# NSA AFFIRMATIVE

## 1ac Example

### 1ac – NSA overreach Advantage

#### Contention 1 – NSA overreach

#### Executive Order 12333 authorizes foreign surveillance, but the NSA is using it to exploit loopholes to create backdoor access for wholly domestic communications

Arnbak and Goldberg 14- cybersecurity and information law research at the Institute for Information Law, LL.M degree from Leiden University, A Competitive Strategy and Game Theory degree from London School of Economics University of Amsterdam; Associate professor in the Computer Science Department at Boston University, phD from Princeton University, B.A.S.c from University of Toronto (Axel and Sharon, “Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting the Network Traffic Abroad”, Working Paper, June 27, 2014)//TT

Legal Loopholes. In Section 2 we start by describing the current U.S. regulatory framework for intelligence gathering. From public and until-recently secret primary legal sources, three regimes can be distinguished, based on where the surveillance is conducted, and who it targets: 1. Surveillance of domestic communications conducted on U.S. soil under s.215 of the “Patriot Act”; 2. Surveillance of foreign communications conducted on U.S. soil under the “Foreign Intelligence Surveillance Act”; and 3. Surveillance conducted entirely abroad under “Executive Order 12333” (EO 12333) and its minimization policies, notably U.S. Signals Intelligence Directive 18 (“USSID 18”). USSID 18 was drafted and approved within the Executive branch with minimal Congressional or Judicial oversight. The first two regimes are overseen by all three branches of the U.S. government, and currently under scrutiny by the government, media and the general public. The third regime, however, is solely the domain of the Executive branch and has largely been ignored by the public and other branches of Government in recent months, especially since relevant legal documents related to EO 12333 remain classified or redacted. However, according to the N.S.A., this third regime under EO 12333 is the ‘primary legal authority’ for its operations [5, p. 2-3]. Thus, it deserves more attention and careful scrutiny. Working with primary legal sources, many of which have only recently been made public and are still redacted on key issues, we make the following central observation. A surveillance operation falls within the EO 12333 regime when it presumes two connected criteria: it does not intentionally target a U.S. person, and is conducted abroad. If an intelligence agency can construct plausible presumptions that these two criteria have been meet, then the permissive legal regime under EO 12333 can be applied to the surveillance operation. The surveillance is then considered to affect non-U.S. persons, and 4th Amendment protections can thus be circumvented even if the operation primarily affects Americans. Our main hypothesis is therefore that there is loophole for surveillance on Americans from abroad resulting from the following interdependence: (1) the complete absence of legal protection for non-U.S. persons under the U.S. regulatory framework [32,33] creates ‘foreignness’-presumptions under EO 12333 and (2) the technical realities of modern Internet communications. Technical Loopholes. At first blush, one might suppose that a surveillance operation conducted abroad should have no impact on the privacy of Americans. However, in Section 3 we discuss why the technical realities of the Internet mean that American’s network traffic can easily be routed or stored abroad, where it can then be collected under the permissive legal regime of EO 12333. Indeed, we already know of surveillance programs that have exploited this legal loophole. The revealed MUSCULAR/TURMOIL program, for example, illustrates how the N.S.A. presumed authority under EO 12333 to acquire traffic between Google and Yahoo! servers located on foreign territory; this program allegedly collected up to 180 million user records per month abroad, including those of Americans [17]. We also discuss other technical means an intelligence agency can exploit the legal loopholes under EO 12333. Instead of eavesdropping on intradomain traffic (i.e., data sent within a network belonging to a single organization, as in the MUSCULAR/TURMOIL program), these loopholes can be exploited in the interdomain setting, where traffic traverses networks belonging to different organizations. We explain why interdomain routing with BGP can naturally cause traffic originating in a U.S. network to be routed abroad, even when it is destined for an endpoint located on U.S. soil. We also discuss why core Internet protocols – BGP and DNS – can be deliberately manipulated to force traffic originating in American networks to be routed abroad. We discuss why these deliberate manipulations fall within the permissive EO 12333 regime, and how they can be used to collect, in bulk, all Internet traffic (including metadata and content) sent between a pair of networks; even if both networks are located on U.S. soil (e.g., from Harvard University to Boston University).

#### The perception that the NSA is using the XO 12333 back-door to circumvent section 702 is causing a global backlash against US tech companies and driving data localization

**Eoyang, 14** - Mieke Eoyang is the Director of the National Security Program at Third Way, a center-left think tank. She previously served as Defense Policy Advisor to Senator Edward M. Kennedy, and a subcommittee staff director on the House Permanent Select Committee on Intelligence, as well as as Chief of Staff to Rep. Anna Eshoo (D-Palo Alto) (“A Modest Proposal: FAA Exclusivity for Collection Involving U.S. Technology Companies” Lawfare, 11/24, <http://www.lawfareblog.com/modest-proposal-faa-exclusivity-collection-involving-us-technology-companies>

Beyond 215 and FAA, media reports have suggested that there have been collection programs that occur outside of the companies’ knowledge. American technology companies have been outraged about media stories of US government intrusions onto their networks overseas, and the spoofing of their web pages or products, all unbeknownst to the companies. These stories suggest that the government is creating and sneaking through a back door to take the data. As one tech employee said to me, “the back door makes a mockery of the front door.” As a result of these allegations, companies are moving to encrypt their data against their own government; they are limiting their cooperation with NSA; and they are pushing for reform. Negative international reactions to media reports of certain kinds of intelligence collection abroad have resulted in a backlash against American technology companies, spurring data localization requirements, rejection or cancellation of American contracts, and raising the specter of major losses in the cloud computing industry. These allegations could dim one of the few bright spots in the American economic recovery: tech. Without commenting on the accuracy of these media reports, the perception is still a problem even if the media reports of these government collection programs are not true---or are only partly true. The tech industry believes them to be true, and more importantly, their customers at home and abroad believe them to be true, and that means they have huge impact on American business and huge impact as well on the relationship between these businesses and an intelligence community that depends on their cooperation. So, how should we think about reforms in response to this series of allegations the Executive Branch can’t, or won’t, address? How about making the FAA the exclusive means for conducting electronic surveillance when the information being collected is in the custody of an American company? This could clarify that the executive branch could not play authority shell-games and claim that Executive Order 12333 allows it to obtain information on overseas non-US person targets that is in the custody of American companies, unbeknownst to those companies. As a policy matter, it seems to me that if the information to be acquired is in the custody of an American company, the intelligence community should ask for it, rather than take it without asking. American companies should be entitled to a higher degree of forthrightness from their government than foreign companies, even when they are acting overseas. Under the FAA, we have a statutory regime that creates judicial oversight and accountability to conduct electronic surveillance outside the US for specific purposes: foreign intelligence (or traditional espionage), counter-terrorism, and prevention of WMD proliferation. It addresses protections for both non-US and US persons. It creates a front-door, though compelled, relationship under which the intelligence community can receive communications contents without individual warrants but with programmatic judicial oversight. FAA exclusivity would say to the rest of the world that when the US conducts bulk electronic surveillance overseas, we are doing so for a particular, national security purpose. The FAA structure with FISC review provides an independent check that the statutory purposes are met. Through transparency agreements with the government, the American companies are able to provide their customers with some sense of how many requests are made.

#### The US needs to draw a sharp distinction between domestic and national security surveillance to make the US Internet Freedom agenda credible – otherwise global internet fragmentation will result

**Fontaine, 14** – President of the Center for a New American Security; was foreign policy advisor to Senator John McCain for more than five years; Worked at the State Department, the National Security Council and the Senate Foreign Relations Committee; was associate director for near Eastern affairs at the National Security Council; B.A. in International Relations from Tulan University (Richard, “Bringing Liberty Online; Reenergizing the Internet Freedom Agenda in a Post-Snowden Era”, Center for a New American Security, September 18, 2014, [http://www.cnas.org/sites/default/files/publications-pdf/CNAS\_BringingLibertyOnline\_Fontaine.pdf)//TT](http://www.cnas.org/sites/default/files/publications-pdf/CNAS_BringingLibertyOnline_Fontaine.pdf%29//TT)

The 2013 revelations of mass surveillance by the U.S. government transformed the global debate about Internet freedom. Where once Washington routinely chided foreign governments and their corporate collaborators for engaging in online censorship, monitoring and other forms of Internet repression, the tables have turned. Edward Snowden, a former National Security Agency (NSA) contractor, leaked thousands of documents revealing America’s most secret electronic surveillance programs, unleashing a tidal wave of criticism and charges of hypocrisy, many directed at some of the very U.S. officials who have championed online freedom. America’s Internet freedom agenda – the effort to preserve and extend the free flow of information online – hangs in the balance.1 Already a contested space, the Internet after the Snowden revelations has become even more politically charged, with deep international divisions about its governance and heated battles over its use as a tool of political change. With 2.8 billion Internet users today, and several billion more expected over the next decade, the contest over online freedom grows more important by the day.2 As an ever-greater proportion of human activity is mediated through Internet-based technologies, the extent of online rights and restrictions takes on an increasingly vital role in political, economic and social life.3 Despite the many complications arising from the Snowden disclosures, America still needs a comprehensive Internet freedom strategy, one that tilts the balance in favor of those who would use the Internet to advance tolerance and free expression, and away from those who would employ it for repression or violence.4 It will need to pursue this strategy while drawing a sharp distinction between surveillance for national security purposes (in which all governments engage) and monitoring as a means of political repression (which democracies oppose). This is not an easy task, but it is an important one. More than a year after the first Snowden revelations emerged, now is the time to reenergize the Internet freedom agenda. Internet Freedom before Snowden The U.S. government’s explicit pursuit of Internet freedom began during the Bush administration’s second term. Among other steps, the establishment of the State Department’s Global Internet Freedom Task Force aimed to coordinate efforts to promote Internet freedom and to respond to online censorship.5 Building on this foundation, Secretary of State Hillary Rodham Clinton made the expansion of online rights a major focus of U.S. foreign policy in the first Obama term. Speaking in 2010, she cited Franklin Delano Roosevelt’s Four Freedoms and added a fifth, the “freedom to connect – the idea that governments should not prevent people from connecting to the Internet, to websites or to each other.”6 A year later, she pledged America’s “global commitment to Internet freedom, to protect human rights” – including the rights to expression, assembly and association – “online as we do offline.”7 And after the Arab Spring, the United States in 2011 established the Freedom Online Coalition, a collaboration of 23 countries to coordinate efforts to expand global Internet freedom.8 The U.S. government has backed up its words with resources. Since 2009, the State Department and other government agencies have spent more than $125 million on Internet freedom programming.9 In addition to the State Department’s efforts, other government agencies, including the Broadcasting Board of Governors, the U.S. Agency for International Development, the Defense Advanced Research Projects Agency and others, fund the development and deployment of tools aimed at expanding Internet freedom. These programs invest in technologies that allow users to circumvent firewalls so as to access censored material, communicate outside the watchful eye of autocratic regimes, secure their websites and data, link computers in decentralized mesh networks, and establish new Internet connections when existing ones have been cut.10 It supplements the provision of technology with training programs in dozens of countries. The Obama administration also took regulatory steps to promote Internet freedom, particularly after technology demonstrably facilitated the 2009 Green Revolution in Iran and the 2011 Arab Spring. The Treasury Department relaxed restrictions on the export of Internet-related software and services to Iran, explicitly to “foster and support the free flow of information to individual Iranian citizens.”11 Two years later, the White House issued an executive order that imposed sanctions on individuals who engaged in computer and network disruption, monitoring and tracking on behalf of the governments of Iran or Syria.12 The United States has aimed to promote the free flow of online information through diplomatic action as well. State Department diplomats pressure repressive regimes to loosen their Internet restrictions, free imprisoned bloggers and ensure that citizens can express themselves online without fear of punishment. U.S. government officials have engaged in significant dialogue with U.S. and multinational technology companies about their involvement in aiding Internet repression and in establishing transparency standards. American diplomats have also pressed for Internet freedom in the proliferating international fora that have taken up the issue. In 2012, for instance, the United States won approval of a U.N. Human Rights Council resolution affirming that freedom of expression and other rights that people have offline must also be protected online.13 Trade agreements have provided yet another vehicle for the U.S. Internet freedom agenda with, for example, hortatory language in the U.S.-Korea Free Trade Agreement calling for the free flow of online information.14 A key element of U.S. action has been aimed at preventing fundamental changes to the multistakeholder model of Internet governance, which brings together individuals, governments, civil society organizations, private firms and others for transparent and consensus-based decisionmaking.15 One such challenge arose at the December 2012 World Conference on International Telecommunications, when 89 countries – a majority of ITU members in attendance – supported an attempt by Russia, China, Iran and others to give governments greater control over the Internet.16 Despite opposition from the United States and others, the session ended with 89 countries signing the revised treaty; 55 other countries did not. As a sign of what may come in future international treaty negotiations, such numbers did not favor the multistakeholder model, and this was so even before the Snowden revelations emerged to complicate U.S. efforts. The Snowden Fallout and the Internet Freedom Agenda The dramatic revelations about NSA spying that began to emerge in June 2013 provoked a storm of international reaction.17 Political leaders expressed outrage at American surveillance practices and threatened a raft of retaliatory measures. President Dilma Rousseff of Brazil cancelled a planned state visit to the United States and the Brazilian government later organized an international meeting (NetMundial) to discuss the future of Internet governance.18 German Chancellor Angela Merkel was deeply affronted by the alleged monitoring of her personal cellphone. Chinese and other officials charged America with blatant hypocrisy. The fallout affected the private sector as well; where previously the focus of many observers had been on the aid given by U.S. companies to foreign governments engaged in Internet repression, the gaze shifted to the role American corporations play – wittingly or not – in enabling U.S. surveillance. Countries that had been the target of American reproaches rebuked the U.S. government for what they saw as hypocrisy. The United Nations and other international venues became platforms for international criticism of the United States. Germany and Brazil together sponsored a resolution adopted by the U.N. General Assembly in late 2013 backing a “right to privacy” in the digital age.19 In June 2014, the U.N. High Commissioner for Human Rights issued a report that endorsed digital privacy as a human right and criticized mass surveillance as “a dangerous habit rather than an exceptional measure.”20 Some European officials began to question the existing Internet governance model itself. In a statement, the European Commission said, “Recent revelations of large-scale surveillance have called into question the stewardship of the US when it comes to Internet Governance. So given the US-centric model of Internet Governance currently in place, it is necessary to broker a smooth transition to a more global model.”21 Nongovernmental groups that might otherwise be partners with the U.S. government in promoting Internet freedom reacted sharply as well. Reporters Without Borders, for instance, listed the NSA as an “Enemy of the Internet” in its 2014 report on entities engaged in online repression. Drawing no distinction between surveillance aimed at protecting national security and surveillance intended to suppress free expression and political dissent, the organization declared the NSA “no better than [its] Chinese, Russian, Iranian or Bahraini counterparts.”22 Mass surveillance methods used by democracies like the United States, it added, are “all the more intolerable” as they “are already being used by authoritarian countries such as Iran, China, Turkmenistan, Saudi Arabia and Bahrain to justify their own violations of freedom of information.”23 Tim Berners-Lee, the inventor of the World Wide Web, said, “Mass surveillance is the most immediate threat to the open Internet and the most insidious because we can’t see it.”24 The Electronic Frontier Foundation asserted that “mass surveillance is inherently a disproportionate measure that violates human rights,”25 and officials with Human Rights Watch observed that the surveillance scandal would render it more difficult for the U.S. government to press for better corporate practices and for companies to resist overly broad surveillance mandates. “Now,” its chief researcher said, “the vision and credibility of the U.S. and its allies on Internet freedom is in tatters.”26 The reactions to the Snowden disclosures threatened to go beyond verbal denunciations, diplomatic protests and critical press. The most serious commercial fallout came in the rising support for data localization requirements. Russia in July 2014 approved legislation that requires data operators to store the personal data of its citizens within the country’s borders.27 Indonesia, Brazil and Vietnam have also called for their citizens’ data held by companies such as Facebook to be stored domestically.28 Data localization has been debated in the European Parliament and elsewhere on the continent as well.29 Apart from the chilling effect on innovation and the loss of business to America companies, Internet freedom itself could become a casualty of such mandates. If a user’s data must be held within the borders of a repressive country, its government will have new opportunities to censor, monitor and disrupt online information flows. Such moves, combined with increasing questions about the multistakeholder approach to Internet governance (and possible support for a governmentdriven approach), together give rise to concerns about the potential “Balkanization” of the Internet, in which a constellation of national-level systems could take the place of the current global online infrastructure. As former NSA general counsel Stewart Baker warned, “The Snowden disclosures are being used to renationalize the Internet and roll back changes that have weakened government control of information.”30 This is evident in other proposed steps as well. Brazil and the European Union have announced plans for an undersea cable that would route data transmissions directly between Europe and Latin America and bypass the United States.31 The European Union threatened to suspend the Safe Harbor data-sharing agreement with the United States and promulgated new rules for it that EU officials said stemmed directly from worries after the Snowden disclosures.32

