountancy firms, 2015 (“2015 BDO Technology Outlook,” March, Available Online at <https://www.bdo.com/insights/industries/tech-life-sciences/2015-bdo-technology-outlook>, Accessed 08-10-2015)

Policy and Tax Concerns Persist

Pending tax proposals in Washington are leaving many finance chiefs uncertain about the future of their business growth. In fact, 24 percent of CFOs cite policy and tax changes as the top factor inhibiting overall business growth, on trend with 2014 (26 percent). Moreover, 50 percent cite U.S. corporate tax rates as the leading tax issue this year, a 35 percent increase from 2014.

Even the debate around tax inversions, particularly for large corporations, is giving tech CFOs pause. Fourteen percent say they are most concerned about taxation of overseas activities, a significant increase from last year when only eight percent expressed similar sentiment. As companies look to expand their global footprint to remain competitive, 41 percent of CFOs believe the domestic tax system hampers their ability to effectively compete in the global marketplace.

“As the focus on U.S. taxation of overseas activities increases, multi-national organizations should carefully consider potential changes to U.S. tax policy when making global investment and operational decisions. Though many CFOs believe U.S. tax rates are too high relative to other countries, the concern hasn’t yet inspired Congress to make a move toward reform,” said Matthew K. Becker, Central Region Tax and National Tax Office Managing Partner at BDO.

#### 3. Status Quo Solves — the Freedom Act boosted trust in U.S. tech companies.

Smith 15 — Brad Smith, General Counsel and Executive Vice President of Legal and Corporate Affairs at Microsoft, 2015 (“USA Freedom Act: An important step forward,” *Microsoft on the Issues*, June 2nd, Available Online at <https://blogs.microsoft.com/on-the-issues/2015/06/02/xxxusa-freedom-act-an-important-step-forward/>, Accessed 08-10-2015)

Earlier this afternoon, the U.S. Congress passed by a 2-to-1 margin the USA Freedom Act, which will bring about significant reforms to the nation’s surveillance programs once it is signed into law as expected by President Obama.

The USA Freedom Act strikes an important balance between protecting public safety and preserving civil liberties. In addition to protecting personal privacy, it provides for greater transparency and increased accountability about the government’s surveillance activities while maintaining national security.

Since the disclosures about surveillance first emerged in 2013, the world has rightfully focused on concerns about government access to personal information. We know that people will not use technology they do not trust. That’s why Microsoft and a broad coalition of tech companies and civil society called on Congress to act to change the surveillance laws.

The USA Freedom Act will increase trust in technology by implementing essential reforms to the USA Patriot Act. The legislation will ensure that the public is aware of what their government is doing by allowing companies to publish detailed transparency reports. Governments also need to act with proper accountability with proper regard for legal process and people’s rights. The reforms of the FISA Court in the bill moves government accountability forward by increasing the transparency of its proceedings and rulings and introducing a process for amicus curiae. And the new law ends the bulk collection of data – a program that a federal court recently struck down.

As we’ve said before, 2015 is a year that calls for solutions – for measures that will ensure people benefit from the privacy and civil liberties they deserve while ensuring law enforcement can access the information it needs to keep the public safe – all pursuant to proper legal process and the rule of law. Congress and the President have provided a solution with this new law. The USA Freedom Act is a substantial step in reforming US surveillance laws, increasing transparency and accountability.

There’s still more work to do, both here in the United States and internationally. High on that list is the creation of new international legal frameworks to tackle other important issues we face in ensuring the free flow of information around the world while respecting national sovereignty. There is no doubt that today marks an important step forward in striking a better balance between public safety and privacy.

#### 4. No Competitiveness Impact — there’s no economic basis for the theory of competitiveness.

Krugman 94 — Paul Krugman, Professor of Economics at the Massachusetts Institute of Technology, 1994 (“Competitiveness: A Dangerous Obsession,” *Foreign Affairs*, March-April, Available Online to Subscribing Institutions via Lexis-Nexis Academic Universe)

It was a disappointing evasion, but not a surprising one. After all, the rhetoric of competitiveness – the view that, in the words of President Clinton, each nation is "like a big corporation competing in the global marketplace" – has become pervasive among opinion leaders throughout the world. People who believe themselves to be sophisticated about the subject take it for granted that the economic problem facing any modern nation is essentially one of competing on world markets – that the United States and Japan are competitors in the same sense that Coca-Cola competes with Pepsi – and are unaware that anyone might seriously question that proposition. Every few months a new best-seller warns the American public of the dire consequences of losing the "race" for the 21st century. n1 A whole industry of councils on competitiveness, "geo-economists" and managed trade theorists has sprung up in Washington. Many of these people, having diagnosed America's economic problems in much the same terms as Delors did Europe's, are now in the highest reaches of the Clinton administration formulating economic and trade policy for the United States. So Delors was using a language that was not only convenient but comfortable for him and a wide audience on both sides of the Atlantic.

Unfortunately, his diagnosis was deeply misleading as a guide to what ails Europe, and similar diagnoses in the United States are equally misleading. The idea that a country's economic fortunes are largely determined by its success on world markets is a hypothesis, not a necessary truth; and as a practical, empirical matter, that hypothesis is flatly wrong. That is, it is simply not the case that the world's leading nations are to any important degree in economic competition with each other, or that any of their major economic problems can be attributed to failures to compete on world markets. The growing obsession in most advanced nations with international competitiveness should be seen, not as a well-founded concern, but as a view held in the face of overwhelming contrary evidence. And yet it is clearly a view that people very much want to hold – a desire to believe that is reflected in a remarkable tendency of those who preach the doctrine of competitiveness to support their case with careless, flawed arithmetic.

This article makes three points. First, it argues that concerns about competitiveness are, as an empirical matter, almost completely unfounded. Second, it tries to explain why defining the economic problem as one of international competition is nonetheless so attractive to so many people. Finally, it argues that the obsession with competitiveness is not only wrong but dangerous, skewing domestic policies and threatening the international economic system. This last issue is, of course, the most consequential from the standpoint of public policy. Thinking in terms of competitiveness leads, directly and indirectly, to bad economic policies on a wide range of issues, domestic and foreign, whether it be in health care or trade.

#### 5. No U.S. Leadership Impact — enduring geopolitical strengths prevent *relative* U.S. economic decline.

Meltzer et al. 13 — Joshua Meltzer, Fellow in the Global Economy and Development Program at the Brookings Institution, Adjunct Professor at The Johns Hopkins University’s School of Advanced International Studies, holds an S.J.D. and L.L.M from the University of Michigan Law School, et al., with David Steven, Nonresident Senior Fellow for the Managing Global Order Project in the Foreign Policy Program at the Brookings Institution, Nonresident Senior Fellow and Associate Director of the Center on International Cooperation at New York University, and Claire Langley, Research Analyst in the Global Economy and Development Program at the Brookings Institution, 2013 (“The United States After The Great Recession: The Challenges of Sustainable Growth,” Brookings Institution Global Economy & Development Working Paper #60, February, Available Online at http://www.brookings.edu/~/media/research/files/papers/2013/02/us%20post%20great%20recession%20meltzer%20steven/02%20us%20post%20great%20recession%20meltzer%20steven.pdf, Accessed 08-11-2013, p. 20)

A New Era of Global Leadership

Although the United States is certain to face headwinds in the coming decades, this does not mean that its stance will be a pessimistic one. Though fears of American decline will continue to surface, a more confident narrative is likely to predominate at most times. Even during the crisis, a slim majority of Americans remained optimistic about the country’s future over the next 50 years.148 At the ballot box, meanwhile, they consistently reward optimistic politicians over negative ones.149 A blind analysis of the speeches of presidential candidates between 1900 and 1984\* showed that the candidate who sounded least pessimistic was elected on 80 percent of occasions, creating strong incentives for politicians to emphasize the potential for renewed American leadership.

At the same time, the United States will be able to draw on enduring absolute geopolitical strengths, even if its relative power continues to diminish due to the economic success of rising powers. It will continue to benefit from:

• Its position as a dominant security actor, which it seems certain to maintain for at least another generation, and its privileged position in most global institutions. 150

• Its internal security, which is more robust than that of countries such as India (currently tackling a Naxalite insurgency in 125 of its 640 districts)151 or China (reported to be spending as much on domestic security as it does on defense).152

• Its growth potential, especially when compared with the EU, but more generally if it manages to use its leadership in key export sectors to exploit the purchasing power of a growing global middle class153 or if one or more of the emerging economies suffers an interruption to its growth.

### 1NC — Cybersecurity Advantage

#### 1. Golden Key Solves — *only* law enforcement should have access.

Washington Post 14 — Washington Post Editorial Board, 2014 (“Compromise needed on smartphone encryption,” October 3rd, Available Online at <http://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html>, Accessed 07-05-2015)

Law enforcement officials deserve to be heard in their recent warnings about the impact of next-generation encryption technology on smartphones, such as Apple’s new iPhone. This is an important moment in which technology, privacy and the rule of law are colliding.

Apple announced Sept. 17 that its latest mobile operating system, iOS 8, includes encryption so thorough that the company will not be able to unlock it for law enforcement. The encryption is to be set by the user, and Apple will not retain the key. Google’s next version of its popular Android operating system also will be unlockable by the company. Both insist they are giving consumers ironclad privacy protection. The moves are in large part a response to public worries about National Security Agency surveillance of Internet and telephone metadata revealed by former government contractor Edward Snowden.

What has the law enforcement community up in arms is the prospect of losing access to the data on these smartphones in cases where they have a valid, court-approved search warrant. The technology firms, while pledging to honor search warrants in other situations, say they simply won’t possess the ability to unlock the smartphones. Only the owner of the phone, who set up the encryption, will be able to do that. Attorney General Eric H. Holder Jr. said this could imperil investigations in kidnapping and other cases; FBI Director James B. Comey said he could not understand why the tech companies would “market something expressly to allow people to place themselves beyond the law.”

This is not about mass surveillance. Law enforcement authorities are not asking for the ability to surveil everyone’s smartphone, only those relatively few cases where there is a court-approved search warrant. This seems reasonable and not excessively intrusive. After all, the government in many other situations has a right — and responsibility — to set standards for products so that laws are followed. Why not smartphones? Moreover, those worried about privacy can take solace from the Supreme Court’s decision in June in Riley v. California, which acknowledged the large amount of private information on smartphones and said a warrant is generally required before a search.

Law enforcement will not be entirely without tools in criminal investigations. Data stored in the “cloud” and other locations will still be available; wiretaps, too. But smartphone users must accept that they cannot be above the law if there is a valid search warrant.

How to resolve this? A police “back door” for all smartphones is undesirable — a back door can and will be exploited by bad guys, too. However, with all their wizardry, perhaps Apple and Google could invent a kind of secure golden key they would retain and use only when a court has approved a search warrant. Ultimately, Congress could act and force the issue, but we’d rather see it resolved in law enforcement collaboration with the manufacturers and in a way that protects all three of the forces at work: technology, privacy and rule of law.

#### 2. Alternate Causality — worker shortages jeopardize cybersecurity. This is more important than technology.

Davidson 15 — Joe Davidson, Columnist at *The* *Washington Post* who writes the *Federal Diary*—a column about federal government and workplace issues, former Assistant City Editor at *The Washington Post*, former Washington and Foreign Correspondent with *The Wall Street Journal*, 2015 (“Lack of digital talent adds to cybersecurity problems,” *Washington Post*, July 19th, Available Online at <https://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/19/lack-of-digital-talent-adds-to-cybersecurity-problems/>, Accessed 08-12-2015)

A big problem exposed by a massive data breach at the Office of Personal Management (OPM) is the woeful state of the federal government’s cybersecurity. It’s not comforting when the Obama administration’s chief information officer says Uncle Sam’s information technology needs bubble wrap and Band-Aids to help counter cyberattacks.

But even if the digital networks were magically modernized, the protection of personal information belonging to federal employees and many other records would still be at risk.

The reason: too few cyber experts.

The federal government has a serious shortage of cyber talent and the future is dim.

Recruiting digital specialists and plugging them into the right slots “is going to be one of our challenges,” Tony Scott, the U.S. chief information officer, told the National Council on Federal Labor-Management Relations last week. He plans to issue recommendations to confront that challenge soon. “It’s the hardest recruiting that there is on the planet today for people with those kinds of skills. . . . We’re going to have to take extraordinary moves to try to develop a broader set of talent and skill base in that area.”