#### Data localization will end internet freedom and cause global democratic rollbacks

**Hill, 14** – Internet Policy at U.S. Department of Commerce (Jonah, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders”, The Hague Institute for Global Justice, Conference on the Future of Cyber Governance, 2014 , May 1, 2014, SSRN)//TT

Free Expression and Internet Freedoms Are Not Well Served Most troubling of all the potential harms of data localization is its effect on free expression and Internet freedom. This is ironic, in that to many of its advocates, data localization is a remedy to the threat posed by the NSA to free expression and Internet freedom. I suggest that the opposite is actually true, that the “remedy” only serves to make the danger greater. The Internet and other online media have become indispensable tools for individuals to communicate globally, and have furthered individual participation in the political process, increased transparency of governmental activities, and promoted fundamental rights. Data localization, by centralizing control over digital infrastructure, can diminish this capacity in a number of ways. As was discussed above, data localization as a local server or local data storage requirement can limit freedom by permitting countries more easily to collect information on their citizens (through domestic surveillance). It allows a government more quickly and effectively to shut down Internet services (usually via legal threats to local Internet service providers) that the government believes is abetting unwanted political opposition. 115 Data localization mandates also can obstruct Internet freedom in other, indirect ways. Restricted routing, in particular, is problematic, because it is not technically possible as the existing Internet is designed or organized. Unlike the telephone network, the Internet operates under a model known as “best effort delivery,” where data is delivered to its destination in the most efficient manner possible, without predetermined routes. For instance, data sent from the United States to Botswana will attempt to travel along the shortest and most direct route possible. However, if there is a bottleneck along the shortest route, a packet may find a longer but more expeditious route. This is a core feature of the Internet that makes network congestion easy to navigate around. In order to restrict data routing to specific geographies as governments are advocating, all Internet routers that are currently programmed to follow this “best effort” routing model would have to be reconfigured to prohibit data from one country from moving through the territory of “prohibited” countries. Moreover, since Internet addresses are not always assigned according to a specific geography, the Internet’s addressing system currently would have to be dramatically altered as well. Thus, the Border Gateway Protocol (one of the core Internet networking protocols), the Internet’s routing tables (the address books by which routers send data), and the process by which IP addresses are allocated, would all have to be modified. Such an undertaking would require a fundamental overhaul not only of the Internet’s operating structures, but also of the governance structures by which those structures are implemented and standardized. These are not just arcane concerns of those involved in Internet governance, although they surely are matters that greatly trouble those who favor an efficient and interoperable Internet. These alterations in the way the Internet works will, I believe, materially restrict the power of the Internet to support free expression. These modifications to these core characteristic of the current Internet – modifications that localization would require – may result in intelligence agencies acquiring a previously unavailable capacity to assess where data had originated and where it was heading, because the origin and destination information would be included in the data packet.116 A centralized governance process, further, which would be required to change the routing protocols and IP allocation system, would give authoritarian countries significantly more influence over how information on the Internet is regulated. In fact, this is one of the main reasons why China, Russia, many Arab states (among others) have pushed for tracked routing protocols in the past, 117 just as they have lobbied for a handover of the global Internet governance system to the U.N.’s International Telecommunications Union. 118 In short, localization would require dramatic changes to the current structure of the Internet, changes that would have adverse consequences for those who see it as a principal – if not the principal – means of global democratization. For some, those adverse consequences would be unintended; more chillingly, there are those who intend precisely those consequences. This would be an enormous price to pay, particularly since the other objectives that are promoted as justifications for localization – namely, security for communications and economic development – are illusory.

#### Democracy as spread by the global internet is vital to the emergence of global publics – that’s the key to solving all existential impacts

**Keane, 11** – Professor of Politics at the University of Sydney (John, “Democracy in the Age of Google, Facebook and WikiLeaks” <http://sydney.edu.au/arts/downloads/news/ALR.pdf>)

Communicative abundance enables one other trend that is of life-and-death importance to the future of democracy: the growth of cross-border publics whose footprint is potentially or actually global in scope. The Canadian Scholar Harold Innis famously showed that communications media like the wheel and the printing press and the telegraph had distance-shrinking effects, but genuinely globalised communication only began (during the nineteenth century) with overland and underwater telegraphy and the early development of international news agencies like Reuters. The process is currently undergoing an evolutionary jump, thanks to the development of a combination of forces: wide-footprint geo-stationary satellites, weblogs and other specialist computer-networked media, the growth of global journalism and the expanding and merging flows of international news, electronic data exchange, entertainment and education materials controlled by giant firms like Thorn-EMI, AOL/Time-Warner, News Corporation International, the BBC, Al Jazeera, Disney, Bertelsmann, Microsoft, Sony and CNN. Global media linkages certainly have downsides for democracy. Global media integration has encouraged loose talk of the abolition of barriers to communication (John Perry Barlow). It is said to be synonymous with the rise of a ‘McWorld’ (Benjamin Barber) dominated by consumers who dance to the music of logos, advertising slogans, sponsorship, trademarks and jingles. In the most media-saturated societies, such as the United States, global media integration nurtures pockets of parochialism; citizens who read local ‘content engine’ newspapers like The Desert Sun in Palm Springs or Cheyenne's Wyoming Tribune-Eagle are fed a starvation diet of global stories, which typically occupy no more than about 2% of column space. And not to be overlooked is the way governments distort global information flows. Protected by what in Washington are called ‘flack packs’ and dissimulation experts, governments cultivate links with trusted or ‘embedded’ journalists, organise press briefings and advertising campaigns, so framing - and wilfully distorting and censoring - global events to suit current government policies. All these fickle counter-trends are sobering, but they are not the whole story. For in the age of communicative abundance there are signs that the spell of parochialism upon citizens is not absolute because global media integration is having an unanticipated political effect: by nurturing a world stage or theatrum mundi, global journalism and other acts of communication are slowly but surely cultivating public spheres in which many millions of people scattered across the earth witness mediated controversies about who gets what, when, and how, on a world scale. Not all global media events - sporting fixtures, blockbuster movies, media awards, for instance - sustain global publics, which is to say that audiences are not publics and public spheres are not simply domains of entertainment or play. Strictly speaking, global publics are scenes of the political. Within global publics, people at various points on the earth witness the powers of governmental and non-governmental organisations being publicly named, monitored, praised, challenged, and condemned, in defiance of the old tyrannies of time and space and publicly unaccountable power. It is true that global publics are neither strongly institutionalised nor effectively linked to mechanisms of representative government. This lack is a great challenge for democratic thinking and democratic politics. Global publics are voices without a coherent body politic; it is as if they try to show the world that it resembles a chrysalis capable of hatching the butterfly of cross-border democracy - despite the fact that we currently have no good account of what ‘regional’ or ‘global’ or ‘cross border’ democratic representation might mean in practice. Still, in spite of everything, global publics have marked political effects, for instance on the suit-and-tie worlds of diplomacy, global business, inter-governmental meetings and independent non-governmental organizations. Every great global issue since 1945 - human rights, the dangers of nuclear war, continuing discrimination against women, the greening of politics - every one of these issues first crystallised within these publics. Global publics sometimes have ‘meta-political’ effects, in the sense that they help create citizens of a new global order. The speech addressed to ‘global citizens’ by Barack Obama at the Siegessaule in the Tiergarten in July 2008 is a powerful case in point, a harbinger of a remarkable trend in which those who are caught up within global publics learn that the boundaries between native and foreigner are blurred. They consequently become footloose. They live here and there; they discover the ‘foreigner’ within themselves. Global publics centred on ground-breaking media events like Live-Aid (in 1985 it attracted an estimated one billion viewers) can be spaces of fun, in which millions taste something of the joy of acting publicly with and against others for some defined common purpose. When by contrast they come in the form of televised world news of the suffering of distant strangers, global publics highlight cruelty; they make possible what Hannah Arendt once called the ‘politics of pity’. And especially during dramatic media events - like the nuclear meltdown at Chernobyl, the Tiananmen massacre, the 1989 revolutions in central-eastern Europe, the overthrow and arrest of Slobodan Milosevic, the 9/11 terrorist attacks and the recent struggles for dignity in Tunisia and Egypt - public spheres intensify audiences’ shared sense of living their lives contingently, on a knife edge, in the subjunctive tense. The witnesses of such events (contrary to McLuhan) do not experience uninterrupted togetherness. They do not enter a ‘global village’ dressed in the skins of humankind and thinking in the terms of a primordial ‘village or tribal outlook’. They instead come to feel the pinch of the world’s power relations; in consequence, they put matters like representation, accountability and legitimacy on the global political agenda, in effect by asking whether new democratic measures could inch our little blue and white planet towards greater openness and humility, potentially to the point where power, wherever it is exercised within and across borders, would come to feel more ‘biodegradable’, a bit more responsive to those whose lives it currently shapes and reshapes, secures or wrecks.

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

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

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

#### Data localization will destroy global economic growth

**Chandler and Le, 15** - \* Director, California International Law Center, Professor of Law and Martin Luther King, Jr. Hall Research Scholar, University of California, Davis; A.B., Harvard College; J.D., Yale Law School AND \*\*Free Speech and Technology Fellow, California International Law Center; A.B., Yale College; J.D., University of California, Davis School of Law (Anupam and Uyen, “DATA NATIONALISM” 64 Emory L.J. 677, lexis)

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

#### That causes World War 3

**James, 14 -** Professor of history at Princeton University’s Woodrow Wilson School who specializes in European economic history (Harold, “Debate: Is 2014, like 1914, a prelude to world war?” 7/3, http://www.theglobeandmail.com/globe-debate/read-and-vote-is-2014-like-1914-a-prelude-to-world-war/article19325504/)

Some of the dynamics of the pre-1914 financial world are now re-emerging. Then an economically declining power, Britain, wanted to use finance as a weapon against its larger and faster growing competitors, Germany and the United States. Now America is in turn obsessed by being overtaken by China – according to some calculations, set to become the world’s largest economy in 2014. In the aftermath of the 2008 financial crisis, financial institutions appear both as dangerous weapons of mass destruction, but also as potential instruments for the application of national power. In managing the 2008 crisis, the dependence of foreign banks on U.S. dollar funding constituted a major weakness, and required the provision of large swap lines by the Federal Reserve. The United States provided that support to some countries, but not others, on the basis of an explicitly political logic, as Eswar Prasad demonstrates in his new book on the “Dollar Trap.” Geo-politics is intruding into banking practice elsewhere. Before the Ukraine crisis, Russian banks were trying to acquire assets in Central and Eastern Europe. European and U.S. banks are playing a much reduced role in Asian trade finance. Chinese banks are being pushed to expand their role in global commerce. After the financial crisis, China started to build up the renminbi as a major international currency. Russia and China have just proposed to create a new credit rating agency to avoid what they regard as the political bias of the existing (American-based) agencies. The next stage in this logic is to think about how financial power can be directed to national advantage in the case of a diplomatic tussle. Sanctions are a routine (and not terribly successful) part of the pressure applied to rogue states such as Iran and North Korea. But financial pressure can be much more powerfully applied to countries that are deeply embedded in the world economy. The test is in the Western imposition of sanctions after the Russian annexation of Crimea. President Vladimir Putin’s calculation in response is that the European Union and the United States cannot possibly be serious about the financial war. It would turn into a boomerang: Russia would be less affected than the more developed and complex financial markets of Europe and America. The threat of systemic disruption generates a new sort of uncertainty, one that mirrors the decisive feature of the crisis of the summer of 1914. At that time, no one could really know whether clashes would escalate or not. That feature contrasts remarkably with almost the entirety of the Cold War, especially since the 1960s, when the strategic doctrine of Mutually Assured Destruction left no doubt that any superpower conflict would inevitably escalate. The idea of network disruption relies on the ability to achieve advantage by surprise, and to win at no or low cost. But it is inevitably a gamble, and raises prospect that others might, but also might not be able to, mount the same sort of operation. Just as in 1914, there is an enhanced temptation to roll the dice, even though the game may be fatal.

### 1ac – Tech leadership Advantage

#### Contention 2 – technological leadership

#### NSA surveillance is crushing U.S. cloud-computing – decks competitiveness and spills over to the entire tech sector

Donohue 15 – Professor of Law, Georgetown Law and Director, Center on National Security and the Law, Georgetown Law (Lauren, HIGH TECHNOLOGY, CONSUMER PRIVACY, AND U.S. NATIONAL SECURITY, Symposium Articles, 4 Am. U. Bus. L. Rev. 11 p.15-18, 2015, Hein Online)//JJ

I. ECONOMIC IMPACT OF NSA PROGRAMS

The NSA programs, and public awareness of them, have had an immediate and detrimental impact on the U.S. economy. They have cost U.S. companies billions of dollars in lost sales, even as companies have seen their market shares decline. American multinational corporations have had to develop new products and programs to offset the revelations and to build consumer confidence. At the same time, foreign entities have seen revenues increase. Beyond the immediate impact, the revelation of the programs, and the extent to which the NSA has penetrated foreign data flows, has undermined U.S. trade agreement negotiations. It has spurred data localization efforts around the world, and it has raised the spectre of the future role of the United States in Internet governance. Even if opportunistic, these shifts signal an immediate and long-term impact of the NSA programs, and public knowledge about them, on the U.S. economy. A. Lost Revenues and Declining Market Share Billions of dollars are on the line because of worldwide concern that the services provided by U.S. information technology companies are neither secure nor private. Perhaps nowhere is this more apparent than in cloud computing. Previously, approximately 50% of the worldwide cloud computing revenues derived from the United States. The domestic market thrived: between 2008 and 2014, it more than tripled in value. But within weeks of the Snowden leaks, reports had emerged that U.S. companies such as Dropbox, Amazon Web Services, and Microsoft's Azure were losing business. By December 2013, ten percent of the Cloud Security Alliance had cancelled U.S. cloud services projects as a result of the Snowden information. In January 2014 a survey of Canadian and British businesses found that one quarter of the respondents were moving their data outside the United States. The Information Technology and Innovation Foundation estimates that declining revenues of corporations that focus on cloud computing and data storage alone could reach $35 billion over the next three years. Other commentators, such as Forrester Research analyst James Staten, have put actual losses as high as $180 billion by 2016, unless something is done to restore confidence in data held by U.S. companies. The monetary impact of the NSA programs extends beyond cloud computing to the high technology industry. Cisco, Qualcomm, IBM, Microsoft, and Hewlett-Packard have all reported declining sales as a direct result of the NSA programs. Servint, a webhosting company based in Virginia, reported in June 2014 that its international clients had dropped by 50% since the leaks began. Also in June, the German government announced that because of Verizon's complicity in the NSA program, it would end its contract with the company, which had previously provided services to a number of government departments. As a senior analyst at the Information Technology and Innovation Foundation explained, "It's clear to every single tech company that this is affecting their bottom line. The European commissioner for digital affairs, Neelie Kroes, predicts that the fallout for U.S. businesses in the EU alone will amount to billions of Euros. Not only are U.S. companies losing customers, but they have been forced to spend billions to add encryption features to their services. IBM has invested more than a billion dollars to build data centers in London, Hong Kong, Sydney, and elsewhere, in an effort to reassure consumers outside the United States that their information is protected from U.S. government surveillance.26 Salesforce.com made a similar announcement in March 2014.27 Google moved to encrypt terms entered into its browser.28 In June 2014 it took the additional step of releasing the source code for End-to-End, its newly-developed browser plugin that allows users to encrypt email prior to it being sent across the Internet.29 The following month Microsoft announced Transport Layer Security for inbound and outbound email, and Perfect Forward Secrecy encryption for access to OneDrive.30 Together with the establishment of a Transparency Center, where foreign governments could review source code to assure themselves of the integrity of Microsoft software, the company sought to put an end to both NSA back door surveillance and doubt about the integrity of Microsoft products.3' Foreign technology companies, in turn, are seeing revenues increase. Runbox, for instance, an email service based in Norway and a direct competitor to Gmail and Yahoo, almost immediately made it publicly clear that it does not comply with foreign court requests for its customers' personal information. Its customer base increased 34% in the aftermath of the Snowden leaks. Mateo Meier, CEO of Artmotion, Switzerland's biggest offshore data hosting company, reported that within the first month of the leaks, the company saw a 45% rise in revenue. Because Switzerland is not a member of the EU, the only way to access data in a Swiss data center is through an official court order demonstrating guilt or liability; there are no exceptions for the United States. In April 2014, Brazil and the EU, which previously used U.S. firms to supply undersea cables for transoceanic communications, decided to build their own cables between Brazil and Portugal, using Spanish and Brazilian companies in the process.36 OpenText, Canada's largest software company, now guarantees customers that their data remains outside the United States. Deutsche Telekom, a cloud computing provider, is similarly gaining more customers. Numerous foreign companies are marketing their products as "NSA proof' or "safer alternatives" to those offered by U.S. firms, gaining market share in the process.

#### The best and newest research confirms the link

**Marthews and Tucker, 15** – \* National Chair at Restore the Fourth AND \*\*PhD in economics and professor of Marketing at MIT (Alex and Catherine, “Government Surveillance and Internet Search Behavior”, 29 April 2015, [file:///C:/Users/17GGonzalez/Downloads/SSRN-id2412564%20(2).pdf)//](file:///C%3A/Users/17GGonzalez/Downloads/SSRN-id2412564%20%282%29.pdf%29//gg)gg

This study is the first to provide substantial empirical documentation of a chilling effect, both domestically in the shorter term and internationally in the longer term, that appears to be related to increased awareness of government surveillance online. Furthermore, this chilling effect appears in countries other than the US to apply to search behavior that is not strictly related to the government but instead forms part of the private domain. Our findings have the following policy implications. From an economic perspective, our finding that there was an effect on international Google users’ browsing behavior has potential policy implications for the effects of government surveillance on international commerce. From a US competitive standpoint, the longer-run effect observed on international Google users’ search behavior indicates that knowledge of US government surveillance of Google could indeed affect their behavior. At the most limited end of the spectrum, it could steer them away from conducting certain searches on US search engines; at the most severe end of the spectrum, they might choose to use non-US search engines. Such effects may not be limited simply to search engines. For example, as Google’s services are embedded in a large array of products, it could potentially hinder sales of Android-enabled mobile phones. Though preliminary attempts are being made to work towards initial measures of the economic impact of surveillance revelations (Dinev et al., 2008), no systematic study yet exists. All we can do, within the context of our data, is to indicate that on the basis of the effects we find, the strong possibility of substantial economic effects exists, and to suggest that such potential adverse economic impacts should be incorporated into the thinking of policy makers regarding the appropriateness of mass surveillance programs. There are limitations to the generalizability of our findings. First, we are not sure how the results generalize outside of the search domain towards important tech industries such as the rapidly growing US cloud computing industry. Second, we are not sure how the revelations affected search on Google’s major competitors, such as Bing and Yahoo! Search. It may be that the effect on their services was lessened by reduced media focus on them relative to Google in the light of the PRISM revelations and potentially the extent to which users anticipated that their servers may be located outside of the US. Third, our results are focused on the effects of revelations about government surveillance as opposed to the direct effects of government surveillance per se. Notwithstanding these limitations, we believe that our study provides an important first step in understanding the potential for effects of government surveillance practices on commercial outcomes and international competitiveness.

#### That undermines US global technological leadership

**Castro and McQuinn 15**, Daniel Castro works at the Center for Data Innovation, Government Technology, The Information Technology & Innovation Foundation, worked at the U.S. Government Accountability Office, went to Carnegie Mellon. Alan McQuinn works at the Federal Communications Commission, previously had the Bill Archer Fellowship at the University of Texas, (June 2015, “Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness”, [file:///C:/Users/Mark/Downloads/2015-beyond-usa-freedom-act.pdf)//AK](file:///C%3A/Users/Mark/Downloads/2015-beyond-usa-freedom-act.pdf%29//AK)

CONCLUSION When historians write about this period in U.S. history it could very well be that one of the themes will be how the United States lost its global technology leadership to other nations. And clearly one of the factors they would point to is the long-standing privileging of U.S. national security interests over U.S. industrial and commercial interests when it comes to U.S. foreign policy. This has occurred over the last few years as the U.S. government has done relatively little to address the rising commercial challenge to U.S. technology companies, all the while putting intelligence gathering first and foremost. Indeed, policy decisions by the U.S. intelligence community have reverberated throughout the global economy. If the U.S. tech industry is to remain the leader in the global marketplace, then the U.S. government will need to set a new course that balances economic interests with national security interests. The cost of inaction is not only short-term economic losses for U.S. companies, but a wave of protectionist policies that will systematically weaken U.S. technology competiveness in years to come, with impacts on economic growth, jobs, trade balance, and national security through a weakened industrial base. Only by taking decisive steps to reform its digital surveillance activities will the U.S. government enable its tech industry to effectively compete in the global market.