Although the need is great, the amount of attention given to cyber talent too often is not.

After personal information for more than 22 million federal employees and others was stolen, the need for modern technology received far more scrutiny during a series of congressional hearings than the need for skilled people to work it. Search for “cyber” on the Government Accountability Office Web site and you’ll find dozens of related documents just this year. But if you ask for a study specifically on cyber talent, GAO will provide one, from 2011.

Overlooking the importance of people is a serious mistake, said Max Stier, president and chief executive of the Partnership for Public Service, a think tank on the federal workforce.

“At the end of the day, give me great talent over great technology,” he said, adding that talent will find a way to fix what technology lacks.

The partnership, along with the Booz Allen Hamilton consulting firm, published a report in April on closing the federal cyber talent gap. It said the government “lacks the cyber workforce it needs and still does not have a comprehensive, enterprise-wide strategy to recruit and retain that workforce. . . . Our nation is at risk as the number and sophistication of cyber-attacks continue to grow, but the government has failed to act with urgency.”

#### 3. No Cyber Impact — the threat is massively exaggerated.

Healey 13 — Jason Healey, Director of the Cyber Statecraft Initiative at the Atlantic Council, President of the Cyber Conflict Studies Association, Lecturer in Cyber Policy at Georgetown University, Lecturer in Cyber National Security Studies at the School of Advanced International Studies at Johns Hopkins University, former Director for Cyber Infrastructure Protection at the White House, holds a Master’s in Computer Security from James Madison University, 2013 (“No, Cyberwarfare Isn't as Dangerous as Nuclear War,” *U.S. News & World Report*, March 20th, Available Online at <http://www.usnews.com/opinion/blogs/world-report/2013/03/20/cyber-attacks-not-yet-an-existential-threat-to-the-us>, Accessed 01-27-2015)

America does not face an existential cyberthreat today, despite recent warnings. Our cybervulnerabilities are undoubtedly grave and the threats we face are severe but far from comparable to nuclear war.

The most recent alarms come in a Defense Science Board report on how to make military cybersystems more resilient against advanced threats (in short, Russia or China). It warned that the "cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War." Such fears were also expressed by Adm. Mike Mullen, then chairman of the Joint Chiefs of Staff, in 2011. He called cyber "The single biggest existential threat that's out there" because "cyber actually more than theoretically, can attack our infrastructure, our financial systems."

While it is true that cyber attacks might do these things, it is also true they have not only never happened but are far more difficult to accomplish than mainstream thinking believes. The consequences from cyber threats may be similar in some ways to nuclear, as the Science Board concluded, but mostly, they are incredibly dissimilar.

Eighty years ago, the generals of the U.S. Army Air Corps were sure that their bombers would easily topple other countries and cause their populations to panic, claims which did not stand up to reality. A study of the 25-year history of cyber conflict, by the Atlantic Council and Cyber Conflict Studies Association, has shown a similar dynamic where the impact of disruptive cyberattacks has been consistently overestimated.

Rather than theorizing about future cyberwars or extrapolating from today's concerns, the history of cyberconflict that have actually been fought, shows that cyber incidents have so far tended to have effects that are either widespread but fleeting or persistent but narrowly focused. No attacks, so far, have been both widespread and persistent. There have been no authenticated cases of anyone dying from a cyber attack. Any widespread disruptions, even the 2007 disruption against Estonia, have been short-lived causing no significant GDP loss.

Moreover, as with conflict in other domains, cyberattacks can take down many targets but keeping them down over time in the face of determined defenses has so far been out of the range of all but the most dangerous adversaries such as Russia and China. Of course, if the United States is in a conflict with those nations, cyber will be the least important of the existential threats policymakers should be worrying about. Plutonium trumps bytes in a shooting war.

This is not all good news. Policymakers have recognized the problems since at least 1998 with little significant progress. Worse, the threats and vulnerabilities are getting steadily more worrying. Still, experts have been warning of a cyber Pearl Harbor for 20 of the 70 years since the actual Pearl Harbor.

The transfer of U.S. trade secrets through Chinese cyber espionage could someday accumulate into an existential threat. But it doesn't seem so seem just yet, with only handwaving estimates of annual losses of 0.1 to 0.5 percent to the total U.S. GDP of around $15 trillion. That's bad, but it doesn't add up to an existential crisis or "economic cyberwar."

#### 4. No Grid Collapse — it’s not technically feasible for hackers to take down the grid.

Perera 14 — David Perera, Cybersecurity Reporter for *Politico*, 2014 (“U.S. grid safe from large-scale attack, experts say,” *Politico*, September 10th, Available Online at <http://www.politico.com/story/2014/09/power-grid-safety-110815.html>, Accessed 09-24-2014)

The specter of a large-scale, destructive attack on the U.S. power grid is at the center of much strategic thinking about cybersecurity. For years, Americans have been warned by a bevy of would-be Cassandras in Congress, the administration and the press that hackers are poised to shut it down.

But in fact, the half-dozen security experts interviewed for this article agreed it’s virtually impossible for an online-only attack to cause a widespread or prolonged outage of the North American power grid. Even laying the groundwork for such a cyber operation could qualify as an act of war against the U.S. — a line that few nation-state-backed hacker crews would wish to cross.

None denied that determined hackers could penetrate the networks of bulk power providers. But there’s a huge gap between that and causing a civilization-ending sustained outage of the grid.

Electrical-grid hacking scenarios mostly overlook the engineering expertise necessary to intentionally cause harm to the grid, say experts knowledgeable about the power generators and high voltage transmission entities that constitute the backbone of the grid — what’s called the bulk power system.

There’s also the enormity of the grid and diversity of its equipment to consider. “The grid is designed to lose utilities all the time,” said Patrick Miller, founder and director of the Energy Sector Security Consortium. “I’m not trying to trivialize the situation, but you’re not really able to cause this nationwide cascading failure for any extended duration of time,” he added.

“It’s just not possible.”

### 1NC — Solvency

#### No Solvency — “reforms” like the plan will be circumvented.

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 (“Congress is Irrelevant on Mass Surveillance. Here’s What Matters Instead.,”

*The Intercept*, November 19th, Available Online at <https://firstlook.org/theintercept/2014/11/19/irrelevance-u-s-congress-stopping-nsas-mass-surveillance/>, Accessed 06-16-2015)

All of that illustrates what is, to me, the most important point from all of this: the last place one should look to impose limits on the powers of the U.S. government is . . . the U.S. government. Governments don’t walk around trying to figure out how to limit their own power, and that’s particularly true of empires.

The entire system in D.C. is designed at its core to prevent real reform. This Congress is not going to enact anything resembling fundamental limits on the NSA’s powers of mass surveillance. Even if it somehow did, this White House would never sign it. Even if all that miraculously happened, the fact that the U.S. intelligence community and National Security State operates with no limits and no oversight means they’d easily co-opt the entire reform process. That’s what happened after the eavesdropping scandals of the mid-1970s led to the establishment of congressional intelligence committees and a special FISA “oversight” court—the committees were instantly captured by putting in charge supreme servants of the intelligence community like Senators Dianne Feinstein and Chambliss, and Congressmen Mike Rogers and “Dutch” Ruppersberger, while the court quickly became a rubber stamp with subservient judges who operate in total secrecy.

Ever since the Snowden reporting began and public opinion (in both the U.S. and globally) began radically changing, the White House’s strategy has been obvious. It’s vintage Obama: Enact something that is called “reform”—so that he can give a pretty speech telling the world that he heard and responded to their concerns—but that in actuality changes almost nothing, thus strengthening the very system he can pretend he “changed.” That’s the same tactic as Silicon Valley, which also supported this bill: Be able to point to something called “reform” so they can trick hundreds of millions of current and future users around the world into believing that their communications are now safe if they use Facebook, Google, Skype and the rest.

## 2NC/1NR — Constitutional Privacy Advantage

### Extend: “Encryption Unconstitutional”

#### Encryption violates the Constitution because it prevents legitimate searches.

Etzioni 15 — Amitai Etzioni, University Professor, Professor of International Affairs, and Director of the Institute for Communitarian Policy Studies at George Washington University, former Professor of Sociology at Columbia University, holds a Ph.D. in Sociology from the University of California-Berkeley, 2015 (“The Ultimate Encryption Debate,” *The Huffington Post*, July 13th, Available Online at http://www.huffingtonpost.com/amitai-etzioni/the-ultimate-encryption-d\_b\_7788064.html, Accessed 08-12-2015)

I have been called "irresponsible" by one of the greatest cryptographers, the famous Ronald Rivest of MIT. (His name provided the "R" in RSA, a computer security firm and a widely used encryption scheme, on both of which he worked.) I gained that dubious distinction for arguing that a new form of encryption is not merely the techies' major gift to terrorists and criminals -- but also a gross violation of the constitution! Hence, it should be outlawed. Rivest states that "it is irresponsible for Etzioni to reach the conclusions he does without providing a plausible technical approach to achieving his stated goal (banning strong encryption) that doesn't incur immense costs to our national security."

What happened is that the techies developed a new form of encryption -- I call it the ultimate encryption -- that only the sender and receiver can decipher. Apple built it into its phone so both the information stored in the phone and the messages sent are completely secure. (If you forget the password, Apple cannot help you, because it cannot decode the information encrypted in the new way). Google and other tech companies are following suit.

Senior law enforcement officials in the U.S. and UK have have expressed alarm about the risks posed by these developments. FBI Director James Comey warned that the advance of "default encryption settings and encrypted devices and networks" will have "very serious consequences for law enforcement and national security agencies at all levels." There were akin to "building cars whose trunks the government could not open" and put terrorist and kidnappers "beyond [the reach of] the law."

Government officials hence asked the tech firms to ensure their capacity to "comply with lawful court orders" by incorporating a "lawful intercept solution" into their products. However, on July 6, 15 computer security specialists including Rivest responded that any such changes would damage our security -- because whatever backdoor they would provide the government to read the encrypted information -- could also be used by cyber criminals. I argued, on the other hand, that the damage ultimate encryption inflicts on security is too high a cost to pay -- and that it should be treated as an "inherently dangerous product," as we treat plastic guns, which we ban because the TSA cannot detect them.

The main point here is that the Constitution never banned all searches; it states that only unreasonable ones are prohibited. And it provides a way to establish what is responsible: show a judge that there is sufficient evidence to hold that a particular person may be a terrorist or a serious criminal. This is the gold standard civil libertarians and libertarians have insisted on for decades.

Now come Professor Rivest and a few of his colleagues, consulting no one – no public, no court or legislature – and declaring that they are entitled to prevent the Constitution from being applied. They will provide one and all with a ready-made way to prevent the government from doing any searches on smart phones and the communications and transactions of their owers even when these searches are perfectly legal and necessary. To put it differently: we are accustomed to draw on the constitution to protect us from government overreach. Here we ought to note that we need to draw on the Constitution in order to have the government that can protect us.

As to my not providing a technical solution, it actually is completely reasonable for me and you to challenge what Rivest, et al. are doing without having a fix, just as it is ok for us to demand that someone stop spreading Ebola even if we do not have a suitable vaccine. But I do have a solution for end-to-end encryption of communications: make it a two step process. Have the client send an encrypted message to Apple. Have Apple re-encrypt the message and send it to its final recipient -- and keep a copy (encrypted of course) in a new Apple vault. To further enhance security, Apple would keep the passwords and identities of the senders and recipients in a different vault than the content of the messages themselves. It would allow the government to read the content of a person's messages only on presenting a court-authorized search warrant based on individualized suspicion. (If you don't trust FISA -- some other federal court). And Apple should invite the Israelis to provide the new vault with the security measures they used to protect the secrets of Dimona for decades from leaking.

Mr. Rivest is welcome to do better. But if he is a responsible American, he has a duty to help do his best to find a reasonable balance between privacy and security and not to slaughter one on the altar of the other. He who sacrifices security for sake of privacy will have neither.