#### Tech leadership is the primary driver of hegemony –

Weiss 14 – Fellow of the Academy of the Social Sciences in Australia, Professor Emeritus in Government and International Relations at the University of Sydney, Honorary Professor of Political Science at Aarhus University. (Linda, America Inc.?: Innovation and Enterprise in the National Security State, Cornell University Press, 4/1/14, p. 1-3)//JJ

\*NSS=National Security State

So what accounts for America’s transformative capacity? Where do its breakthrough innovations come from? My answer traces the relationship between high technology, national security, and political culture. It advances three interlinked propositions regarding the role of the NSS as technology enterprise and commercialization engine; its geopolitical drivers; and the institutional consequences of an antistatist constraint. The national security state as technology enterprise. First, America's capacity for transformative innovation derives not merely from the entrepreneurship of its private sector, or simply from the state as such, but from the national security state—a particular cluster of federal agencies that collaborate closely with private actors in pursuit of security-related objectives. The NSS is a wholly new postwar creation that is geared to the permanent mobilization of the nation's science and technology resources for military primacy, and here I document and explain why it has had to become increasingly involved in commercial undertakings. Although centered on defense preparedness, the NSS is a good deal broader than the military, yet narrower than the state as a whole. In addition to its defense core in the Department of Defense, the NSS comprises several other components created at the height of the Cold War to pursue, deliver, or underwrite innovation in the service of securing technological supremacy. Although some are designated as "civilian" in their ori- gins, evolution, and current mix of activities, these NSS components remain deeply enmeshed in national security or dual-use functions (as we shall see in chapter 2).4 Acting as commander in chief, the president sits at the peak of this complex, supported by the Oval Office and, in particular, the Office of Science and Technology Policy. In sum, I discuss NSS activities not in the more popular sense of a surveillance state, but as a national "technology enterprise" in which the military is the central, but far from exclusive, actor. In telling this Story, I demonstrate and account for a major shift in NS.S innovation programs and policies that involved the national security agencies cultivating and undertaking commercialization ventures. (c. 1945 up to the 1970s), this process of fostering commercially relevant (general-purpose or dual-use) technologies took both direct and indirect forms. Then (especially from the 1980s onward) it also took a more proactive form, via patenting and licensing reforms and cooperative agreements to transfer technology from the federal labs to the private sector, via the launching of new procurement and joint innovation initiatives, and via the creation of new venture capital (VC) schemes. By placing greater emphasis on commercialization opportunities, some of these incentives sought to sweeten collaboration with the DOD and other security-related agencies, and thus to increase NISS influence over the direction of technology. A significant problem for the NSS has been that since the late 1970s, it has become progressively more challenging to enlist innovative companies in the private sector to work on security-related projects. While traditional defense suppliers grew increasingly large and specialized in systems integration, by the 1970s the more innovative producer companies—above all, critical suppliers Of integrated circuits—had begun to pull away from the federal market. Attracting nondefense firms to do defense work was at one time easy because the government market (in semiconductors and computers, for instance) was so much larger than the private market, and healthy profits could be made. But by the mid- 1970s commercial markets had come into their own, leading firms to reorient production to suit the more standardized demand. One consequence of lacking the earlier pull power Of massive demand is that NISS agencies have had to create new incentives to foster private-sector collaboration. One of the major incentives intended to reattract the private sector is the inclusion of commercial goals in NSS technology policies. Commercial viability therefore has to stand alongside security and technological supremacy in NSS policy. For instance, if a firm works with an agency to create a technology, service, or prototype for use by the U.S. Army, it will also be encouraged from the outset of the project to create a similar product for the commercial market. In this way, and many more, the NSS has progressively been drawn into promoting commercial innovation for security reasons. One implication, demonstrated in some detail, is that the NISS has achieved a much broader reach than commonly implied by the notion Of a military-industrial complex. Geopolitical drivers. What are the drivers of the NSS technology enterprise? Geopolitics and related threat perceptions have been the original catalyst for NSS formation and its evolution as an innovation engine. This state- (and technology-) building dynamic has occurred in three broad phases: the Cold War, the rise of Japan as techno-security challenge, and the post-9/11 era of asymmetric threats. The NSS emerged and expanded in fits and starts after World War II in response to a perceived international threat, emanating from the Soviet Union, that proved both enduring and persistent. It is instructive to note that in this phase the NSS bears at least some comparison with the erstwhile "developmental states" of Northeast Asia. They too emerged in response to an intensely perceived security threat, from neighboring China and North Korea, but instead sought national security more broadly via economic improvement, or industrial catch-up. Living on the fault lines of the Cold War in the presence of a credible and unyielding security threat exerted an unusual pressure on the East Asian states to pursue security by building economic strength. More distinctively in the case of Japan, Peter Katzenstein has developed the argument that, against the backdrop of terrible defeat, domestic power struggles succeeded in reorienting Japan's conception of security in favor Of economic rather than military strength. Thus the Japanese state practices a form of "technological national security" in order to ensure against its resource dependence and reduce its exposure to international supply disruptions (Katzenstein 1996, 2005; also Samuels 1994). Fundamental motivations drawn from different historical experiences thus serve to underline a unique feature of the NSS. In contrast to Japan (and the East Asian developmental states more generally), America's national security State has been geared to the pursuit of technological superior, not for reasons of national independence, economic competitiveness, or resource dependency, but in order to maintain American primacy. For the United States, the experience of World War Il drove home the point that science and technology (S&T) was a game changer—the key to winning the war—and that future preparedness would depend on achieving and sustaining technological superiority. Geopolitics is thus the driver, not economics. I emphasize this point because many analysts have viewed the Pentagon as the source of an industrial policy that is pursued beneath the radar6—a claim that this book disputes since it mistakes the nature of the primary driver. From its inception, the NSS was tasked with ensuring the technology leadership of the United States for the purpose of national defense. Even as the Soviet menace retreated, security proved paramount as the U.S. confronted a newly resurgent Japan that threatened to dethrone it as the regnant technology power. Appreciating the strength and intensity of the U.S. security focus means never underestimating the significance of this point: as long as U.S. military strategy continues to rely on a significant technology lead over its adversaries (real or potential), threats to that lead can never be simply (or even primarily) a commercial matter—even when the NSS "goes commercial.

#### Hegemonic decline causes great power wars

**Zhang et al., Carnegie Endowment researcher, 2011**

(Yuhan, “America’s decline: A harbinger of conflict and rivalry”, 1-22, <http://www.eastasiaforum.org/2011/01/22/americas-decline-a-harbinger-of-conflict-and-rivalry/>, ldg)

This does not necessarily mean that the US is in systemic decline, but it encompasses a trend that appears to be negative and perhaps alarming. Although the US still possesses incomparable military prowess and its economy remains the world’s largest, the once seemingly indomitable chasm that separated America from anyone else is narrowing. Thus, the global distribution of power is shifting, and the inevitable result will be a world that is less peaceful, liberal and prosperous, burdened by a dearth of effective conflict regulation. Over the past two decades, no other state has had the ability to seriously challenge the US military. Under these circumstances, motivated by both opportunity and fear, many actors have bandwagoned with US hegemony and accepted a subordinate role. Canada, most of Western Europe, India, Japan, South Korea, Australia, Singapore and the Philippines have all joined the US, creating a status quo that has tended to mute great power conflicts. However, as the hegemony that drew these powers together withers, so will the pulling power behind the US alliance. The result will be an international order where power is more diffuse, American interests and influence can be more readily challenged, and conflicts or wars may be harder to avoid. As history attests, power decline and redistribution result in military confrontation. For example, in the late 19th century America’s emergence as a regional power saw it launch its first overseas war of conquest towards Spain. By the turn of the 20th century, accompanying the increase in US power and waning of British power, the American Navy had begun to challenge the notion that Britain ‘rules the waves.’ Such a notion would eventually see the US attain the status of sole guardians of the Western Hemisphere’s security to become the order-creating Leviathan shaping the international system with democracy and rule of law. Defining this US-centred system are three key characteristics: enforcement of property rights, constraints on the actions of powerful individuals and groups and some degree of equal opportunities for broad segments of society. As a result of such political stability, free markets, liberal trade and flexible financial mechanisms have appeared. And, with this, many countries have sought opportunities to enter this system, proliferating stable and cooperative relations. However, what will happen to these advances as America’s influence declines? Given that America’s authority, although sullied at times, has benefited people across much of Latin America, Central and Eastern Europe, the Balkans, as well as parts of Africa and, quite extensively, Asia, the answer to this question could affect global society in a profoundly detrimental way. Public imagination and academia have anticipated that a post-hegemonic world would return to the problems of the 1930s: regional blocs, trade conflicts and strategic rivalry. Furthermore, multilateral institutions such as the IMF, the World Bank or the WTO might give way to regional organisations. For example, Europe and East Asia would each step forward to fill the vacuum left by Washington’s withering leadership to pursue their own visions of regional political and economic orders. Free markets would become more politicised — and, well, less free — and major powers would compete for supremacy. Additionally, such power plays have historically possessed a zero-sum element. In the late 1960s and 1970s, US economic power declined relative to the rise of the Japanese and Western European economies, with the US dollar also becoming less attractive. And, as American power eroded, so did international regimes (such as the Bretton Woods System in 1973). A world without American hegemony is one where great power wars re-emerge, the liberal international system is supplanted by an authoritarian one, and trade protectionism devolves into restrictive, anti-globalisation barriers. This, at least, is one possibility we can forecast in a future that will inevitably be devoid of unrivalled US primacy.

### 1ac – plan

#### The United States federal government should substantially curtail its surveillance of information in the custody of American corporations by exclusively limiting surveillance to investigations carried out under section 702 of the FISA Amendments Act.

### 1ac – Solvency

#### Contention 3 – Solvency

#### The plan’s curtailment of surveillance of U.S. companies to exclusive section 702 authority is vital to restoring domestic and international trust in surveillance

**Eoyang and Bishai, 15** - \*Mieke Eoyang is the Director of the National Security Program at Third Way, a center-left think tank. She previously served as Defense Policy Advisor to Senator Edward M. Kennedy, and a subcommittee staff director on the House Permanent Select Committee on Intelligence, as well as as Chief of Staff to Rep. Anna Eshoo (D-Palo Alto); \*\*Chrissy Bishai is a Fellow at Third Way (“Restoring Trust between U.S. Companies and Their Government on Surveillance Issues” 3/19, <http://www.thirdway.org/report/restoring-trust-between-us-companies-and-their-government-on-surveillance-issues>

Fixing the Problem Means Changing the Existing Legal Framework Currently, the U.S. collects electronic communications under four main authorities. For collection occurring under both 215 and 702, the companies would have been served with an order compelling production of their data. But outside the U.S., Executive Order 12333,15 the long-standing guidance for foreign intelligence activities, would govern the kind of collection that has caused international outrage. E.O. 12333, signed by President Reagan, set the ground rules and authorization for foreign intelligence collection when the nation’s primary security threat was the Soviet Union. At that time, traditional intelligence activities would have been focused on other nation-states—identifying their spies, trying to recruit spies for the U.S., and trying to steal other countries’ secrets while protecting our own. But the growth of terrorist groups’ capabilities, and particularly the 9/11 attacks, helped dissolve the separation between traditional overseas espionage and counter-terrorism. As the nation was grappling with new threats posed by terrorism, people around the world were sharing more and more of their information online and using mostly American companies to do so. Yet the legal framework that had once recognized privacy rights was ill-suited to the Internet Age. The Intelligence Community’s traditional position that constitutional rights like the Fourth Amendment’s privacy protections didn’t apply to non-Americans outside the U.S. might have been clear when travelling and communicating internationally were more difficult. But today’s free-flowing movement of people and data means that the “nationality” of an individual’s communications is far less obvious.16 While extending constitutional or privacy protections to foreigners abroad is a tricky legal proposition, for many their data is being held by entities that are entitled to the due process and privacy protections of the U.S. Constitution: American companies. Our tech firms often act as custodians of other people’s data, and as such don’t have the same heightened privacy interests as the targets of that data. But accessing the companies’ data without even giving notice to the owner of the servers raises serious constitutional questions. As a politician once famously noted, “corporations are people too.”17 As a legal (if not political) matter, he was right—these American tech companies are “U.S. Persons,” and they therefore should know when the government seeks to access the data they possess. The companies should be entitled to notice, especially since they can be compelled to cooperate with law enforcement requests to hand over user data. Those protections should hold true regardless of whether the user data sought by the U.S. government is that of Americans or non-Americans. In addition to those privacy protections that all U.S. persons enjoy under the Constitution, both at home and abroad, surveillance reform should meet the following principles when dealing with information about or from Americans: The U.S. government should have a process, consistent with the Constitution, to acquire from companies the information that it needs to secure the country. The U.S. government should have a national security reason to collect the information that it requests. U.S. companies should not have to fear unauthorized access to their data or products from their own government. Any process to acquire information from U.S. companies should have safeguards to prevent misuse or intentional over-collection. The Solution Include Overseas Collection from American Companies in Existing Statutory Frameworks In order to meet the principles above, we propose that FAA’s 702 framework be the exclusive means for conducting electronic surveillance when the information is in the custody of an American company (“FAA Exclusivity”). Section 702 of FAA provides procedures to authorize data collection of foreign targets reasonably believed to be outside the U.S. It empowers the Attorney General (AG) and Director of National Intelligence (DNI) to jointly certify a high volume of targeting and does not require the requesters to identify specific non-U.S. persons who will be targeted. Under this 702 framework, information on foreigners that’s in the custody of a U.S. company should be subject to the following rules: 1. The data must relate to targets “reasonably believed” to be outside the U.S. (can include foreign persons, governments or their factions and similar entities). 2. The AG and DNI must jointly submit annual “certifications” to the Foreign Intelligence Surveillance Court (FISC). 3. Certifications must identify categories of foreign intelligence targets that the Government wants to surveil electronically; they do not need to identify specific persons to be targeted. 4. Certifications may include information or representations from other federal agencies authorized to cooperate with the AG, DNI, or Director of the NSA. 5. Certifications must be reviewed by the FISC, which can authorize the targeting if they deem that the statutory requirements have been met. 6. After the certifications are approved, the AG and DNI issue (written) “directives” to the providers, ordering them to assist the government. 7. Collection should be executed with the appropriate “minimization procedures” in place to limit the acquisition, retention, and dissemination of any non–publicly available U.S. person information acquired through the Section 702 program. 8. The AG, in consultation with the DNI, must adopt FISC-approved targeting and minimization procedures that are “reasonably designed” to ensure that the Government does not collect wholly domestic communications, and that only persons outside the U.S. are surveilled. 9. The AG and DNI must also create acquisition guidelines (which are not subject to FISC approval). Advantages of an FAA Framework Shifting the legal authority for collection of data in the custody of an American company from E.O. 12333 to an FAA framework would have a number of advantages. Most importantly, it would create a way for the government to get the data it needs from American companies while giving those firms assurances that their data would not be accessed in other unauthorized ways. In particular, the FAA framework would create specific purposes for which the information could be sought, rather than allow the indiscriminate scooping up of every aspect of a person’s communications. FAA’s stated purpose is to acquire foreign intelligence information, which it defines as "information that relates to the ability of the U.S. to protect against an actual or potential attack by a foreign power; sabotage, international terrorism, or the proliferation of weapons of mass destruction by a foreign power; or clandestine intelligence activities by a foreign power." The FAA framework would also create a requirement that the Executive Branch explain how the information sought meets the statutory purposes. And there would be the additional check of an independent judge who would review the certifications and issue directives. Though this process is ex parte, and therefore a potential rubber stamp for the government, there have been no documented instances of intentional abuses of the system in seeking information beyond the statutory purposes. Finally, the FAA framework would subject information sought from U.S. companies to the statutory oversight requirements of the law. These are extensive and explicit.18 In addition to FAA’s inherent protections, FAA Exclusivity would send a powerful message to the rest of the world: when the U.S. conducts electronic surveillance overseas from American companies, it is doing so for a particular national security purpose. The FAA structure with FISC review provides an independent check that the statutory purposes are met. Through transparency agreements with the government, the American companies would be able to provide their customers with some sense of how many requests are made. FAA Exclusivity would not change the E.O. 12333 authorities with respect to non-U.S. companies. It would not change E.O. 12333 authorities when the Executive Branch seeks to obtain the information in some way other than through a U.S. company that holds the data (i.e. traditional espionage, like breaking into a target’s laptop, parking a surveillance van outside their house, or sending a spy, would still be permissible). Of course, FAA Exclusivity wouldn’t solve every problem. It would not prevent foreign governments from collecting information themselves and then providing it to U.S. intelligence agencies, as U.S. law cannot bind a foreign government. And some may argue that FAA provides inadequate civil liberties protections for Americans. This proposal says nothing about the adequacy of that statute in this respect. What it says is that for data held by an American company about a target that is not a U.S. person, the checks within FAA are stronger than those solely under E.O. 12333. Others have argued that the FAA shifts the burden of cooperation solely onto the company, which will suffer greater reputational harm as a more witting participant in affirmatively granting the government’s requests. However, companies have suffered reputational harm as a result of allegations of unwitting cooperation. Making the cooperation known, even if it’s secret, gives the companies the opportunity to account for it in their own planning. The move by certain U.S. companies to place subsidiaries in foreign ownership to resist requests by the U.S. government presents an interesting twist on this idea. In shifting the balance back to increased protections for U.S. companies, this legislation would change the incentives so that claiming U.S. law would have operational advantages in giving companies uniformity of law for all their data. This would also encourage the use of a single choice of law for all data governed by a company—that of the nationality of incorporation—rather than encouraging a choice of law patchwork to govern the data as it flows around the world. Finally, some foreign multinational companies operating in the U.S. and abroad may argue that this is inconsistent with principles that we treat all companies operating in the U.S. the same way for purposes of law. While that would remain true under this proposal, it would create a difference in how the U.S. treats U.S. companies operating abroad compared to how it treats foreign companies abroad. But stretching the U.S. Constitution to foreign companies abroad is to stretch the document too far. If, on the other hand, those companies see advantage in changing their nationality to U.S. in order to claim protections of those laws, then that is the corporate version of the kind of immigration patterns that America has seen since its founding. Conclusion Using FAA’s framework as the exclusive means to access data that U.S. companies are holding will give the Intelligence Community a statutory framework to be able to get the intelligence information that it needs to protect the nation while restoring the trust relationship between the companies and our government. In addition, it will help restore the faith of foreign governments and customers that when American companies are acting overseas, they bring with them American values, including those of privacy protections.

#### Limiting the use of surveillance on US-based servers to national security interests and increasing transparency regarding surveillance is vital to restoring trust and US credibility

**Kehl, 14** – Policy Analyst at New America’s Open Technology Institute (Danielle, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

The NSA mass surveillance programs described in the introduction, conducted domestically pursuant to USA PATRIOT Act Section 215 and FISA Amendments Act Section 702 and conducted outside the U.S. under Executive Order 12333, have arguably had the greatest and most immediate impact on America’s tech industry and global standing. Strictly limiting the scope and purpose of surveillance under these authorities—not just in regard to surveillance of Americans but of non-Americans as well—will be critical to regaining the trust of individuals, companies and countries around the world, as well as stemming the economic and political costs of the NSA programs. The President’s NSA Review Group acknowledged the need for such reform in its report on surveillance programs, affirming that “the right of privacy has been recognized as a basic human right that all nations should respect,” and cautioned that “unrestrained American surveillance of non-United States persons might alienate other nations, fracture the unity of the Internet, and undermine the free flow of information across national boundaries.”324 In addition to recommending a variety new protections for U.S. persons, the Review Group urged in its Recommendation 13 that surveillance of non-U.S. persons under Section 702 or “any other authority”—a reference intended to include Executive Order 12333325 — should be strictly limited to the purpose of protecting national security, should not be used for economic espionage, should not be targeted based solely on a person’s political or religious views, and should be subject to careful oversight and the highest degree of transparency possible.326 Fully implementing this recommendation—and particularly restricting Section 702 and Executive Order 12333 surveillance to specific national security purposes rather than foreign intelligence collection generally—would indicate significant progress toward addressing the concerns raised in the recent Report of the Office of the United Nations High Commissioner for Human Rights on “The Right to Privacy in the Digital Age.” The UN report highlights how, despite the universality of human rights, the common distinction between “‘foreigners’ and ‘citizens’…within national security surveillance oversight regimes” has resulted in “significantly weaker – or even non-existent – privacy protection for foreigners and non-citizens, as compared with those of citizens.”327 The leading legislative reform proposal in the U.S. Congress, the USA FREEDOM Act, would go a long way to protecting both U.S. and non-U.S. persons against the bulk collection under Section 215 of records held by American telephone and Internet companies.328 On that basis, passage of the law would very much help address the trust gap that the NSA programs have created. However, with regard to Section 702, the bill as originally introduced only added new protections for U.S. persons or for wholly domestic communications,329 and even those protections were stripped out or weakened in the version of the bill that was passed by the House of Representatives in May 2014.330 Meanwhile, neither the bill as introduced nor as passed by the House addresses surveillance conducted extraterritorially under Executive or 12333. Therefore, even if USA FREEDOM is eventually approved by both the House and the Senate and signed into law by the President, much more will ultimately need to be done to reassure foreign users of U.S.-based communications networks, services, and products that their rights are being respected. Provide for increased transparency around government surveillance, both from the government and companies. Increased transparency about how the NSA is using its authorities, and how U.S. companies do—or do not—respond when the NSA demands their data is critical to rebuilding the trust that has been lost in the wake of the Snowden disclosures. In July 2013, a coalition of large Internet companies and advocacy groups provided a blueprint for the necessary transparency reforms, in a letter to the Obama Administration and Congress calling for “greater transparency around national security-related requests by the US government to Internet, telephone, and web-based service providers for information about their users and subscribers.”331 Major companies including Facebook, Google, and Microsoft—joined by organizations such as the Center for Democracy and Technology, New America’s Open Technology Institute, and the American Civil Liberties Union—demanded that the companies be allowed to publish aggregate numbers about the specific types of government requests they receive, the types of data requested, and the number of people affected. They also also urged the government to issue its own transparency reports to provide greater clarity about the scope of the NSA’s surveillance programs.332 “This information about how and how often the government is using these legal authorities is important to the American people, who are entitled to have an informed public debate about the appropriateness of those authorities and their use, and to international users of US-based service providers who are concerned about the privacy and security of their communications,” the letter stated.333 Two months later, many of the same companies and organizations issued another letter supporting surveillance transparency legislation proposed by Senator Al Franken (D-MN) and Representative Zoe Lofgren (D-CA) that would have implemented many of the original letter’s recommendations.334 Elements of both bills, consistent with the coalition’s recommendations, were included in the original version of the USA FREEDOM Act introduced in the House and the Senate—as were new strong transparency provisions requiring the FISA court to declassify key legal opinions to better educate the public and policymakers about how it is interpreting and implementing the law. Such strong new transparency requirements are consistent with several recommendations of the President’s Review Group335 and would help address concerns about lack of transparency raised by the UN High Commissioner for Human Rights.336 Unfortunately, all of these transparency provisions from the original USA FREEDOM Act were substantially weakened in the version of the bill that was passed by the House of Representatives in May 2014.337 Congress will need to include stronger transparency provisions in any final version of the USA FREEDOM Act if it intends to meaningfully restore trust in the U.S. Internet and telecommunications industries and stem the loss of business that has begun as a result of the NSA programs. As commentator Mieke Eoyang put it, “If reforms do not deliver sufficient protections and transparency for [tech companies’] customers, especially those abroad who have the least constitutional protections, they will vote with their feet.”338 Recommit to the Internet Freedom agenda in a way that directly addresses issues raised by NSA surveillance, including moving toward international human-rights based standards on surveillance. The United States must act immediately to restore the credibility of the Internet Freedom agenda, lest it become another casualty of the NSA’s surveillance programs. As described in Part IV, various agencies within the U.S. government have taken initial steps to demonstrate goodwill in this area, particularly through the NTIA’s announcement that it intends to transition stewardship of the IANA functions to a global multistakeholder organization and the State Department’s speech outlining six principles to guide signals intelligence collection grounded in international human rights norms. However, it will take a broader effort from across the government to demonstrate that the United States is fully committed to Internet Freedom, including firmly establishing the nature of its support for the evolving multistakeholder system of Internet governance and directly engaging with issues raised by the NSA surveillance programs in international conversations. Supporting international norms that increase confidence in the security of online communications and respect for the rights of Internet users all around the world is integral to restoring U.S. credibility in this area. “We have surveillance programmes that abuse human rights and lack in transparency and accountability precisely because we do not have sufficiently robust, open, and inclusive debates around surveillance and national security policy,” writes Matthew Shears of the Center for Democracy & Technology.339 It is time to begin having those conversations on both a national and an international level, particularly at key upcoming Internet governance convenings including the 2014 Internet Governance Forum, the International Telecommunications Union’s plenipotentiary meeting, and the upcoming WSIS+10 review process.340 Certainly, the United States will not be able to continue promoting the Internet Freedom agenda at these meetings without addressing its national security apparatus and the impact of NSA surveillance on individuals around the world. Rather than being a problem, this presents an opportunity for the U.S. to assume a leadership role in the promotion of better international standards around surveillance practices.

###

# NSA Overreach Extensions

## Internal Links

#### MUSCULAR allows domestic communications to be re-routed abroad – XO12333 incentivizes it

Arnbak and Goldberg 14- cybersecurity and information law research at the Institute for Information Law, LL.M degree from Leiden University, A Competitive Strategy and Game Theory degree from London School of Economics University of Amsterdam; Associate professor in the Computer Science Department at Boston University, phD from Princeton University, B.A.S.c from University of Toronto (Axel and Sharon, “Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting the Network Traffic Abroad”, Working Paper, June 27, 2014)//TT