#### Encryption violates the Fourth Amendment — it impedes legal searches.

Rogers 15 — Mike Rogers, National Security Commentator for CNN, former Member of the United States House of Representatives (R-MI) where he served as Chairman of the Permanent Select Committee on Intelligence, 2015 (“Encryption a growing threat to security,” *CNN*, August 1st, Available Online at http://www.cnn.com/2015/08/01/opinions/rogers-encryption-security-risk/, Accessed 08-12-2015)

Unfortunately, the tech industry argues that Americans have an absolute right to absolute privacy. But while Americans absolutely do have a right to privacy, the Constitution both provides protections and offers a path for the government to pursue illegal behavior. Indeed, the criteria for securing a warrant is well established in the law, and we do not have to sacrifice Fourth Amendment protections to fix this growing problem. If technology companies build encryption systems where only they retain access, then when necessary, law enforcement would be able to follow the appropriate legal process to obtain the suspected bad actors' records. It is really that simple.

This is not the first time in America's history that private industry has been asked by society through law enforcement to strike the proper balance between profit and public interest. American companies should be able to make a profit and protect innocent users' privacy, while still allowing law enforcement to be able to catch the world's worst criminals and terrorists with time-tested legal measures.

If landlords have the moral responsibility to protect a community from illegal use of their property, shouldn't tech companies have the same moral responsibility to protect the broader online community from illegal use of their property?

So yes, the tech industry should continue to encrypt communications to offer citizens privacy. But they should also keep a master key, because it may one day save thousands of lives. Americans' privacy is protected every day by laws that prevent police from entering a criminal's home without a warrant. Why should the rules or risks be any different in cyberspace?

If we can work together on this difficult problem, I know we will find a solution. Let's not create a new threat for profit's sake.

### Extend: “Privacy Already Dead”

#### Private sector threats to privacy are more serious. Government surveillance is vital to counteract them.

Simon 14 — William H. Simon, Arthur Levitt Professor of Law at Columbia University, Gertrude and William Saunders Chair Emeritus at Stanford Law School, holds a J.D. from Harvard Law School, 2014 (“Rethinking Privacy,” *Boston Review*, October 20th, Available Online at <https://www.bostonreview.net/books-ideas/william-simon-rethinking-privacy-surveillance>, Accessed 08-07-2015)

The critics’ preoccupation with the dangers of state oppression often leads them to overlook the dangers of private abuse of surveillance. They have a surprisingly difficult time coming up with actual examples of serious harm from government surveillance abuse. Instead, they tend to talk about the “chilling effect” from awareness of surveillance.

By contrast, there have been many examples of serious harm from private abuse of personal information gained from digital sources. At least one person has committed suicide as a consequence of the Internet publication of video showing him engaged in sexual activity. Many people have been humiliated by the public release of a private recording of intimate conduct, and blackmail based on threats of such disclosure has emerged as a common practice. Some of this private abuse is and should be illegal. But the legal prohibitions can only be enforced if the government has some of the surveillance capacities that critics decry. Illicit recording and distribution can only be restrained if the wrongdoers can be identified and their actions effectively restrained. Less compromising critics would deny government these capacities.

With low crime rates and small risks of terrorism in the United States, privacy advocates do not feel compelled to address the potential chilling effect on speech and conduct that arises from fear of private lawlessness, but we do not have to look far to see examples of such an effect abroad and to recognize that its magnitude depends on the effectiveness of public law enforcement. To the extent that law enforcement is enhanced by surveillance, we ought to recognize the possibility of a warming effect that strengthens people’s confidence that they can act and speak without fear of private aggression.

#### Corporations are more likely to violate privacy than government.

Callahan 13 — David Callahan, Senior Fellow at Demos—a U.S.-based research and policy center, former Fellow at the Century Foundation, holds a Ph.D. in Politics from Princeton University, 2013 (“How Could Cato Think That Government Poses a Bigger Threat to Privacy Than Corporations?,” *PolicyShop*—a Demos blog, November 27th, Available Online at <http://www.demos.org/blog/11/27/13/how-could-cato-think-government-poses-bigger-threat-privacy-corporations>, Accessed 08-05-2015)

The Cato Institute claims to be a leading defender of individual liberty, and in that role, it has endlessly sounded the alarm about government surveillance and other state encroachments on people's privacy. Weirdly, though, Cato rarely mentions even bigger threats to privacy from corporations.

That's quite a blind spot. After all, who spends more time and energy scouring the details of your life: The U.S. government or Google? Who is more likely to track everything you buy, everyplace you go, what you eat, and how you vote – the geeks at the NSA or consumer data firms like Acxiom, which is said to have information on 500 million consumers worldwide, including nearly every adult in the U.S., with up to 1,500 data points per person? Who is more likely to materially affect your life chances – say, for getting a mortgage or a job—federal intelligence agencies or private credit rating agencies, including those that sell information about your borrowing history or criminal record that may be incorrect? Finally, what's scarier to you—the idea that your medical records and genetic information could end up in the hands of health and life insurance companies or end up in some computer at the U.S. Department of Health and Human Services?

The answers to these questions seem pretty clear: Private entities not only have a lot more information about our lives, they are more likely to misuse that information in ways that adversely affect our lives. Just look at Demos' research about how employee credit checks bar people from jobs they desperately need—even though there is no evidence that one's credit history predicts job performance. Or look at the studies of how errors in credit reports lead people to have lower credit scores and thus pay more for loans.

When was the last time that the NSA increased anyone's mortgage payments?

I'm not saying that government intelligence agencies don't pose a threat to our liberties. They do, and there is a long history of such agencies abusing their powers to monitor and repress domestic dissent. Scary stuff. But most people have come to recognize that surveillance capacities of corporations are pretty damn scary, too. And, in fact, polls show that Americans are concerned about both private and public threats to privacy and want better controls in each sphere—including tighter regulations of corporations.

### Extend: “No Impact To Privacy”

#### Ordinary people have nothing to fear from surveillance agencies. Aff authors are answering a strawperson argument.

Wittes 14 — Benjamin Wittes, Senior Fellow in Governance Studies at the Brookings Institution, Editor in Chief of Lawfare, Member of the Task Force on National Security and Law at the Hoover Institution, 2014 (“Why Glenn Greenwald's Challenge is Asking the Wrong Question,” *Lawfare*—a national security blog curated by the Brookings Institution, January 14th, Available Online at https://www.lawfareblog.com/why-glenn-greenwalds-challenge-asking-wrong-question, Accessed 08-07-2015)

Indeed, when people make the argument that they don't fear government surveillance because they have nothing to hide, they are generally not contending that they have no secrets they want to keep from anyone or that they want their entire lives exposed to the public. People who genuinely believe that install webcams in their bedrooms. The claim that one has nothing to hide is not a claim that one's dignity could survive malicious intrusion by a reporter devoted maximally to embarrassing one with full access to one's stuff. It's not a claim either that the Stasi couldn't find something on one.

The claim, rather, is more modest. It's a claim that one does not fear law enforcement and intelligence entities operating within their lawful powers as set by democratic institutions, subject to constitutional constraint, and faced with competing priorities. It's a statement that one has a basic comfort level with the power of these entities to collect material because one believes the laws and rules will protect one if followed and one believes as well that they will be followed. It's a statement that the speaker believes that no rational intelligence or law enforcement agency would devote energy to investigating the speaker, because he or she hasn't done anything worth the attention of those agencies—being basically a law-abiding person in a world full of serious law enforcement intelligence threats. And it's a statement of comfort with the fact that should one's material be swept up in the course of investigations of others, that would be a bummer—but one the speaker's dignity could survive because it's not juicy enough to spark sustained interest. In other words, it's a statement of belief on the speaker's part that the collection powers of the state will not be maliciously directed against the speaker.

#### Surveillance authority *won’t* be abused — there is aggressive oversight.

Liepman 13 — Andrew Liepman, Senior Policy Analyst at the RAND Corporation, former Principal Deputy Director of the National Counterterrorism Center, served in the Central Intelligence Agency for over 30 years, holds a B.S. in Forestry from the University of California-Berkeley, 2013 (“What did Edward Snowden get wrong? Everything,” *Los Angeles Times*, August 10th, Available Online at <http://articles.latimes.com/2013/aug/10/opinion/la-oe-0811-liepman-snowden-and-classified-informat-20130811>, Accessed 08-07-2015)

Let me break this to you gently. The government is not interested in your conversations with your aunt, unless, of course, she is a key terrorist leader. More than 100 billion emails were sent every day last year — 100 billion, every day. In that vast mass of data lurk a few bits that are of urgent interest and vast terabytes of tedium that are not. Unfortunately, the metadata (the phone numbers, length of contact, and so forth, but not the content of the conversations) that sketch the contours of a call to your family member may fall into the same enormous bucket of information that includes information on the next terrorist threat. As Jeremy Bash, the former chief of staff of the CIA, memorably put it, "If you're looking for a needle in the haystack, you need a haystack."

Unfortunately, during the Snowden affair, many news outlets have spent more time examining ways the government could abuse the information it has access to while giving scant mention to the lengths to which the intelligence community goes to protect privacy. We have spent enormous amounts of time and effort figuring out how to disaggregate the important specks from the overwhelming bulk of irrelevant data.

This is done under tight and well-thought-out strictures. I witnessed firsthand the consequences of breaking the privacy rules of my former organization, the National Counterterrorism Center. As the center's deputy director, I had to fire people, good people, and remove others from their posts for failing to follow the rules about how information could be accessed and used. It didn't happen often, and it was never a malicious attempt to gather private information. We had mandatory training and full-time staffers to supervise privacy regulations. We used precious resources to hire lawyers and civil liberties experts to oversee our efforts. And on those few occasions when we made mistakes, the punishments were swift and harsh.

### Extend: “Weigh Consequences”

#### The Constitution is an open-ended framework, not a “side constraint.”

Litchwick 11 — Dahlia Lithwick, journalist covering courts and the law for *Slate*, 2011 (“Read It and Weep,” *Slate*, January 4th, Available Online at http://www.slate.com/articles/news\_and\_politics/jurisprudence/2011/01/read\_it\_and\_weep.single.html, Accessed 04-30-2012)

This newfound attention to the relationship between Congress and the Constitution is thrilling and long overdue. Progressives, as Greg Sargent points out, are wrong to scoff at it. This is an opportunity to engage in a reasoned discussion of what the Constitution does and does not do. It's an opportunity to point out that no matter how many times you read the document on the House floor, cite it in your bill, or how many copies you can stuff into your breast pocket without looking fat, the Constitution is always going to raise more questions than it answers and confound more readers than it comforts. And that isn't because any one American is too stupid to understand the Constitution. It's because the Constitution wasn't written to reflect the views of any one American.

The problem with the Tea Party's new Constitution fetish is that it's hopelessly selective. As Robert Parry notes, the folks who will be reading the Constitution aloud this week can't read the parts permitting slavery or prohibiting cruel and unusual punishment using only their inside voices, while shouting their support for the 10th Amendment. They don't get to support Madison and renounce Jefferson, then claim to be restoring the vision of "the Framers." Either the Founders got it right the first time they calibrated the balance of power between the federal government and the states, or they got it so wrong that we need to pass a "Repeal Amendment" to fix it. And unless Tea Party Republicans are willing to stand proud and announce that they adore and revere the whole Constitution as written, except for the First, 14, 16th, and 17th amendments, which totally blow, they should admit right now that they are in the same conundrum as everyone else: This document no more commands the specific policies they espouse than it commands the specific policies their opponents support.

This should all have been good news. The fact that the Constitution is sufficiently open-ended to infuriate all Americans almost equally is part of its enduring genius. The Framers were no more interested in binding future Americans to a set of divinely inspired commandments than any of us would wish to be bound by them. As Justice Stephen Breyer explains in his recent book, Making Our Democracy Work: A Judge's View, Americans cannot be controlled by the "dead hands" of one moment frozen in time. The Constitution created a framework, not a Ouija board, precisely because the Framers understood that the prospect of a nation ruled for centuries by dead prophets would be the very opposite of freedom.

#### It is impossible to resolve constitutional issues without weighing costs and benefits. There should be no “decision rules.”