We have just argued the that collection of US person’s network traffic from abroad presents a major loophole that can be exploited to circumvent legal safeguards protecting Americans and oversight mechanisms in other branches of Government. Put differently, the current regulatory framework for network surveillance by intelligence agencies creates incentives for conducting surveillance on foreign soil, regardless of whether it actually affects American communications or not. We now discuss how the technical details of Internet’s core protocols can cause traffic sent by Americans to be routed abroad, where it can be collected under the most permissive third legal regime for network surveillance. We distinguish two settings: (1) situations where the vagaries of Internet protocols cause Americans’ traffic to naturally be routed abroad, and (2) situations where Internet protocols can be deliberately manipulated to cause Americans’ traffic to be routed abroad. 3.1 Why US Traffic can Naturally be Routed Abroad. The Internet was not designed around geopolitical borders; instead, its design reflects a focus on providing robust and reliable communications while, at the same time, minimizing cost. For this reason, network traffic between two endpoints located on US soil can sometimes be routed outside the US. 3.1.1 Interception in the Intradomain. A network owned by a single organization (even an organization that is nominally “based” in the U.S. such as Yahoo! or Google) can be physically located in multiple jurisdictions. The revealed MUSCULAR/TURMOIL program illustrates how the N.S.A. exploited this by presuming authority under EO 12333 to acquire traffic between Google and Yahoo! servers located on foreign territory, collecting up to 180 million user records per month, regardless of nationality [17].5 Yahoo! and Google replicate data across multiple servers that periodically send data to each other, likely for the purpose of backup and synchronization. These servers are located in geographically diverse locations, likely to prevent valuable data from being lost in case of failures or errors in one location. The MUSCULAR/TURMOIL program collects the traffic sent between these servers: while this traffic can traverse multiple jurisdictions, it remains with the logical boundaries of the internal networks of Yahoo! and Google. Thus, we already have one example where loopholes under the legal regime of EO 12333 were exploited in the intradomain, i.e., within the logical boundaries of a network owned by a single organization. 3.1.2 Interception in the Interdomain. Another possibility is the interdomain setting, where traffic traverses networks belonging to different organizations. Specifically, interdomain routing with BGP can naturally cause traffic originating in a U.S. network to be routed abroad, even when it is destined for a network that is located on U.S. soil. BGP (i.e., the Border Gateway Protocol) is the routing protocol that enables communication between networks owned by different organizations (Autonomous Systems or ASes, e.g., Google’s network, China Telecom’s network, or Boston University’s network). As shown in Fig. 1, ASes are interconnected, creating a graph where nodes are ASes and edges are the links between them. ASes use BGP to learn paths through the AS-level graph; an AS discovers a path to a destination AS via BGP messages that it receives from each of its neighboring ASes. An AS then uses its local routing policies to choose a single most-preferred path to the destination AS from the set of paths it learned from its neighbors, and then forwards all traffic for the destination AS to the neighboring AS that announced the most-preferred path. Importantly, the local policies used to determine route selection in BGP are typically agnostic to geopolitical considerations; path selection is often based on the price of forwarding traffic to the neighboring AS that announced the path, as well as on the number of ASes on the path announced by that neighbor. This means that it can sometimes be cheaper to forward traffic through a neighboring AS that is physically located in a different country, rather than one located in the same country; this situation is common, for example, in South America (where network paths between two South American endpoint ASes often cross undersea cables to Miami [24]) and Canada (where network paths between two Canadian endpoint ASes regularly traverse American ASes [10]). Ongoing work by one of the authors seeks to measure how often this occurs when both endpoints are located in the US. 3.2 How Deliberate Manipulations can Divert US traffic Abroad. In addition to situations where Americans’ traffic is naturally routed abroad, the Internet’s core protocols – BGP and DNS – can be deliberately manipulated to force traffic originating and terminating in an American network to be routed abroad. As we discussed earlier, deliberately manipulating Internet protocols for subsequent data collection from abroad, even when the manipulation was performed from within the U.S., does not fall under the legal definition for ‘electronic surveillance’ in FISA; instead, these manipulations are regulated under the most permissive third legal regime for network surveillance, EO 12333 (and perhaps further specified in non-public guidelines). 3.2.1 Deliberate BGP Manipulations. We know of numerous real-world incidents where manipulations of the BGP protocol have caused network traffic to take unusual paths, including situations where traffic from two American endpoint ASes was rerouted through ASes physically located abroad. While there is no evidence that these incidents were part of a surveillance operation, or even a clear understanding of why they occurred, it is instructive to consider them as examples of how an authority could circumvent the legal safeguards protecting U.S. persons by forcing their network traffic to be diverted abroad. In 2013, Renesys observed a number of highly-targeted manipulations of BGP that caused traffic sent between two American endpoint ASes to be routed through Iceland [26]. One manipulation that occurred on June 31, 2013, is shown in Fig. 1. Traffic originating at an endpoint physically located in Denver and logically located inside Atrato’s AS, then travels to an Icelandic AS (Siminn) and then back to its destination, which is physically located in Denver and logically located in Qwest/Centurylink’s AS. Renesys also observed nine other Icelandic ASes, as well as a few ASes based in Belarus, performing similar BGP manipulations. Similar incidents have been known to occur periodically in the Internet [9]. In 2010, for example, a routing incident caused traffic sent between multiple American endpoint ASes to be diverted through China Telecom during a single 18-minute time period [11]. In 2008, a presentation at DEFCON [27] demon- strated how these manipulations could be performed in a covert manner that could be used to confound the network measurement mechanisms (e.g., tracer- oute, BGP looking glasses) that researchers used to detect the 2010 and 2013 incidents mentioned above. Target and Location of the BGP Manipulation. To understand how the legal framework applies to manipulations of the BGP protocol for the purpose of surveillance, we need to understand who is targeted, and where the manipulation is executed. The incidents mentioned above are executed as follows. Per Fig. 1, the manip- ulating AS (e.g., Icelandic AS Siminn) manages to divert traffic to itself by send- ing, to some carefully selected neighboring ASes, BGP messages that “imper- sonate” those sent by the legitimate destination AS (Qwest/Centurylink’s AS). Because BGP lacks authentication mechanisms, these neighbors (Atrato’s AS) accept the BGP message for the impersonated route,and select the impersonated route. They then forwards their traffic along the impersonated route to the ma- nipulator’s AS (Icelandic AS Siminn). The manipulator receives the traffic, and forwards it back to the legitimate destination AS (Qwest/Centurylink) via a le- gitimate route. The manipulator AS therefore becomes a man-in-the-middle be- tween targeted source AS (Atrato) and the destination AS (Qwest/Centurylink). While Fig. 1 shows traffic between two individual endpoints within Atrato and Qwest/Centurylink being intercepted by the BGP manipulation, typically all traffic originating inside Atrato and destined to the Qwest/Centurylink AS would be intercepted by the manipulator. To further understand the targets of this manipulation, we consider what it means to send BGP messages that “impersonate” a legitimate destination AS. First, we provide more detail on BGP messages. A BGP message is used to ad- vertise the path to a specific IP address block hosted by a particular destination AS.6 Each AS in the Internet is allocated one of more IP address blocks, used to identify devices operated by that AS. Multiple devices can use a single IP address; thus, referring back to our legal analysis, a single IP address can be used by multiple devices or even ‘persons’. A separate BGP message is used to advertise each IP address block allocated to a particular destination AS. Thus, sending a BGP message that “impersonates” a legitimate destination AS means that the manipulator AS (Icelandic AS Siminn) sends a BGP message that claims a false route to the IP address block (206.51.69.0/24). As shown in Fig. 1, the manipulator AS (Siminn) falsely claims that the IP address block 206.51.69.0/24 is allocated to Siminn’s own customer AS, the Icelandic Opin Kerfi AS 48685; in reality that IP address block is allocated to the legitimate destination AS (Qwest/Centurylink). Because BGP lacks mechanisms that can authenticate allocations of IP address blocks, the manipulator’s neighbors will accept this impersonated route, and forward all traffic destined to the IP ad- dresses in the disputed block to manipulator’s AS (Siminn), instead of the legiti- mate destination (Qwest/Centurylink). This “impersonated” route will continue to propagate through the network, as the ASes that select the “impersonated” route pass it on to their own neighbors. Thus, we can see that the “target” of this BGP manipulation is (1) all traffic sent by each source AS that selected the impersonated route (e.g., all traffic from Atrato) that (2) is sent to IP addresses in the block that the manipulator falsely claims is allocated to him (e.g., the 256 IP addresses contained in the block 206.51.69.0/24). That has important legal implications: the permissive legal regime under EO 12333 applies to such surveillance operations, as it does not necessarily ‘intentionally’ target a ‘known, particular U.S. person’. It is also important to note that this BGP manipulation (which involves sending just a single “impersonated” BGP message from the Icelandic AS Siminn, shown in red in Figure 1) is executed entirely outside of the targeted endpoint ASes (Atrato and Qwest/Centurylink). Thus, this BGP manipulation can be executed entirely abroad. 3.2.2 Deliberate DNS Manipulations. An alternate network protocol manipulation that can divert traffic to servers located abroad involves manipulating the DNS (i.e., Domain Name System). The DNS is a core Internet protocol that maps human-readable domain names (e.g., www.facebook.com) to the IP addresses that identify the servers hosting the domain (e.g., 69.63.176.13); applications that wish to communicate with the domain (www.facebook.com) first perform a DNS lookup to learn the IP address of the server that hosts the domain, and then direct their network traffic to that IP address. DNS lookups for end users and applications within a single AS are typically performed by a device called a recursive resolver, typically located within the AS; see Fig. 2. Recursive resolvers engage in the DNS protocol with devices located outside their AS, and return responses to DNS lookups to users and applications within their AS. The DNS is well known to be vulnerable to manipulations the subvert the mapping from a domain name to IP address [8, 20, 22].7 These manipulations, which have often been observed in the wild as mechanisms for performing net- work censorship [1, 35], can also be used to redirect network traffic through servers located abroad. Fig. 2 presents an example. Suppose that a manipulator wants network traffic destined to www.facebook.com from a given source AS (e.g., Boston University) to be routed though a foreign server located abroad. Suppose the foreign server has IP address 6.6.6.6. The manipulator can execute a DNS manipulation that causes the recursive resolver in the source AS (Boston University) to map www.facebook.com to IP address 6.6.6.6. All network traffic for www.facebook.com from the source AS (Boston University) will then flow to the foreign server at IP address 6.6.6.6. Finally, the foreign server will silently for- ward the traffic it receives to the real facebook server at IP address 69.63.176.13. Thus, the foreign server becomes a man-in-the-middle for traffic sent between two US endpoints (Boston University and www.facebook.com). Target and Location of the DNS Manipulation. This manipulation is more fined-grained than the BGP manipulation we discussed earlier: it targets all traffic sent to a particular domain (www.facebook.com) that is sent by all users and applications served by the targeted recursive resolver (i.e., within a Boston University’s AS). Again, the permissive legal regime under EO 12333 applies to such surveillance operations, as the traffic does not necessarily ‘intentionally target a U.S. person’. Moreover, like the BGP manipulations we described earlier, these DNS manipulations can be conducted entirely abroad; Hertzberg and Shulman [20] describe a technique that allows this manipulation to be executed by a device located entirely outside the targeted source AS. For those interested in the de- tails, we sketch out the technique below and in Fig. 3: Figure 3: We show how the manipulator located abroad can subvert the DNS mapping for www.facebook.com at the target source AS 111 (Boston University). First, it is important to observe that recursive resolvers usually do not accept messages from senders outside their AS; however, mailservers do. (Mailservers are devices that provide email services for an AS. They therefore need to accept emails from outside the AS.) Thus, a manipulator located outside the target AS can use the mailserver to attack the recursive resolver. Specifically, the manipulator sends some carefully-crafted messages to a mailserver located inside the target AS. These messages act as a trigger for the mailserver to send DNS queries to the DNS resolver inside the AS; the DNS resolver accepts messages from the mailserver, because the mailserver is inside the AS. The recursive resolver then proceeds to resolve the mailserver’s DNS queries. To do this, the recursive re- solver sends DNS messages to other DNS servers outside the target AS. Finally, the manipulator responds to these DNS messages with carefully-crafted bogus DNS messages of its own; this allows the manipulator to subvert the recursive resolver’s mapping from a domain name to an IP address. Observe that this manipulation just involves sending messages from outside the AS; no internal devices in the AS need to be compromised.

#### XO 12333 is used to collect large quantities of metadata and find personal information on U.S. citizens

Rotenberg, EPIC President and Executive Director, 6-16-15 [Electronic privacy information center, non-profit research and educational organization established in 1994 to focus

public attention on emerging privacy and civil liberties issues.12 We work with a distinguished panel of advisors in the fields of law, technology and public policy., COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER, [file:///C:/Users/Jonah/Downloads/EPIC-12333-PCLOB-Comments-FINAL.pdf](file:///C%3A/Users/Jonah/Downloads/EPIC-12333-PCLOB-Comments-FINAL.pdf)] Schloss2