Posner 7 — Richard A. Posner, Judge of the United States Court of Appeals for the Seventh Circuit, Senior Lecturer at the University of Chicago Law School, was identified by *The Journal of Legal Studies* as the most cited legal scholar of the 20th century, holds an L.L.B. from Harvard 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)

Cole’s review does, however, raise an important question, which is whether judges can get away from “balancing” as the method for resolving constitutional disputes in which the stakes are great. Cole is correct that I reject the possibility of resolving such disputes by a distinctively legal methodology involving, in his words, “an effort, guided by text, precedent, and history, to identify the higher principles that guide us as a society”; “the judge’s attempt, informed by text, tradition, precedent, and reason, to identify and enforce those principles that rise above day-to-day cost-benefit analysis”; “we must insist on a Constitution of principle.” Lovely sentiments, but empty. One sees this in Cole’s call for a “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.” So much for guidance by text, for the text of the Fourth Amendment does not require that searches be conducted pursuant to warrants. It places tight limits on warrants; the only limits it places on searches without warrants is that they not be “unreasonable.” Although Cole says that “the Constitution does not trust government officials to balance in some ad hoc fashion the value of the information they hope to obtain from suspects against the harms their tactics may inflict,” a standard of reasonableness is an invitation to do just that, and it is an invitation that the Supreme Court has accepted. Whether electronic surveillance without a warrant is constitutional will turn on whether five Supreme Court Justices think it’s “reasonable.”

David Cole must realize at some level that his ardent civil libertarian views are not the product of “text, tradition, precedent, and reason,” since equally capable legal thinkers hold opposite views. This is possible because there is no consensus on what methodology to use to resolve constitutional disputes and because text, tradition, precedent, and reason so often tug in different directions. As a result, his “higher principles” have no better constitutional pedigree than the “higher principles” that his conservative opponents purport to derive from the same Constitution. The text is very old and to a degree obsolete, tradition is a mixed bag (the Alien and Sedition Acts and Lincoln’s suspension of habeas corpus in the Civil War are part of the tradition), the precedents are mixed as well and many Cole rejects, and “reason” as lawyers use the term is in the eye of the beholder. Realism requires recognition that constitutional decision-making at the highest level (the US Supreme Court) in the most difficult cases is driven in the main by policy judgments based usually on just the kind of balancing that Cole deplores. Or pretends to deplore; for I imagine that au fond the reason he dislikes the administration’s counterterrorism measures is that he thinks they impose greater costs, in harm to civil liberties, than the benefits that they confer in reducing the risk of further terrorist attacks. The rest is rhetoric.

### Extend: “Security Outweighs Privacy”

#### When in conflict, security must always outweigh privacy. Without security, there’s no value to privacy.

Himma 7 — Kenneth Einar Himma, Associate Professor of Philosophy at Seattle Pacific University, holds a Ph.D. in Philosophy from the University of Washington and a J.D. from the University of Washington Law School, 2007 (“Separation, Risk, and the Necessity of Privacy to Well-Being: A Comment on Adam Moore's Toward Informational Privacy Rights,” *San Diego Law Review* (44 San Diego L. Rev. 847), Fall, Available Online to Subscribing Institutions via Lexis-Nexis)

IV. Why We Care about Privacy: Because it Conduces to Security Interests

Even in these cases, my principal concern is to protect some aspect of my security. I do not, for example, conceptualize identity theft, the principal concern here, as a threat to privacy. It is rather a threat to my financial security that can cause me great trouble in taking out loans or retaining property that has been paid for by loans. Much of what seems to be, on the surface, a concern with privacy is really, at bottom, a concern for material security — suggesting that, at the end of the day, privacy is not, other things being equal, as important as security.

This brings me to my second concern with the argument. I think there are a couple of problems with Moore's approach to balancing privacy and security. First, I think the requirement that probable cause be shown before privacy can be breached in the interest of security is far too onerous. Indeed, if this requirement were correct, then it would follow [\*855] that passenger bags could not be searched prior to check-in without obtaining a warrant based on probable cause from a magistrate. While I cannot say that I agree with every regulation that the Federal Aviation Administration has adopted with respect to airport security, or for that matter with every provision of the USA PATRIOT Act, n20 it seems clear that submitting all carry-on bags to x-ray inspection prior to boarding a flight is an infringement of privacy that is justified by security concerns. Moore's analysis implies that this general requirement is not justified - which strikes me as a counterexample to his analysis. n21

Second, it seems clear to me that security trumps privacy, other things being equal - and many arguments can be, and have been, made in support of this proposition. n22 One cannot, for example, enjoy the benefits of any other interest, including privacy, if security interests are not generally protected. The protection of security is a necessary prerequisite for the exercise of any other interest that gives rise to a moral right of some kind.

From an intuitive standpoint, it seems clearly rational to prefer security to privacy in cases where the most egregious breach of one or the other is threatened. I would rather disclose the most private piece of information about myself than suffer death, grievous bodily injury, or even loss of financial security (say, through loss of a job). Indeed, I would view anyone who made a conflicting valuation in need of therapy. It seems clear from an intuitive standpoint that, other things being equal, security wins in a conflict with privacy.

Finally, security interests tend to be valued intrinsically (namely, as ends in themselves), while informational privacy is generally valued instrumentally (as a means to another end). Although it is true that I sometimes value solitude for its own sake, in addition to its value in enabling me to rest, I am not convinced solitude is an interest that falls under the rubric of informational privacy. There is much information about me that I regard as private and want protected not because I value privacy for its own sake, but rather because of the problems that information might cause for me with employers or insurance companies. Much else that I value as private is contingent: people do, while dogs do not, feel a [\*856] need to use the bathroom in private. That preference on our part is not hardwired into us as necessary to our well-being, but is rather the result of social conventions that have evolved over time and might very well change in the future.

In contrast, I am hardwired to value my life and freedom from grievous bodily injury and severe pain and to value them, at least in part, as ends in themselves — rather than as means to ends. It is true that my continuing sentient existence also has instrumental value to me. I cannot have fun of any kind without being conscious. But I value it as an end in itself, to be valued for its own sake. I would not judge someone who does not care at all about privacy interests as necessarily being in need of mental therapy. I would, on the other hand, judge someone who did not care at all about security interests as being in need of mental therapy.

In closing, I should point out that no one who takes the view, as I do, that - other things being equal - security trumps privacy is committed to claiming that "any increase in security should be preferred to any increase in privacy or any decrease in privacy is to be preferred to any decrease in security." n23 Sometimes it makes sense to give up a little security to protect a lot of privacy. I should also point out that the security trumps privacy view does not logically entail, contra Moore, that those who provide security are completely trustworthy. Indeed, I do not trust the Bush Administration very much at all these days, but I still think it is as clear as anything can be that security wins in direct conflicts with privacy. It is, of course, a difficult and contentious issue when privacy and security come into direct conflict, but I think it is clear that when they do, the security interests have to win. Civilized life is not possible otherwise.

But the main point here is that while security is essential to well-being, privacy is primarily valuable insofar as it conduces to security interests. And this connection is contingent, as Moore's own risk argument makes clear. We value privacy because it is conducive to avoiding those in a society contingently organized like ours with bigots and profiteers willing to dispose of someone on the basis of private information. But this just speaks to contingent qualities of human beings. Accordingly, while well-being is not possible without security, it is possible without privacy - even if we live in a society where the contingent features of the society continue to expose risks to our well-being through disclosure of private information. But while privacy is not an essential constituent of well-being, security is. Therefore, Moore's argument for Premise One fails.

#### Intuitively, security is more important than privacy. We would *all* give up our privacy rather than be killed or seriously injured.

Himma 7 — Kenneth Einar Himma, Associate Professor of Philosophy at Seattle Pacific University, holds a Ph.D. in Philosophy from the University of Washington and a J.D. from the University of Washington Law School, 2007 (“Privacy Versus Security: Why Privacy is Not an Absolute Value or Right,” *San Diego Law Review* (44 San Diego L. Rev. 857), Fall, Available Online to Subscribing Institutions via Lexis-Nexis)

V. The Argument from Intuitive Case Judgments

From an intuitive standpoint, the idea that the right to privacy is an absolute right seems utterly implausible. Intuitively, it seems clear that there are other rights that are so much more important that they easily trump privacy rights in the event of a conflict. For example, if a psychologist knows that a patient is highly likely to commit a murder, then it is, at the very least, morally permissible to disclose that information about the patient in order to prevent the crime - regardless of whether such information would otherwise be protected by privacy rights. Intuitively, it seems clear that life is more important from the standpoint of morality than any of the interests protected by a moral right to privacy.

Still one often hears - primarily from academics in information schools and library schools, especially in connection with the controversy regarding the USA PATRIOT Act - the claim that privacy should never be sacrificed for security, implicitly denying what I take to be the underlying rationale for the PATRIOT Act. This also seems counterintuitive because it does not seem unreasonable to believe we have a moral right to security that includes the right to life. Although this right to security is broader than the right to life, the fact that security interests include our interests in our lives implies that the right to privacy trumps even the right to life - something that seems quite implausible from an intuitive point of view. If I have to give up the most private piece of information about myself to save my life or protect myself from either grievous bodily injury or financial ruin, I would gladly do so without hesitation. There are many things I do not want you to know about me, but should you make a credible threat to my life, bodily integrity, financial security, or health, and then hook me up to a lie detector machine, I will truthfully answer any question you ask about me. I value my privacy a lot, but I value my life, bodily integrity, and financial security much more than any of the interests protected by the right to privacy.

It is true, of course, that the hierarchy defined by my personal attributions of value may not reflect the hierarchy implied by the moral values themselves, but I would be surprised if there are any rational persons who would react differently to the choice presented above. Personal valuations can be idiosyncratic and for this reason not tell us [\*877] anything about the corresponding moral values. But if it is true, as I would hypothesize, that very few, if any, people would choose to withhold some piece of private information about themselves if needed to save their lives, or protect them from serious physical injury or financial ruin, that is a pretty good reason to think that these valuations do tell us something about morality. It would be very odd if, on the one hand, all, or nearly all, rational persons assign greater value to what I have described as the most important of security interests than to the most important of privacy interests where there is a genuine conflict between the two but, on the other hand, morality assigned more value to privacy than to security.

## 2NC/1NR — Tech Leadership Advantage

### Extend: “Alternate Causality – STEM”

#### Contrarians are wrong — there *is* a STEM shortage.

Rothwell 14 — Jonathan Rothwell, Fellow at the Metropolitan Policy Program at the Brookings Institution, former Senior Research Analyst at Haver Analytics, holds a Ph.D. in Public Affairs from Princeton University and an M.A. in Economics from New School University, 2014 (“Short on STEM Talent,” *U.S. News & World Report*, September 15th, Available Online at <http://www.usnews.com/opinion/articles/2014/09/15/the-stem-worker-shortage-is-real>, Accessed 08-09-2015)

It should be well-accepted that the U.S. economy could use more workers with high levels of knowledge in science, technology, engineering and mathematics. The shortage of these skilled STEM professionals eased during the recession, but by any conventional definition, now it appears to have returned.

For one thing, wages have grown relatively fast in most STEM-oriented occupations, which is a clear indication of a shortage. From 2000 to 2013, analyzing Bureau of Labor Statistics data and adjusting for inflation, median salaries for workers in computer and mathematical, health care practitioner, engineering, and science occupations rose 8 percent, 7 percent, 6 percent and 5 percent respectively, even as those for the average U.S. worker showed no growth. Software developers, for instance, saw salaries soar 26 percent over the same period, culminating in an average of $82,000 in 2013, up from $48,000 in 1980. More broadly, an analysis I completed earlier this summer for the Brookings Institution of census data showed a large relative increase in the STEM earnings premium – about 60 percent – from 1980 to 2012, controlling for education, experience and gender.

In addition, vacancies for STEM jobs are going unfilled in large numbers. My recent report analyzes this phenomenon using a rich database with millions of vacancies posted on company websites compiled by Burning Glass, a labor market analytics firm. There are some 40,000 computer science bachelor’s degree earners each year but roughly 4 million job vacancies for computer workers. In all, the median duration of advertising for STEM vacancies is more than twice that of those in other fields.

Moreover, many people are economically better off with STEM skills. It’s often noted that college graduates outearn those with only high school diplomas, and among workers with college degrees, STEM majors earn some of the highest salaries.

Likewise, jobs are more plentiful in STEM fields, which is why the unemployment rates are low for grads with these degrees. According to the Conference Board, there are currently three job vacancies advertised online for every unemployed computer worker; by contrast, there are more than six unemployed construction workers per vacancy.

Oddly, a small contrarian group of academics claims that not only is there no shortage of STEM talent, but the U.S. actually has too many graduates in these fields. They say that universities oversupply such grads, citing statistics showing that many computer science majors work in other occupations, for example. In fact, the skills of these graduates are highly valued beyond a narrow subset of occupations, further evidence of STEM’s high demand. Indeed, computer science degree holders are commonly employed in managerial positions, business operations, engineering, and even as top executives – hardly evidence of a wasted education.

#### Prefer our evidence — their authors misrepresent the data.

Nager and Atkinson 15 — Adams B. Nager, Economic Research Analyst at the Information Technology and Innovation Foundation, holds an M.A. in Political Economy and Public Policy and a B.A. in Economics and Political Economy from Washington University in St. Louis, and Robert D. Atkinson, Founder and President of the Information Technology and Innovation Foundation, Co-Chair of the White House Office of Science and Technology Policy’s China-U.S. Innovation Policy Experts Group, Member of the U.S. State Department’s Advisory Committee on International Communications and Information Policy, Member of the U.S. Department of Commerce’s National Advisory Council on Innovation and Entrepreneurship, Member of the Markle Foundation Task Force on National Security in the Information Age, serves on the boards or advisory councils of the Internet Education Foundation, the NetChoice Coalition, the University of Oregon’s Institute for Policy Research and Innovation, and the State Science and Technology Institute, has held positions in the Clinton, Bush, and Obama Administrations, holds a Ph.D. in City and Regional Planning from the University of North Carolina-Chapel Hill, 2015 (“Debunking the Top Ten Arguments Against High-Skilled Immigration,” Report by The Information Technology & Innovation Foundation, April, Available Online at <http://www2.itif.org/2015-debunking-myths-high-skilled.pdf>, Accessed 08-09-2015, p. 1-2)

Until recently there was widespread agreement that the United States faced a shortage of science, technology, engineering, and mathematics (STEM) workers. However, that consensus has begun to fracture, largely due to an assertive campaign by some liberal economists more interested in protecting the salaries of high-wage professionals than in helping the broad base of American consumers and workers. In particular, in their single-minded campaign to eliminate the H-1B visa program, these advocates have engaged in a determined effort to cast doubt on the reality of the U.S. STEM shortage.

Introduction

For leading advocates who make this claim, such as Ron Hira, Hal Salzman, and Michael Teitelbaum, economic policy reflects a fundamental tension between capital and labor: if capital gets less, labor gets more. One way of ensuring capital gets less is to restrict the supply of labor so that businesses must bid up wages. To be sure, these labor advocates have every right to make this argument, but they should be upfront about their real agenda and its implications, including on progressivity. Engineers, for example, earn 2.5 times the median national wage with a median yearly income of $88,720. 1 This places them in the top 5 percent of single income earners.2 Why is it progressive to raise their incomes by restricting the supply of STEM workers, when the result would be fewer jobs in the rest of the economy, higher prices for American consumers of all incomes, and reduced U.S. global competitiveness? Indeed, limiting the supply of STEM professionals in the United States will raise prices for consumers, reduce the output of U.S. firms in globally traded [end page 1] sectors (like manufacturing and software), and cost the jobs of tens of thousands of Americans who work alongside engineers and IT professionals.

When pressed, some of these advocates will privately acknowledge that the United States would be better off with more STEM workers, whether from increased domestic education and training or more immigration, but their intense opposition to the H-1B high-skilled immigration program leads them to argue publically that there is an over-abundance of STEM labor. As such the “no STEM worker shortage” camp makes a number of claims that are simply not supported by the evidence.

Recent testimony from Hal Salzman and Ron Hira before the Senate Judiciary Committee provides a handy guidebook for these flawed claims.3 According to them: 1) there is no unmet demand for STEM skills; 2) foreign STEM workers displace native STEM workers, especially recent graduates, competing for the same limited pool of jobs; 3) a rising supply of STEM labor depresses wages, harming American workers and discouraging students from entering STEM fields; 4) immigration is a foot in the door for foreign companies who want to compete in American markets; and 5) U.S. companies can remain competitive without high-skilled immigration. Unfortunately, all of those points are wrong or misleading. America faces a shortage of high-skilled STEM talent, especially in IT industries.

This report identifies these and other claims made by labor advocates and refutes each myth.

Myths Surrounding High-Skilled Immigration

Myth 1: Data disprove the STEM shortage

A common tactic for opponents of the H-1B program is to accuse industry of making up the STEM shortage in order to gain access to cheaper labor, claiming that the data proves that the shortage does not actually exist. For example, Salzman’s testimony claims that a “preponderance of evidence” shows the STEM shortage is a myth, while he dismisses data supporting the shortage of STEM workers as “largely based on anecdotal evidence and testimonials from employers, rather than solid evidence.”4

There are data sources that would seem to support Salzman’s dismissal. However, many of these metrics are poorly constructed or intentionally misleading. Advocates for artificially constraining the STEM labor supply then adopt them, misinterpret them and present weak arguments as fact. For example, a Census Bureau definition of STEM which includes psychology and political science majors has been used to claim that STEM graduates do not go into STEM fields, and therefore the United States has excess labor. Hira’s testimony uses anecdotal wage evidence to insinuate that H-1B workers are paid up to 49 percent less than native workers when in reality wages are comparable.5

In addition, many arguments against high-skilled immigration begin with stories about individuals in STEM fields who have been unable to find work. While this is indeed troublesome, the plural of anecdote is not data, and in reality these are relatively isolated incidents. Unemployment in STEM fields is actually very low.6

### Extend: “Alternate Causality – Taxes”

#### Tech companies are *forced* to move money overseas because of a broken U.S. tax system. This is a huge barrier to industry growth.

Turrentine 13 — Dan Turrentine, Vice President of Government Relations and Business Development at TechNet—the preeminent bipartisan political network of CEOs and Seniors Executives that promotes the growth of technology-led innovation, 2013 (“Study Misses the Mark; US Tax Policy Locks Out Foreign Profits of American Companies,” *The Huffington Post*, January 29th, Available Online at <http://www.technet.org/op-eds-articles/>, Accessed 08-10-2015)

Last week, the Citizens for Tax Justice released a study about the money U.S. based-companies technology companies have overseas. Unfortunately, the entire premise of the study misses the forest for the trees.

The United States economy today faces intense global competition for economic advantages, particularly in innovation-based, high-wage industries. We are currently one of only six other Organization for Economic Cooperation and Development (OECD) countries (Chile, Ireland, Korea, Mexico, and Poland) that use a worldwide tax regime in which foreign earnings are subject to domestic tax when remitted home (the difference between the jurisdiction where the earnings occurred and the American corporate rate). Importantly, the other five nations have a much lower corporate tax rate than the United States.

To add further insult to injury, many of the most prominent U.S. technology companies did not exist or existed in a very different form when our tax code was last rewritten in 1986. At the time, a company’s success was largely determined by business in the United States. Today, success is determined by business all over the globe, from here at home to Europe, to the BRICs (Brazil, Russia, India and China), to other emerging markets like Africa.

For many technology companies, the majority of their profits are now earned overseas, ranging from 60 percent to 80 percent. At the same time, the majority of their research and development, ranging from 70 percent to 90 percent, is done in the United States. The fact is that many American high-tech, high-paying jobs are dependent upon their companies success overseas.

The answer to making America more competitive and to maintaining our title as the innovation capitol of the world is to lower the corporate tax rate and move to a competitive, market-based territorial tax system. Advocating for both higher taxes and the continuation of a world-wide tax system are wrong for American jobs of today and particularly for American jobs of the future.

#### High taxes are the largest threat to the U.S. tech industry.

Jones 14 — Kara Jones, Intern at *Town Hall*, Student at the University of South Carolina Honors College, citing Curtis S. Dubay, Research Fellow in Tax and Economic Policy at The Heritage Foundation, former Senior Associate at PricewaterhouseCoopers, former Senior Economist for the Tax Foundation, holds an M.A. in Economics from the University of Connecticut and a B.A. in Economics and Leadership Studies from the University of Richmond, 2014 (“Another American Company Goes Abroad, Escaping High Tax Rates,” *Town Hall*, June 23rd, Available Online at <http://townhall.com/tipsheet/karajones/2014/06/23/another-american-company-goes-abroad-escaping-high-tax-rates-n1854843>, Accessed 08-10-2015)

The world’s largest medical technology company, Medtronic, has announced plans to move its corporate headquarters from Minneapolis to Dublin, Ireland. With U.S. corporate tax rate at a mighty 35 percent, one of the highest in the world, it is no wonder Medtronic would rather operate from Ireland, where the tax rate is only 12.5 percent.

Medtronic is already familiar with the global stage, having reached more than 140 countries with its technology. The company is able to make the move overseas by buying out Dublin-based rival Covidien for $42.9 billion. Acquisition and corporate takeover are now legally required for a business to relocate its tax base to another country.

It is important to understand just how detrimental this current tax system is to American business:

Heritage Foundation tax expert Curtis Dubay predicted this trend nearly a year ago, arguing that if the United States didn’t change its destructive corporate tax code, multinational companies would move their business elsewhere.

 “We are the only developed country in the world that attempts to tax the foreign earnings of our businesses, and we do so at the highest rate in the industrialized world,” Dubay said.

“U.S. businesses will keep moving abroad as long as Congress fails to move to a territorial system,” Dubay said.

Medtronic is just one of many American companies that has recently made the switch to having a foreign executive base. We saw a strikingly similar transition in 2012 with electrical equipment manufacturer Eaton, who also acquired an Irish company and moved its headquarters from Cleveland to Dublin.

### Extend: “Status Quo Solves”

#### The Freedom Act was a big win for the tech industry — it restored trust.

Schwartz 15 — Eric Hal Schwartz, Technology Reporter at *DC Inno*, holds an M.S. in Science and Medical Journalism from Boston University and a B.A. in Journalism from the University of Arizona, 2015 (“Why the Senate NSA Reform Vote is a Win for Tech Companies,” *DC Inno*, June 1st, Available Online at <http://dcinno.streetwise.co/2015/06/01/nsa-reform-vote-a-win-for-tech-internet-companies/>, Accessed 08-10-2015)

Phone and tech companies have been trying to get something like this reform passed for a long time. McConnell's resistance has not made companies like Google, Facebook as well as phone companies very happy. They've argued that the surveillance has hurt their ability to offer safe and private services and technology to their customers. It's a rare point of unity among tech company trade groups like TechNet, BSA - The Software Alliance and the Internet Association, groups that are more usually butting heads over policy.

"Protecting global Internet users through surveillance reform is of paramount importance to the Internet industry and our member companies, many of whom have expressed strong support for the USA Freedom Act," the Internet Association said in a statement about the USA Freedom Act.

"The bill’s provisions to end overly broad data collection and increased transparency are important steps in restoring trust in the U.S. surveillance regime," BSA said in an emailed comment. "Just as importantly, though, the bill ensures the continued availability of other important national security authorities."

#### The Freedom Act was *sufficient* to restore trust in U.S. companies.

Vijayan 14 — Jaikumar Vijayan, freelance technology writer specializing in computer security and privacy topics, 2014 (“Tech groups press Congress to pass USA Freedom Act,” *ComputerWorld*, September 9th, Available Online at <http://www.computerworld.com/article/2604630/tech-groups-press-congress-to-pass-usa-freedom-act.html>, Accessed 08-10-2015)

As Congress returned from summer recess Monday, several technology and civil rights groups quickly renewed their push for a bill that seeks to put curbs on the bulk collection of phone records and Internet data by the government.

In a letter, representatives of the Computer and Communications Industry Association, the Software Alliance, the Information Technology Industry Council and the Software and Information Industry Association urged Senate lawmakers to quickly approve the USA Freedom Act (S. 2685).

Introduced in July by Sens. Patrick Leahy (D-Vt.), Al Franken (D-Minn.), Mike Lee (R-Utah) and Dean Heller (R-Nev.), the bill would put new limits on the federal government's authority to ask telecommunications companies and Internet service providers for customer records under Section 215 of the USA Patriot Act.

It would also require the secretive Foreign Intelligence Surveillance Act (FISA) Court to be more transparent about its decisions regarding the government's use of FISA to collect data on individuals suspected of terrorist activity. In addition, the USA Freedom Act seeks to limit the use of data collected by entities such as the National Security Agency and the FBI under FISA and the Patriot Act.