Despite the restrictions placed on the Intelligence Community by Executive Order 12333 and the foreign intelligence surveillance laws, the NSA and CIA continue to engage in bulk collection and interception of communications and sensitive information about United States Persons.33 As Senate Intelligence Committee member Senator Ron Wyden recently noted, “Today there’s a global communications infrastructure, so there’s a greater risk of collecting on Americans when the NSA collects overseas.”34 EPIC also raised this issue during a PCLOB’s public meeting last year, pointing out that, “Although 12333 requires a court order to target a United States Person, this is of little comfort. Given the global nature of communications, the indiscriminate mass surveillance the NSA conducts overseas captures the information of United States Persons.”35 Now that communications are transmitted via a global telecommunications network, the territorial restrictions of EO 12333 do not meaningfully limit the bulk collection of U.S. person information and private communications transmitted via U.S. companies. These programs significantly infringe citizens’ rights under both the Privacy Act and the Fourth Amendment. Yet there is very little independent oversight of these programs; collection activities of the IC are difficult to monitor. As EPIC previously stated in a letter to PCLOB, “[t]he Privacy Act defines the right to privacy with regard to the collection and use of personal information by federal agencies . . . . Much has happened since 9-11 that is clearly contrary to the purposes of Privacy Act and the expectation of many Americans who rightly believe that the U.S. government would not develop massive databases to secretly profile Americans.”36 The Supreme Court recently issued a landmark ruling on digital privacy rights, finding that the Fourth Amendment requires officers to obtain a warrant prior to searching an individuals’ cell phone incident to arrest. 37 The Court emphasized that “the Fourth Amendment was the founding generation’s response to the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era, which allowed British officers to rummage through homes in an unrestrained search of evidence of criminal activity.”38 The Court also held that the Fourth Amendment requires heightened protections for digital content and communications, finding digital files are fundamentally different than analog records.39 Government programs of mass surveillance that indiscriminately collect data about U.S. Persons are similar to the reviled “general warrants” that the Founders sought to abolish.40However, in the context of foreign intelligence collection, it is difficult to ensure that collection is properly targeted and limited. As EPIC has emphasized, “the only check on surveillance under EO 12333 comes from Executive oversight. This type of self-regulation has proven to be ineffective at best in limiting surveillance overreach. The minimal oversight in place does not even give the appearance of the checks and balances provided by judicial or congressionaloversight.”41 It is urgent that PCLOB examine the scope of collection currently conducted under EO12333, given that courts have already ruled that other NSA bulk collection programs wereillegal.42 EPIC previously reported on one of these other agency programs: “On October 3, 2011,the FISC ruled that the NSA ‘upstream collection’ of Internet communications violated the Fourth Amendment and the FISA. Specifically, the targeting and minimization procedures adopted by the NSA were not sufficient to protect the significant number (more than 50,000 per year) of wholly domestic communications obtained via ‘upstream collection.’”43 Courts have already imposed new restrictions on these narrower surveillance programs conducted under Congressional and Judicial oversight, and the much broader EO 12333 bulk collection programs present an even more pressing need for new oversight and limitations. The privacy impact of these surveillance programs is not limited to the collection of the contents of U.S. persons’ communications; the collection of metadata can be even more intrusive. In an amicus curiae brief in the U.S. Court of Appeals for the Ninth Circuit, EPIC emphasized that “Analysis of large metadata sets equivalent to those created by the NSA can reveal even more personal information including the identities of our friends and associates, the identities of our loved ones, and even our political, religious, or social affiliations.”44 EPIC stressed that “[a]ll metadata can be used to make inferences about our daily activities, but location data is particularly sensitive since it can uniquely identify individuals, reconstruct a person’s movements across space and time, predict future movements, and determine social interactions and private associations.”45 Collection of metadata can be a massive invasion of privacy, especially if the procedures for collection are too expansive.

### AT: Freedom Act solves

#### The Freedom Act didn’t actually curtail surveillance

**Brenner, 15** - Senior Fellow, the Center for Transatlantic Relations; Professor of International Affairs, University of Pittsburgh (Michael, Huffington Post, “The NSA's Second Coming” 6/8,

<http://www.huffingtonpost.com/michael-brenner/the-nsas-second-coming_b_7535058.html>

That all makes for one awesome production. Doubtless there will be a film adaptation immortalized in a script by Bob Woodward. Something like that will happen -- even though it is a concocted yarn whose meaning has been twisted and whose significance has been vastly inflated. For the truth is that what Congress did, and what it did not do earlier, changes very little -- and nothing of cardinal importance. The main effect is to give the impression of change so as to release pressure for reform that might really be meaningful. The base truth is that everything that counts remains the same. To entrench and to legitimate a system of massive surveillance that undercuts our privacy while doing nothing to secure our well-being. Let's look at the false notes struck by this narrative. Matters of Fact 1. The so-called restrictions on bulk data collection apply only to telephone calls. All else is exempted: emails, Internet searches, social media, and info regarding each that is retained in our communicating devices. 2. The restrictions on real-time surveillance of telephone calls can be overcome by the granting of a warrant by the FISA upon request by NSA, FBI, Justice Department, CIA -- not to speak of local authorities. That Court, over the past eight years, has refused only 11 of 33,900 requests. The judges, by the way, are handpicked by Supreme Court Chief Justice John Roberts who has jumped into the policy arena by declaring himself strongly opposed to any tightening of restrictions on how the court operates or on the NSA's methods. The FISA court's attitude toward government spying on Americans has been generous to the extreme. Former lead judge of the FISA Court, John D. Bates, has campaigned vigorously on behalf of the status quo. He even objected to the extra workload of requiring that courts approve all national security letters, which are administrative subpoenas allowing the F.B.I. to obtain records about communications and financial transactions without court approval. 3. The specified targets may be organizations, groups and networks as well as an individual. In practice, that means each grant of surveillance power may authorize comprehensive electronic spying on hundreds or thousands of citizens. Currently the NSA is overwhelmed by the billions of communications they register and try to catalogue each week. Long-term data retention only makes sense if there is a project afoot to exploit it systematically in order to control, to suppress, to penalize. There is no such Big Brother plan in place or on the horizon. NSA operations fortunately have instead been conceived and managed by fantasists and bureaucratic empire builders -- as is demonstrated by Edward Snowden's leaks of their immense target list and their major intelligence failures. 4. The terms of the warrants allow for a two-step "hop" from the identified target to others whose suspect communications emerge from the initial combing. Here is one hypothetical scenario. The NSA requests approval from the FISA court to collect the communications of the Arab-American Civil Rights League on the grounds that it suspects some dubious characters have been using its facilities. Over a period of months (if there a restriction on the duration of electronic surveillance under FISA rules), they register 1,000 communications. Using 'first hop' privileges they identify 250 persons whose own communications they wish to tap. Using "second hop" privileges they next identify a total of 1,500 more people whose communications they wish to tap. That makes a total of 2,700 persons whose telephone calls they are monitoring and storing. Each year, the NSC requests warrants from the FISA courts about 500 times. Hence, we can project more than 1 million telephone numbers now under surveillance for an indefinite period of time. For we should further note that once an official investigation is begun the records acquire the status of legal documents in a judicial or quasi-judicial proceeding. 5. There is an exemption for on-going investigations. The Patriot Act's Section 224, its "grandfather clause", allows active investigations that began prior to midnight on Monday to continue using the expired programs.They number in the thousands given the hyper-activism of our security agencies in identifying subjects for their attentions in order to justify vast capabilities and vast budgets. Those broadly cast investigations can go on for years. And all of this is secret.

#### FREEDOM Act reforms for the FISA court are hollow – no substantive protections

**Brenner, 15** - Senior Fellow, the Center for Transatlantic Relations; Professor of International Affairs, University of Pittsburgh (Michael, Huffington Post, “The NSA's Second Coming” 6/8,

<http://www.huffingtonpost.com/michael-brenner/the-nsas-second-coming_b_7535058.html>

8. Sponsors of the Freedom Act trumpet a supposed breakthrough insofar as it mandates some small transparency from the secret Foreign Intelligence Surveillance Court. It vaguely affirms that the Court will be required to declassify a few of its tightly held opinions. Those are opinions explaining why a warrant request is approved -- as they automatically are. There is no reason to expect any great revelations. After all, the essence of the FISA Court's reasoning is well known. We live in dangerous times -- as witness 9/11; the government assures us that there is compelling evidence of dangerous persons on the prowl and plots afoot; the classified information upon which that assessment is made is persuasive -- even though we have been granted only a glimpse of a brief summary; this Court cannot take on itself the responsibility of overriding the professional judgment of our public servants and thereby put at risk the security and well-being of the American people; blah-blah, blah. Judge Bates reflects the reigning philosophy of the FISA court in warning that greater public disclosure of unclassified summaries of court rulings would "likely to promote confusion and misunderstanding" among the likes of you and me. 9. The new legislation also allows the judges to appoint a "friend of court" to argue on behalf of privacy concerns. This does not mean that there will be adversary proceedings or a systematic examination of the case for a warrant. It simply means that there may be designated persons available to remind the FISA judges that privacy considerations should be taken into account in their deliberations. For all that is worth, they might as well prepare a form letter that is emailed to the Court every time that a request arrives on their computers.

#### The Freedom Act is largely symbolic – hardly restricts surveillance

Timm 6/2 - co-founder and the executive director of the Freedom of the Press Foundation (Trevor Timm, Boing Boing, 6/2/2015, http://boingboing.net/2015/06/02/congress-passes-usa-freedom-ac.html)//MBB

Today the Senate passed a version of the USA Freedom Act, a bill touted by its authors as surveillance reform that will end the NSA’s mass, suspicionless collection of Americans’ personal data. Given that parts of the Patriot Act expired on June 1st, and that the government is pretending the expiration is a “crisis” rather than an opportunity, President Obama is expected to sign the bill as soon as possible. While the bill has many significant flaws, the USA Freedom Act vote is also historic: it’s the first time since the 1970s that Congress has indicated its intention to restrict the vast powers of intelligence agencies like the NSA, rather than exponentially expand them. It also shows the power that investigative journalism and brave whistleblowing can have on even the most entrenched government interests. Two years ago, debating these modest changes would’ve been unthinkable, and it is absolutely a vindication for Edward Snowden. Unfortunately, the bill is also woefully inadequate and largely symbolic, and Congress would’ve been better off letting Section 215 of the Patriot Act expire permanently. The USA Freedom Act supposedly bans bulk collection of phone records or any other private records, and we certainly hope it actually does. But its provisions are vague and confusing, leading many legal experts to believe they could be re-interpreted in secret—by NSA lawyers with a history of warping the common definitions of ordinary words beyond recognition—and could lead the FISA court to continue to allow the NSA to collect large quantities of Americans’ data in secret. (The administration will shamefully now re-start the phone program that expired on Monday for six months, as allowed under the new law's "transition" period.) The ultra-secret FISA court, a Kafkaesque nightmare for civil liberties, also gets to keep many of its worst features, with just minor changes around the edges. Such an anathema to democracy should be dismantled entirely. The USA Freedom Act also does not touch on two of the NSA’s most powerful and controversial tools: the FISA Amendments Act and Executive Order 12333, which have been used to scan untold billions of emails coming in and out of the United States, and give the agency free rein to spy on 95% of the world’s population with virtually no restrictions. And perhaps most shamefully, given that Congress never would’ve even had this debate without Edward Snowden, the bill does nothing for whistleblowers who can be prosecuted as spies under the Espionage Act for speaking to journalists and telling the American public the truth. As Snowden himself said two weeks ago, we hope the USA Freedom Act is just the beginning of Congress’ reform of the NSA, and not the end. And we are reminded that it took more than five years for the Church Committee’s intelligence reforms to make their way through Congress in the 1970s.

### AT: No metadata abuse

#### We kill people based on metadata – it generates more info than actual content

Schneier, 15 - fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc (Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Introduction)//AK

There are other sources of intimate data and metadata. Records of your purchasing habits reveal a lot about who you are. Your tweets tell the world what time you wake up in the morning, and what time you go to bed each night. Your buddy lists and address books reveal your political affiliation and sexual orientation. Your e-mail headers reveal who is central to your professional, social, and romantic life. One way to think about it is that data is content, and metadata is context. Metadata can be much more revealing than data, especially when collected in the aggregate. When you have one person under surveillance, the contents of conversations, text messages, and emails can be more important than the metadata. But when you have an entire population under surveillance, the metadata is far more meaningful, important, and useful. As former NSA general counsel Stewart Baker said, “Metadata absolutely tells you everything about somebody’s life. If you have enough metadata you don’t really need content.” In 2014, former NSA and CIA director Michael Hayden remarked, “We kill people based on metadata.”