Supporters of the bill say the changes are vital to reining in the NSA's domestic surveillance practices.

Concerns over the U.S. government's data collection activities have caused substantial problems for U.S. technology companies over the past year. Former NSA contractor Edward Snowden's leaks about PRISM and other NSA data collection programs have caused U.S. companies to lose customers and business in other countries.

Technology giants like IBM and Cisco have reported blowback from overseas customers as a result of concerns stoked by Snowden's revelations. Some have predicted that U.S. cloud hosting companies could lose tens of billions of dollars over the next few years as overseas customers take their business to foreign rivals.

Many vendors, including Google, Microsoft and others have asked the government for permission to disclose more details about the the kind of customer data they have provided to the government in recent years in response to requests under the Patriot Act and FISA. The companies have argued that such transparency is vital to regaining the confidence of international customers.

It is against this background that the tech groups are calling for quick passage of the USA Freedom Act. Reforms contained in the bill "will send a clear signal to the international community and to the American people that government surveillance programs are narrowly tailored, transparent, and subject to oversight," this week's letter to the senators noted.

U.S. technology companies have experienced losses in overseas markets as a result of the surveillance programs revelations, the letter noted. Other countries are also mulling proposals that would limit free data flows between countries, the letter cautioned.

The measures in the USA Freedom Act would alleviate some of these concerns and would help restore faith in the U.S. government and the U.S. technology sector, the letter said.

### Extend: “No Competitiveness Impact”

#### “Competitiveness” is the wrong focus — it’s a bankrupt metaphor.

Krugman 11 — Paul Krugman, Columnist for the *New York Times*, Professor of Economics and International Affairs at Princeton University, and Recipient of the 2008 Nobel Prize in Economics, 2011 (“The Competition Myth,” *New York Times*, January 23rd, Available Online at http://www.nytimes.com/2011/01/24/opinion/24krugman.html, Accessed 08-11-2013)

Meet the new buzzword, same as the old buzzword. In advance of the State of the Union, President Obama has telegraphed his main theme: competitiveness. The President’s Economic Recovery Advisory Board has been renamed the President’s Council on Jobs and Competitiveness. And in his Saturday radio address, the president declared that “We can out-compete any other nation on Earth.”

This may be smart politics. Arguably, Mr. Obama has enlisted an old cliché on behalf of a good cause, as a way to sell a much-needed increase in public investment to a public thoroughly indoctrinated in the view that government spending is a bad thing.

But let’s not kid ourselves: talking about “competitiveness” as a goal is fundamentally misleading. At best, it’s a misdiagnosis of our problems. At worst, it could lead to policies based on the false idea that what’s good for corporations is good for America.

About that misdiagnosis: What sense does it make to view our current woes as stemming from lack of competitiveness?

It’s true that we’d have more jobs if we exported more and imported less. But the same is true of Europe and Japan, which also have depressed economies. And we can’t all export more while importing less, unless we can find another planet to sell to. Yes, we could demand that China shrink its trade surplus — but if confronting China is what Mr. Obama is proposing, he should say that plainly.

Furthermore, while America is running a trade deficit, this deficit is smaller than it was before the Great Recession began. It would help if we could make it smaller still. But ultimately, we’re in a mess because we had a financial crisis, not because American companies have lost their ability to compete with foreign rivals.

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.

#### Krugman is *right* — “competitiveness” is economically bankrupt.

Schrage 94 — Michael Schrage, writer, consultant and research associate at the Massachusetts Institute of Technology, 1994 (“The Myth of a 'Competitive' Economic Policy,” *Los Angeles Times*, March 10th, Available Online at http://articles.latimes.com/print/1994-03-10/business/fi-32358\_1\_economic-policy, Accessed 08-11-2013)

An American economy that cares a great deal about boosting domestic productivity requires policy-makers who care very little about global competitiveness.

A Zen koan for the nationalistic '90s? The sound of one Keynesian clapping? A lyric for aspiring autarkists?

None on the above. It's the startling pronouncement of MIT's Paul Krugman, one of the country's most brilliant young economists, a nonpartisan academic with a reputation for intellectual honesty and a cruel tongue.

You might recall that Krugman was widely quoted criticizing industrial-policy economist Laura D'Andrea Tyson's research when President Clinton named her chairwoman of his Council of Economic Advisers.

Alternating between statistical scalpels and macroeconomic machetes, Krugman bloodily eviscerates "competitiveness" as a policy doctrine without any kind of economic validity.

What supply-side "economics" was to Reaganomics, Krugman asserts, competitiveness has become to Clintonomics: a sort of psuedo-rational pastiche that Nobel Prize-winning chemist Irving Langmuir once described as "pathological science"--that is to say, no science at all.

"To make a harsh but not entirely unjustified analogy," he says in his essay "Competitiveness: A Dangerous Obsession" in the current issue of Foreign Affairs, "a government wedded to the ideology of competitiveness is as unlikely to make good economic policy as a government committed to creationism is to make good science policy, even in areas that have no direct relationship to the theory of evolution."

"Gee, we must be making progress," smiles Dan Burton, president of the Council of (sigh) Competitiveness, which was formed by frustrated high-tech executives in the wake of the Ronald Reagan Administration's rejection of its own presidential commission on the topic. "In 1987, competitiveness was dismissed as a buzzword. Today, it's graduated to being a dangerous obsession."

Might Krugman be the one with the dangerous obsession? Not after you see the numbers. His arguments would command respect even without his impeccable credentials. They're important because he takes the global competitiveness champions like Tyson, U.S. Trade Representative Mickey Kantor, Labor Secretary Robert B. Reich and health care guru Ira Magaziner on their own terms, impatiently redoes their arithmetic for them and makes a strong case that competitiveness issues amount to little more than a rounding error in the $6-trillion U.S. economy.

### Extend: “No U.S. Leadership Impact”

#### No short-term impact to slow growth — any effect on military power is long-term.

Morgan 11 — Iwan Morgan, Professor of U.S. Studies and Head of U.S. Programmes at the Institute of the Americas at University College London, former Professor of U.S. Studies at the Institute for the Study of the Americas at the School of Advanced Study at the University of London, Professor of American Governance at London Metropolitan University, and Fulbright Educational Exchange Lecturer at Indiana University-Purdue University at Fort Wayne, holds a Ph.D. in International History from the London School of Economics, 2011 (“The American Economy and America’s Global Power,” *The United States after Unipolarity*, Published by the London School of Economics, December, Available Online at http://www.lse.ac.uk/IDEAS/publications/reports/pdf/SR009/morgan.pdf, Accessed 08-11-2013, p. 30)

In immediate terms, it is clear that the United States is far from any tipping point where it has to scale back its military power very significantly because of economic and debt problems at home. True, its supporting rather than lead role in the NATO intervention in Libya owed something to the Obama White House’s desire to contain defence costs while America is still actively engaged against the Taliban in Afghanistan and has just started to run down its Iraq commitments. In Obama’s Fiscal Year (FY) 2012 budget plan, defence outlays are also scheduled to decline from 5.1 percent of GDP in FY 2011 to 3.4 percent of GDP in FY 2016. Nevertheless, the savings will largely result from the running down of commitments in Afghanistan and Iraq and waste elimination rather than the reduction of core strength. Even if a new crisis demanded expansion of military spending in the course of the next decade, the United States should be able to meet that need without imposing a strain on its economy.

#### No leadership impact — the U.S. is *not* indispensable.

Zenko 14 — Micah Zenko, Douglas Dillon Fellow with the Center for Preventive Action at the Council on Foreign Relations, former Research Assistant at the Belfer Center for Science and International Affairs at the Kennedy School of Government at Harvard University, former Researcher at the Brookings Institution, 2014 (“The Myth of the Indispensable Nation,” *Foreign Policy*, November 6th, Available Online at <http://foreignpolicy.com/2014/11/06/the-myth-of-the-indispensable-nation/>, Accessed 08-10-2015)

Indispensables also hold an unrealistic faith in the latent power of leadership that flows from suppose it indispensable-ness. During a House hearing in September, Gerald Feierstein, Principal Deputy Assistant Secretary of State for Near Eastern Affairs, declared: "When the United States stands up and demonstrates resolve and demonstrates a direction, the international community generally supports and falls into place behind." Really? This hypothesis would surprise anyone who tracks multilateral fora where U.S. officials state their policy positions and then repeatedly fail to compel other leaders to get in line — see, for example, the Climate Change Conference in Copenhagen in December 2009, and the WTO trade talks since the Doha Round opened in 2001.

And if Feierstein is referring only to warfare, then why do so few countries with deployable military assets participate in U.S.-led campaigns in a meaningful way? The United States provided the majority of the actual combat forces and airpower in Iraq, Afghanistan, and Libya, and is doing so again in the air campaign to counter the Islamic State (IS). Most countries that could participate have either declined to do so, or are taking part by providing such limited and constrained capabilities that they are not significantly enhancing the coalition’s capabilities. In each of these military interventions, the United States decried unilateralism, attempted to form a large coalition, and then found itself paying most of the costs, dropping most of the bombs, sacrificing the most soldiers, and losing most of his credibility.

Whether it is multilateral talks or military operations, other governments do not do as Washington demands because, quite simply, it is not in their national interests to do so. Moreover, the United States refuses to employ the political will or coercive leverage to force them to. The point being is that few, if any, substantive and enduring foreign-policy activities can be done unilaterally, and asserting one’s indispensability does nothing to alter others’ interests. It is often stated that countries in the Middle East or East Asia are looking for America "to lead," but they actually want U.S. leadership on their terms, and in support of their own narrow objectives. The moment that leadership conflicts with the visions and objectives those countries hold, they cease or severely limit their partnerships with the United States.

Finally, the Indispensables belief that America’s role in the world is "absolutely necessary" in all areas is simply arrogant. It discounts the tremendous and essential contributions from non-U.S. countries, international non-governmental organizations, and civil society. This includes the 128 countries contributing 104,184 troops and police forces currently deployed in support of sixteen U.N. peacekeeping operations worldwide. The United States provides only 113 troops to U.N. peacekeeping operations, but, importantly, foots 27 percent of the bill and provides logistics support. Or, consider the billions of dollars from the Gates Foundation, Norwegian Refugee Council, Mercy Corps, International Red Cross and Red Crescent, and countless others, which improve the lives of the poorest and most in need. Each of these public health, humanitarian, and development organizations offer the deep pockets and political neutrality that allows them access to areas where the United States simply cannot or will not go.

The reason that the United States is not the indispensable nation is simple: the human and financial costs, the tremendous risks, and degree of political commitment required to do so are thankfully lacking in Washington. Moreover, the structure and dynamics of the international system would reject or resist it, as it does in so many ways that frustrate the United States from achieving its foreign policy objectives. The United States can be truly indispensable in a few discrete domains, such as for military operations, which as pointed out above has proven disastrous recently. But overall there is no indispensable nation now, nor has there been in modern history. Indispensables may feel compelled to repeat this feel-good myth, but nobody should believe them.

## 2NC/1NR — Cybersecurity Advantage

### Extend: “Golden Key Solves”

#### A Golden Key system *is* technically feasible — the Internet proves.

Crovitz 15 — L. Gordon Crovitz, Columnist and Former Publisher of *The Wall Street Journal*, former Executive Vice-President of Dow Jones, 2015 (“Why Terrorists Love Silicon Valley,” *Wall Street Journal*, July 5th, Available Online at <http://www.wsj.com/articles/why-terrorists-love-silicon-valley-1436110797>, Accessed 07-20-2015)

Silicon Valley never met a problem it couldn’t solve—until now. Top Internet companies say there is no technical way for them to protect their users’ legitimate privacy with encryption while also enabling intelligence agents and law enforcement to gain access to what terrorists plot online.

FBI director James Comey says Silicon Valley’s no-can-do attitude is “depressing.” Terror attacks are increasingly planned online, outside the reach of intelligence and law enforcement. Islamic State reaches an estimated 200,000 prospects daily through posts on social media. Once a recruit is identified, ISIS tells him to switch to an encrypted smartphone. Legal wiretaps are useless because the signal is indecipherable. Even when the devices are lawfully seized through court orders, intelligence and law-enforcement agencies are unable to retrieve data from them.

“Our job is to find needles in a nationwide haystack, needles that are increasingly invisible to us because of end-to-end encryption,” FBI Director Comey recently told CNN. The FBI says it can no longer estimate how many recruits in the U.S. are communicating with ISIS and other terrorist groups.

Benjamin Wittes, who edits the Lawfare blog for the Brookings Institution, summarized the problem last week: “As a practical matter, that means there are people in the U.S. whom authorities reasonably believe to be in contact with ISIS for whom surveillance is lawful and appropriate but for whom useful signals interception is not technically feasible. That’s a pretty scary thought.” Mr. Wittes asks “whether we really want ISIS to be able to recruit people on Twitter and then have secure communications with them elsewhere. And if we don’t want that, what then?”

Silicon Valley acts as if it’s above having to comply with legal searches. Last year, Apple announced that its iPhone operating system would encrypt data by default. “Unlike our competition,” Apple bragged, “it’s not technically feasible for us to respond to government warrants.” Google now has similar encryption for Android devices, as does Facebook for its WhatsApp app.

Congress requires traditional telephone companies to retain records so that they can be disclosed under court orders. These records and wiretaps are basic tools for preventing terrorism. Silicon Valley executives and lobbyists want their technologies to be exempt.

They need to be reminded that the Fourth Amendment of the Constitution permits reasonable searches and seizures. That creates duties for responsible companies to be able to comply. The original justification for national regulation of electronic communication was self-defense. The Communications Act of 1934, which created the Federal Communications Commission, said “the purpose of the national defense” justified federal oversight of “interstate and foreign commerce in communication by wire and radio.”

Earlier this year Mr. Comey asked Congress to act unless technologists come up with ways of allowing encryption to protect privacy from hackers while also allowing government agencies to conduct legal searches. “Technical people say it’s too hard,” he said. “My reaction to that is: Really? Really too hard? Too hard for the people we have in this country to figure something out? I’m not that pessimistic.”

The head of the National Security Agency, Michael Rogers, proposes that technology companies create digital keys to allow access to smartphones and other devices, with the key divided into pieces so that no company or government agency (or hacker) can gain access to the information on its own. “I don’t want a back door,” he said, meaning unfettered ability to bypass device security. “I want a front door. And I want the front door to have multiple locks.”

Internet executives should know better than anyone that using multiple keys can work—because multiple keys are the means by which the Internet itself is protected. The engineers who designed the Internet applied this approach to ensure the integrity of global Internet addresses and names.

The Internet Corporation for Assigned Names and Numbers, or Icann, requires people acting together to gain access to the core of the Internet. Seven people from around the world meet several times a year, with each bringing an old-fashioned metal key to unlock a safe-deposit box that contains a smartcard. The group then verifies that there has been no tampering with the root zone of Internet names and addresses. Old-fashioned physical keys could likewise be used by Internet companies and government officials acting together to enable court-ordered access.

This week, the Senate Judiciary Committee holds a hearing, “Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy.” Lawmakers aren’t giving up on finding a way to accommodate both of these important interests. Neither should Silicon Valley.

#### Prefer our evidence — crypto experts exaggerate the difficulty of a Golden Key.

Wittes 15 — Benjamin Wittes, Senior Fellow in Governance Studies at the Brookings Institution, Editor in Chief of Lawfare, Member of the Task Force on National Security and Law at the Hoover Institution, 2015 (“Thoughts on Encryption and Going Dark, Part II: The Debate on the Merits,” *Lawfare*—a national security blog curated by the Brookings Institution, July 12th, Available Online at http://www.lawfareblog.com/thoughts-encryption-and-going-dark-part-ii-debate-merits, Accessed 07-13-2015)

Consider the report issued this past week by a group of computer security experts (including Lawfare contributing editors Bruce Schneier and Susan Landau), entitled "Keys Under Doormats: Mandating Insecurity By Requiring Government Access to All Data and Communications." The report does not make an in-principle argument or a conceptual argument against extraordinary access. It argues, rather, that the effort to build such a system risks eroding cybersecurity in ways far more important than the problems it would solve. The authors, to summarize, make three claims in support of the broad claim that any exceptional access system would "pose . . . grave security risks [and] imperil innovation." What are those "grave security risks"?

\* "[P]roviding 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."

\* "[B]uilding in exceptional access would substantially increase system complexity" and "complexity is the enemy of security." Adding code to systems increases that system's attack surface, and a certain number of additional vulnerabilities come with every marginal increase in system complexity. So by requiring a potentially complicated new system to be developed and implemented, we'd be effectively guaranteeing more vulnerabilities for malicious actors to hit.

\* "[E]xceptional access would create concentrated targets that could attract bad actors." If we require tech companies to retain some means of accessing user communications, those keys have to stored somewhere, and that storage then becomes an unusually high-stakes target for malicious attack. Their theft then compromises, as did the OPM hack, large numbers of users.

The strong implication of the report is that these issues are not resolvable, though the report never quite says that. But at a minimum, the authors raise a series of important questions about whether such a system would, in practice, create an insecure internet in general—rather than one whose general security has the technical capacity to make security exceptions to comply with the law.

There is some reason, in my view, to suspect that the picture may not be quite as stark as the computer scientists make it seem. After all, the big tech companies increase the complexity of their software products all the time, and they generally regard the increased attack surface of the software they create as a result as a mitigatable problem. Similarly, there are lots of high-value intelligence targets that we have to secure and would have big security implications if we could not do so successfully. And when it really counts, that task is not hopeless. Google and Apple and Facebook are not without tools in the cybersecurity department.

The real question, in my view, is whether a system of the sort Comey imagines could be built in fashion in which the security gain it would provide would exceed the heightened security risks the extraordinary access would involve. As Herb Lin puts it in his excellent, and admirably brief, Senate testimony the other day, this is ultimately a question without an answer in the absence of a lot of new research. "One side says [the] access [Comey is seeking] inevitably weakens the security of a system and will eventually be compromised by a bad guy; the other side says it doesn’t weaken security and won’t be compromised. Neither side can prove its case, and we see a theological clash of absolutes." Only when someone actually does the research and development and tries actually to produce a system that meets Comey's criteria are we going to find out whether it's doable or not.

### Extend: “Alternate Causality – Workforce”

#### The large workforce shortage is more important than tech issues.

Wang 15 — Nancy Wang, Reporter covering business and technology for Medill News Service, 2015 (“Cybersecurity has a talent shortage,” United Press International, March 10th, Available Online at <http://www.upi.com/Top_News/US/2015/03/10/Cybersecurity-has-a-talent-shortage/3711425913442/>, Accessed 08-12-2015)

The cybersecurity industry is grappling with a new threat: hiring.

Information security experts and executives said the fast-growing cybersecurity field is facing a scarce talent pool, with thousands of positions to fill as demand grows.

"It is pretty much impossible to hire folks within the indicated backgrounds," said Alex Stamos, Yahoo's chief information officer and a world-renowned cybersecurity expert. "There are maybe four or five thousand people in North America I can hire right now who have the technical skills keen to us."

Stamos is one of many U.S. security professionals having trouble hiring people as cyberattacks and data breaches continue to increase. A recent independent survey by the Ponemon Institute, sponsored by IBM, showed that personal information of almost half of the nation's adults — 110 million Americans — was hacked in 2014.

Add to that this data point: The Bureau of Labor Statistics has projected the demand for information security analysts will increase by 37 percent between 2012 and 2022. There will be approximately 100,000 more jobs available in the field of cybersecurity seven years from now, according to the bureau's Occupational Outlook Handbook.

The demand for information security professionals is quickly exceeding the number of people who are capable of doing the job, said Peter W. Singer, former director of the Center for 21st Century Security and Intelligence at Brookings Institute and a strategist at the New America Foundation, a public policy institute.

"We don't have enough expertise in the right places now," said Singer, co-author of a recent book "Cybersecurity and Cyberwar". "We often frame cybersecurity as a technology problem. It is a human problem."

#### There is a critical skills gap in cybersecurity — there aren’t enough qualified workers.

Loeb 15 — Matt Loeb, Chief Executive Officer of ISACA—a global IT association serving 115,000 cybersecurity, risk, and audit professionals, former Staff Executive for the Institute of Electrical and Electronics Engineers and Executive Director of the IEEE Foundation, 2015 (“Cybersecurity talent: Worse than a skills shortage, it’s a critical gap,” *The Hill*, April 17th, Available Online at <http://thehill.com/blogs/congress-blog/technology/239113-cybersecurity-talent-worse-than-a-skills-shortage-its-a>, Accessed 08-12-2015)

The U.S. House of Representatives next week is expected to consider important measures aimed at bulking up American cyber defenses in the wake of numerous and relentless attacks. Leaders from government and the private sector continue to reinforce that cybersecurity is everyone’s business. The problem, however, is that we don’t have the workforce needed to address the challenges before us.

ISACA recently teamed up with RSA Conference to conduct a study entitled “The State of Cybersecurity: Implications for 2015,” which gives detailed insights into this challenge. We surveyed 649 global cybersecurity and IT managers and practitioners to obtain their insights into the depth of the challenge we face, the potential pitfalls and where we need to set our focus.

The results reinforce an increasingly familiar problem: 77 percent of respondents said they experienced an increase in attacks in 2014. And 82 percent of organizations expect to be attacked in 2015. Even more alarming is that less than half of those surveyed believe that their current security teams have the ability to detect and respond to complex incidents. There are simply an insufficient number of qualified, skilled professionals available to do what’s needed to protect organizations and consumers.

While February’s White House Summit at Stanford and the current movement in Congress are steps in the right direction, increased awareness of the talent issue is now urgently needed. We are not just facing a shortage of cybersecurity professionals; it is a gaping skills gap. Just over half of those surveyed, or 52 percent, said that less than a quarter of applicants for cybersecurity positions have the necessary skills for the open position. As a result, 53 percent said it can take three to six months to find a qualified candidate. This means three to six months where a short-staffed security team is trying to fend off cybercriminals while safeguarding intellectual property, sensitive customer data or even critical infrastructure.

### Extend: “No Cyber Impact”

#### Cyber attacks are not existential threats — aff authors exaggerate.

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)

Bamford: Along those lines, one of the things we’re focusing on in the program is the potential extent of cyber warfare. And we show a dam, for example, in Russia, where there was a major power plant under that. This was a facility that was three times larger than the Hoover Dam, and it exploded. One of the turbines, which weighed as much as two Boeing 747s, exploded 50 feet into the air and then crashed down and killed 75 people. And that was all because of what was originally thought was a cyber-attack, but turned out to be a mistaken piece of cyber that was sent to make this happen. It was accidental.

But the point is this is what can happen if somebody wants to deliberately do this, and I don’t think that’s what many people in the U.S. have a concept of, that this type of warfare can be that extensive. And if you could just give me some ideas along those lines of how devastating this can be, not just in knocking off a power grid, but knocking down an entire dam or an entire power plant.

Snowden: So I don’t actually want to get in the business of enumerating the list of the horrible of horribles, because I don’t want to hype the threat. I’ve said all these things about the dangers and what can go wrong, and you’re right that there are serious risks. But at the same time, it’s important to understand that this is not an existential threat. Nobody’s going to press a key on their keyboard and bring down the government. Nobody’s going to press a key on their keyboard and wipe a nation off the face of the earth.

We have faced threats from criminal groups, from terrorists, from spies throughout our history, and we have limited our responses. We haven’t resorted to total war every time we have a conflict around the world, because that restraint is what defines us. That restraint is what gives us the moral standing to lead the world. And if we go, there are cyber threats out there, this is a dangerous world, and we have to be safe, we have to be secure no matter the cost, we’ve lost that standing.

We have to be able to reject disproportionate and unjustified responses in the cyber domain just as we do in the physical domain. We reject techniques like torture regardless of whether they’re effective or ineffective because they are barbaric and harmful on a broad scale. It’s the same thing with cyber warfare. We should never be attacking hospitals. We should never be taking down power plants unless that is absolutely necessary to ensure our continued existence as a free people.

#### Catastrophic cyber attacks are extremely unlikely — tech complexity, image factor, and accident issue.

Conway 11 — Maura Conway, Lecturer in International Security in the School of Law and Government at Dublin City University, 2011 (“Against Cyberterrorism: Why cyber-based terrorist attacks are unlikely to occur,” *Communications of the ACM*, Volume 54, Number 2, February, Available Online to Subscribing Institutions via ACM Online)

Three Arguments Against Cyberterrorism

In my opinion, the three most compelling arguments against cyberterrorism are:

The argument of Technological Complexity;

The argument regarding 9/11 and the Image Factor; and

The argument regarding 9/11 and the Accident Issue.

The first argument is treated in the academic literature; the second and third arguments are not, but ought to be. None of these are angles to which journalists appear to have devoted a lot of thought or given adequate consideration.

In the speech mentioned earlier, FBI Director Mueller observed "Terrorists have shown a clear interest in pursuing hacking skills. And they will either train their own recruits or hire outsiders, with an eye toward combining physical attacks with cyber attacks." That may very well be true, but the argument from Technological Complexity underlines that 'wanting' to do something is quite different from having the ability to do the same. Here's why:

Violent jihadis' IT knowledge is not superior. For example, in research carried out in 2007, it was found that of a random sampling of 404 members of violent Islamist groups, 196 (48.5%) had a higher education, with information about subject areas available for 178 individuals. Of these 178, some 8 (4.5%) had trained in computing, which means that out of the entire sample, less than 2% of the jihadis came from a computing background.3 And not even these few could be assumed to have mastery of the complex systems necessary to carry out a successful cyberterrorist attack.

Real-world attacks are difficult enough. What are often viewed as relatively unsophisticated real-world attacks undertaken by highly educated individuals are routinely unsuccessful. One only has to consider the failed car bomb attacks planned and carried out by medical doctors in central London and at Glasgow airport in June 2007.

Hiring hackers would compromise operational security. The only remaining option is to retain "outsiders" to undertake such an attack. This is very operationally risky. It would force the terrorists to operate outside their own circles and thus leave them ripe for infiltration. Even if they successfully got in contact with "real" hackers, they would be in no position to gauge their competency accurately; they would simply have to trust in same. This would be very risky.

So on the basis of technical know-how alone cyberterror attack is not imminent, but this is not the only factor one must take into account. The events of Sept. 11, 2001 underscore that for a true terrorist event spectacular moving images are crucial. The attacks on the World Trade Center were a fantastic piece of performance violence; look back on any recent roundup of the decade and mention of 9/11 will not just be prominent, but pictures will always be provided.

The problem with respect to cyber-terrorism is that many of the attack scenarios put forward, from shutting down the electric power grid to contaminating a major water supply, fail on this account: they are unlikely to have easily captured, spectacular (live, moving) images associated with them, something we—as an audience—have been primed for by the attack on the World Trade Center on 9/11.

The only cyberterrorism scenario that would fall into this category is interfering with air traffic control systems to crash planes, but haven't we seen that planes can much more easily be employed in spectacular "real-world" terrorism? And besides, aren't all the infrastructures just mentioned much easier and more spectacular to simply blow up? It doesn't end there, however. For me, the third argument against cyberterrorism is perhaps the most compelling; yet it is very rarely mentioned.

In 2004, Howard Schmidt, former White House Cybersecurity Coordinator, remarked to the U.S. Senate Committee on the Judiciary regarding Nimda and Code Red that "we to this day don't know the source of that. It could have very easily been a terrorist."4 This observation betrays a fundamental misunderstanding of the nature and purposes of terrorism, particularly its attention-getting and communicative functions.

A terrorist attack with the potential to be hidden, portrayed as an accident, or otherwise remain unknown is unlikely to be viewed positively by any terrorist group. In fact, one of the most important aspects of the 9/11 attacks in New York from the perpetrators viewpoint was surely the fact that while the first plane to crash into the World Trade Center could have been accidental, the appearance of the second plane confirmed the incident as a terrorist attack in real time. Moreover, the crash of the first plane ensured a large audience for the second plane as it hit the second tower.

Alternatively, think about the massive electric failure that took place in the northeastern U.S. in August 2003: if it was a terrorist attack—and I'm not suggesting that it was—but if it was, it would have been a spectacular failure.

Conclusion

Given the high cost—not just in terms of money, but also time, commitment, and effort—and the high possibility of failure on the basis of manpower issues, timing, and complexity of a potential cyberterrorist attack, the costs appear to me to still very largely outweigh the potential publicity benefits. The publicity aspect is crucial for potential perpetrators of terrorism and so the possibility that an attack may be apprehended or portrayed as an accident, which would be highly likely with regard to cyberterrorism, is detrimental. Add the lack of spectacular moving images and it is my belief that cyberterrorism, regardless of what you may read in newspapers, see on television, or obtain via other media sources, is not in our near future.

So why then the persistent treatment of cyberterrorism on the part of journalists? Well, in this instance, science fiction-type fears appear to trump rational calculation almost every time. And I haven't even begun to discuss how the media discourse has clearly influenced the pronouncements of policymakers.

### Extend: “No Grid Collapse”

#### Cyber attacks *won’t* take down the grid — their evidence is fearmongering.

Richardson 14 — Michelle Richardson, Legislative Counsel at the Washington Legislative Office of the American Civil Liberties Union, former counsel to the House Judiciary Committee where she specialized in national security, civil rights, and constitutional issues for Democratic Ranking Member John Conyers, 2014 (“Cyberalarmism's threat to privacy,” *Al Jazeera America*, March 12th, Available Online at <http://america.aljazeera.com/opinions/2014/3/cybersecurity-nsaalexandersnowden.html>, Accessed 08-12-2015)

When members of Congress talk cybersecurity, it doesn’t take long for the discussion to turn apocalyptic. The Feb. 27 meeting of the Senate Intelligence Committee was no different when Lindsey Graham, R-S.C., asked Gen. Keith Alexander, retiring director of the National Security Agency (NSA) and commander of United States Cyber Command, to describe in 30 seconds what a major cyberattack could do to the United States.

“I think they could shut down the power in the Northeast,” Gen. Alexander responded. “Shut down the New York stock exchange … shut down some of our government networks … impact our transportation areas … water supplies, they could do damage to that.” If something like this occurred, according to Alexander, the wreckage could include thousands of dead Americans and trillions of dollars in damage.

“On the cyber front, you’ve described a Pearl Harbor on steroids,” Graham replied. Alexander did not disagree.

While there are legitimate cyberthreats in the world, these melodramatic hypotheticals don’t help real cyberdefense and deterrence. Instead they serve only to create a sense of urgency around passing rash and overreaching laws that undermine Americans’ privacy even more — a tall task after whistle-blower Edward Snowden’s revelations. (Full disclosure: The American Civil Liberties Union, for which I work, represents Snowden.)

Should you panic or lose sleep over the prospects of a cyber–World War III? No. Don’t unplug and move to a cabin in the woods just yet. As an average person, you are far more likely to be affected by everyday Internet crime that can be thwarted by sensible precautions. If there are immediate risks, it is that your credit card number will be stolen or you will be enticed to click on a phony link and share sensitive information.

But even when talking about sensitive targets that have far-reaching implications, such as electrical grids and government systems, the demonstrated weak points invariably rest with human error — failing to change default passwords, plugging compromised memory sticks into computers or losing entire unencrypted laptops. Of course, this sort of mundane incompetence is not the basis of Jason Bourne movies and isn’t incredibly sexy. The slow grind of fixing these sorts of problems won’t necessarily net contractors large contracts or land a member of Congress on “Meet the Press.”

#### Grid collapse is highly unlikely even if severely attacked — layers of defense.

Chertoff Group 14 — The Chertoff Group, a risk-management and security consulting company, headed by Michael Chertoff, United States Secretary of Homeland Security under President George W. Bush, Employees include Paul A. Schneider, former deputy secretary of DHS, Mark Weatherford, former deputy under-secretary of DHS, and Michael Hayden, a former director of the National Security Agency and the Central Intelligence Agency, 2014 (“Addressing Dynamic Threats to the Electric Power Grid Through Resilience,” The Chertoff Group, November, Available Online at <http://www.chertoffgroup.com/cms-assets/documents/187850-384796.addressing-dynamic-threats-to-the-elec>, Accessed 03-30-2015)

When considering the broad range of threats that could impact the Bulk Power System, electric companies recognize that any single security element or mitigation measure relied on can be defeated or can fail. Therefore, the industry strategically applies what is known as defense-in-depth. Defense-in-depth is an approach to security that is characterized by the layering of security elements to successfully harden a target and mitigate its risk, especially during an attack. Through a layered approach of complementary elements, vulnerabilities can be mitigated and the impact of a negative event greatly reduced.

The defense-in-depth approach is successfully implemented across various industries, including government agencies and the military, to address both cybersecurity and physical threats. Within the electric power industry, the layering of security elements, as well as the creation of fault tolerant design, helps to prevent any single point of failure or wide-scale disruption of grid operations.

Protecting power grid infrastructure and supporting assets, which include physical assets, computer networks, and the control systems that support them, is a top priority for the electric power industry. The industry is proactively working through a variety of industry initiatives with a single goal in mind: strengthening the security, reliability, and resiliency of the electric power grid.

In 2011, the electric power industry sought to proactively and systematically identify threats that, if successful, would result in major consequences and interrupt companies’ ability to generate, transmit, or distribute power. The Threat Scenario Project 3 described the top threat scenarios facing U.S. electric companies, the likely attack paths or target types, and the ways to mitigate or reduce possible areas of weakness or vulnerability. While not a comprehensive security risk analysis and assessment guide for each specific electric facility, the Threat Scenario Project helps electric companies quickly identify areas where security measures are sufficient and where gaps may exist, and begin the dialogue about additional measures that can be taken to help detect, protect against, respond to, and recover from a range of potential threat scenarios. Another example of an initiative to ensure reliability of the grid is the industry’s mutual assistance network, which is a voluntary partnership of electric companies from across the country committed to helping restore power following an emergency situation. This mutual assistance network provides an effective and coordinated effort to immediately mobilize assets and personnel needed to aid with the response and restoration of power under any circumstances.

Coordinated on a regional level through what are known as Regional Mutual Assistance Groups, electric companies request and receive line workers, tree cutting personnel, equipment, spare parts, and other forms of aid to restore critical power service to affected communities and customers.

## 2NC/1NR — Solvency

### Extend: “Plan Gets Circumvented”

#### The plan will be circumvented — “mandate” gets lawyered.

Newman 14 — Lily Hay Newman, Staff Writer and Lead Blogger for *Future Tense*—a partnership of Slate, New America, and Arizona State University, 2014 (“Senator Proposes Bill to Prohibit Government-Mandated Backdoors in Smartphones,” *Future Tense*, December 5th, Available Online at <http://www.slate.com/blogs/future_tense/2014/12/05/senator_wyden_proposes_secure_data_act_to_keep_government_agencies_from.html>, Accessed 06-30-2015)

It's worth noting, though, that the Secure Data Act doesn't actually prohibit backdoors—it just prohibits agencies from mandating them. There are a lot of other types of pressure government groups could still use to influence the creation of backdoors, even if they couldn't flat-out demand them.

Here's the wording in the bill: "No agency may mandate that a manufacturer, developer, or seller of covered products design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product, by any agency."

#### There are loopholes that allow circumvention by FBI *and* NSA.

Cushing 14 — Tim Cushing, Contributor to *Tech Dirt*, 2014 (“Ron Wyden Introduces Legislation Aimed At Preventing FBI-Mandated Backdoors In Cellphones And Computers,” *Tech Dirt*, December 5th, Available Online at <https://www.techdirt.com/articles/20141204/16220529333/ron-wyden-introduces-legislation-aimed-preventing-fbi-mandated-backdoors-cellphones-computers.shtml>, Accessed 06-30-2015)

Here's the actual wording of the backdoor ban [pdf link], which has a couple of loopholes in it.

(a) IN GENERAL.—Except as provided in subsection (b), no agency may mandate that a manufacturer, developer, or seller of covered products design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product, by any agency.

Subsection (b) presents the first loophole, naming the very act that Comey is pursuing to have amended in his agency's favor.

(b) EXCEPTION.—Subsection (a) shall not apply to mandates authorized under the Communications Assistance for Law Enforcement Act (47 U.S.C. 1001 et seq.).

Comey wants to alter CALEA or, failing that, get a few legislators to run some sort of encryption-targeting legislation up the Congressional flagpole for him. Wyden's bill won't thwart these efforts and it does leave the NSA free to continue with its pre-existing homebrewed backdoor efforts -- the kind that don't require mandates because they're performed off-site without the manufacturer's knowledge.