## Internet Freedom Scenario

### Uniqueness – US pushing IF agenda

#### The US government continues to push for IF reforms

**Fontaine, 14** – President of the Center for a New American Security; was foreign policy advisor to Senator John McCain for more than five years; Worked at the State Department, the National Security Council and the Senate Foreign Relations Committee; was associate director for near Eastern affairs at the National Security Council; B.A. in International Relations from Tulan University (Richard, “Bringing Liberty Online; Reenergizing the Internet Freedom Agenda in a Post-Snowden Era”, Center for a New American Security, September 18, 2014, http://www.cnas.org/sites/default/files/publications-pdf/CNAS\_BringingLibertyOnline\_Fontaine.pdf)//TT

Despite the international outrage, and both public and private criticism of U.S. surveillance policies, the U.S. government has continued its Internet freedom–related activities, albeit at a lower public volume. In early 2014, Secretary of State John Kerry, addressing the Freedom Online Coalition conference in Estonia, called for an “open, secure, and inclusive Internet.”33 U.S. Internet freedom programming continues: the State Department’s Bureau of Democracy, Human Rights and Labor alone planned to expend roughly $18 million in 2014 on anti-censorship technology, secure communications, technology training and rapid response to bloggers under threat.34 In June, the United States sponsored a successful U.N. Human Rights Council resolution reaffirming that the same rights that people have offline, including freedom of expression, must be protected online, regardless of frontiers.35 While continuing to execute the Internet freedom agenda, U.S. officials have attempted to reconcile their government’s surveillance practices with its expressed desire for greater online freedom. This is challenging, to say the least. U.S. officials draw a critical distinction between monitoring communications for purposes of protecting national security and surveillance aimed at repressing political speech and activity. While this distinction is intuitive to many Americans, it is likely to be lost on many others, particularly where autocratic regimes consider domestic political dissent to be a national security threat. At its bluntest, the American position is that it is legitimate, for example, for the U.S. government, but not for the Chinese government, to surveil Chinese citizens. This is and will remain a tough sell. Secretary Kerry has defended the Obama administration’s reforms to signals intelligence collection, saying that they are based on the rule of law, conducted pursuant to a legitimate purpose, guided by proper oversight, characterized by greater transparency than before and fully consistent with the American vision of a free and open Internet.36 In March 2014, Deputy Assistant Secretary of State Scott Busby addressed the linkage between surveillance and Internet freedom and added two principles to Kerry’s – that surveillance should not be arbitrary but rather as tailored as possible, and that decisions about intelligence collection priorities should be informed by guidance from an authority outside the collection agency.37 In addition, the U.S. government has taken other steps to temper the international reaction. For example, the Department of Commerce opted to relinquish its oversight of ICANN – the organization that manages domain name registries – to the “global Internet community.”38

### Overreach kills internet freedom

#### NSA surveillance wrecks US cred in promoting Internet Freedom and spills over to larger foreign policy cred

**Kehl, 14** – Policy Analyst at New America’s Open Technology Institute (Danielle, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

Mandatory data localization proposals are just one of a number of ways that foreign governments have reacted to NSA surveillance in a manner that threatens U.S. foreign policy interests, particularly with regard to Internet Freedom. There has been a quiet tension between how the U.S. approaches freedom of expression online in its foreign policy and its domestic laws ever since Secretary of State Hillary Clinton effectively launched the Internet Freedom agenda in January 2010.170 But the NSA disclosures shined a bright spotlight on the contradiction: the U.S. government promotes free expression abroad and aims to prevent repressive governments from monitoring and censoring their citizens while simultaneously supporting domestic laws that authorize surveillance and bulk data collection. As cybersecurity expert and Internet governance scholar Ron Deibert wrote a few days after the first revelations: “There are unintended consequences of the NSA scandal that will undermine U.S. foreign policy interests – in particular, the ‘Internet Freedom’ agenda espoused by the U.S. State Department and its allies.”171 Deibert accurately predicted that the news would trigger reactions from both policymakers and ordinary citizens abroad, who would begin to question their dependence on American technologies and the hidden motivations behind the United States’ promotion of Internet Freedom. In some countries, the scandal would be used as an excuse to revive dormant debates about dropping American companies from official contracts, score political points at the expense of the United States, and even justify local monitoring and surveillance. Deibert’s speculation has so far proven quite prescient. As we will describe in this section, the ongoing revelations have done significant damage to the credibility of the U.S. Internet Freedom agenda and further jeopardized the United States’ position in the global Internet governance debates. Moreover, the repercussions from NSA spying have bled over from the Internet policy realm to impact broader U.S. foreign policy goals and relationships with government officials and a range of other important stakeholders abroad. In an essay entitled, “The End of Hypocrisy: American Foreign Policy in the Age of Leaks,” international relations scholars Henry Farrell and Martha Finnemore argue that a critical, lasting impact of information provided by leakers like Edward Snowden is “the documented confirmation they provide of what the United States is actually doing and why. When these deeds turn out to clash with the government’s public rhetoric, as they so often do, it becomes harder for U.S. allies to overlook Washington’s covert behavior and easier for U.S. adversaries to justify their own.”172 Toward the end of the essay, Farrell and Finnemore suggest, “The U.S. government, its friends, and its foes can no longer plausibly deny the dark side of U.S. foreign policy and will have to address it head-on.” Indeed, the U.S. is currently working to repair damaged bilateral and multilateral relations with countries from Germany and France to Russia and Israel,173 and it is likely that the effects of the NSA disclosures will be felt for years in fields far beyond Internet policy.174

#### This overreach will end US internet leadership and cause global fragmentation

**Eoyang, 13** - Director of the National Security Program (Mieke, “NSA Snooping's Negative Impact On Business Would Have The Founding Fathers 'Aghast'” Forbes, <http://www.forbes.com/sites/realspin/2013/12/20/nsa-snoopings-negative-impact-on-business-would-have-the-founding-fathers-aghast/>

Second, what will this mean for the future of Internet governance? Since its earliest days, the U.S.-based Internet Corporation for Assigned Names and Numbers (ICANN) has governed the web. As the Internet has expanded, several nations, especially China, have been pressing to end American dominance and transfer control of Internet governance to the International Telecommunication Union (ITU), a specialized agency within the United Nations. Worse still for prospects of continued American dominance, the NSA revelations have prompted calls for extensive regional control of the Internet. For example, Brazil, which has long called for such regional control, will host an important Internet governance conference in April that could challenge America’s role. Unless the U.S. government takes steps to restore some degree of trust, the groundswell of international interest in a new approach to Internet governance could undermine or end U.S. Internet leadership. This could leave management of the Internet to nations like China or Russia that do not share America’s commitment to safety, openness, competition, and growth. Recommendations for change are coming from many corners. President Obama’s advisory group on NSA reform is calling for an end to bulk collection of Americans’ metadata and other steps to restore protections abroad. Major Internet companies have called for greater restrictions on surveillance activities, saying the balance has tipped too far from the individual. The government should heed these calls for reflection and reform. Without understanding the economic implications of our security policies and taking reasonable steps to restore trust in America’s surveillance efforts, our Internet dominance and our economy could pay the price.

#### US hypocrisy in surveillance policies kills Internet freedom agenda

**Gross, 13** – Covers technology and telecom policy in the US government for the IDG News Service, was an editor and reporter at daily newspapers for 10 years (Grant, “The NSA scandal has damaged U.S. credibility online”, Computer World, December 5, 2013, http://www.computerworld.com/article/2486546/internet/the-nsa-scandal-has-damaged-u-s--credibility-online.html)//TT

The U.S. government has a huge image problem worldwide as it promotes Internet freedom on one hand and conducts mass surveillance on the other, potentially creating major problems for U.S. technology companies, a former official with President Barack Obama's administration said Thursday. Many U.S. policy makers don't recognize the level of distrust created by recent revelations about U.S. National Security Agency surveillance, and that lack of trust will drive other countries away from U.S. technology firms, said Andrew McLaughlin, former White House deputy CTO. "We, as an advocate for freedom of speech and privacy worldwide, are much, much, much more screwed than we generally think in Washington, and ... American industry and our Internet sector is more much, much, much more screwed than we think internationally," McLaughlin said during a speech at a Human Rights First summit in Washington, D.C. Many overseas critics of the U.S. see the Obama administration's push for Internet freedom as "profoundly hypocritical" in the face of the NSA surveillance revelations and a continued push by U.S. trade officials to have U.S. trading partners filter the Internet to protect against copyright violations, said McLaughlin, now president of Digg, the online news aggregation service. The NSA surveillance has led to an intense "level of anger and the degree of betrayal" in many countries that U.S. policy makers don't seem to fully appreciate, he said. And many countries have begun to explore other options beyond U.S. technology companies because of the surveillance revelations, he added. There's now a perception outside the U.S. that the country's technology companies "are willing instruments of violation of civil rights and civil liberties," McLaughlin said. "We have essentially nationalized what were previously seen as stateless Internet entities." Many countries will move to use domestic technology companies and require citizen data to stay within their borders, he said. "If you're an American company that sells cloud services, I think you've probably sold your last contract to a foreign government," he said.

### Internet freedom key to democracy

#### Internet freedom facilitates democratic transitions—extensive scholarship proves

**Nisbet et al 12** – PhD in communication, assistant professor at the School of Communication at The Ohio State University, research on public diplomacy, foreign policy, comparative democratization, and communication (Erik, “Internet Use and Democratic Demands: A Multinational, Multilevel Model of Internet Use and Citizen Attitudes About Democracy”, Journal of Communication, April 2012, [http://onlinelibrary.wiley.com/doi/10.1111/j.1460-2466.2012.01627.x/epdf)//DBI](http://onlinelibrary.wiley.com/doi/10.1111/j.1460-2466.2012.01627.x/epdf%29//DBI)

Moving from institutions to citizens, an open question is whether greater Internet penetration and use influence individual attitudes about democracy? Though not empirically tested, Howard (2009) answers this question in the affirmative, theorizing that Internet use plays an important role in shaping and mobilizing citizen attitudes about democracy in transitioning or emerging democracies. Howard asserts that traditional media in nondemocratic states ‘‘constrains’’ public opinion to those of ruling elites, creating a passive public incapable of challenging autocratic institutions and power-relations. Leslie (2002) and Howard view the Internet as distinct from the one-way communication of radio, television, and print media that provide information to an audience, but are incapable of soliciting immediate feedback. The Internet is lauded as having great democratic potential because it does allow for feedback and encourages the development of ‘‘participant’’ citizens, as described by Almond and Verba (1963). Rather than acting as passive receptors of political information, participant citizens are more sophisticated and engage with political information provided to them and subsequently respond or make ‘‘demands’’ from it (Almond & Verba, 1963). For example, as Lei (2011) observes in the case of China, the ‘‘Internet has contributed to a more critical and politicized citizenry’’ with ‘‘citizens no longer merely compliant receivers of official discourse’’ (p. 311). In this sense, Howard sees the potential of the Internet, especially when paired with organizations such as political parties or movements, to promote the formation of ‘‘mass’’ public opinion that demands political change within authoritarian or democratizing states. Other scholars also embrace the Internet’s capacity to promote political change by serving as a pluralistic media platform (Bratton et al., 2005; Groshek, 2009; Lei, 2011). Bratton and colleagues (2005) argue that media use in transitioning or emerging democracies ‘‘expands the range of considerations that people bear in forming their political and economic attitudes,’’ which promotes democratic citizenship and greater demand for democratic processes and reform (Bratton et al., 2005, p. 209). Media that enjoys low government regulation and high plurality of content have ‘‘the greatest impact in inducing an audience to reject authoritarian rule, especially one- party rule,’’ compared to other forms of media use (p. 210). In this context, Groshek (2009) draws upon media dependency theory (Ball-Rokeach & DeFleur, 1976) to argue that Internet use influences the democratic orientations of audiences—which in turn promotes (democratic) change in sociopolitical systems in which audiences are embedded. Internet penetration, in other words, allows citizens to access more pluralistic content that increases citizen demand for democracy. Increased demand promotes ‘‘bottom-up’’ democratization by increasing the likelihood of democratic transitions in nondemocratic states or strengthening democratic institutions in young democracies. Lei (2011) asserts this bottom-up democratization has emerged in China, with ‘‘netizens’’ constituting ‘‘an important social force that imposes much pressure on the authoritarian state’’ (p. 311). Moreover, this theoretical perspective is consistent with scholarship examining the role of citizen attitudes in processes of democratization (Inglehart & Welzel, 2005; Mattes & Bratton, 2007; Welzel, 2007).

### Democracy solves war

#### Empirics prove that democracies are in wars less and if they are lose a lot less than other systems

Hegre, Peace and Conflict Research, 14 [Havard, Department of Peace and Conflict Research, Uppsala University & Peace Research Institute Oslo (PRIO), Democracy and Armed Conflict, jpr.sagepub.com/content/early/2014/01/08/0022343313512852.full.pdf] Schloss

The interstate democratic peace has been studied at several ‘levels of analysis’ (Gleditsch & Hegre, 1997). At the dyadic level, there is considerable agreement that the ‘absence of war between democratic states comes as close as anything we have to an empirical law in international relations’ (Levy, 1989: 270).3 Important studies in favor of the proposition are Rummel (1983), Doyle (1983, 1986), and a string of studies by Bruce Russett and coauthors (e.g. Maoz & Russett, 1992, 1993; Russett & Oneal, 2001). Following the review of Gleditsch (1992), JPR became a major outlet for the debate.4 The dyadic finding has to a large degree withstood a series of counter-arguments. I discuss these in detail below. There is less compelling evidence for democratic countries being less warlike overall – the ‘monadic’ level of the democratic peace. The bulk of the early large-N studies (e.g. Small & Singer, 1976; Weede, 1984), agree with Chan (1984) who found that ‘relatively free’ countries participated in war just as much as the ‘less free’. Gleditsch & Hegre (1997) show that democracies rarely initiate wars, and Hegre (2008) that they are more peaceful overall when controlling for their military potential. Research at the system level has recently attracted renewed attention.5 Gleditsch & Hegre (1997) suggest that a world with an intermediate share of democracy may be associated with more war since the probability of war on average is highest in dyads with one democracy and one non-democracy. However, an increase in the proportion of countries that are democratic may alter the dyadic and monadic probabilities as systemic democratization affects international interactions (Russett, 1993; Huntley, 1996; Mitchell, Gates & Hegre, 1999; Kadera, Crescenzi & Shannon, 2003). Cederman (2001) rephrases the standard account of Kant (1795/1991), seeing the development of the democratic peace as a dialectic process where states gradually learn to form (democratic) pacific unions. He shows that the risk of war between democracies has been falling over the past two centuries. The risk of non-democratic war has also declined, but less swiftly. Relatedly, Mitchell (2002) shows that non-democracies in the Americas became much more likely to settle territorial claims peacefully when the proportion of democracies in the system increased. Gartzke & Weisiger (2013), on the other hand, argue that regime type becomes a less salient indicator of ‘otherness’ as more states become democratic, and their empirical analysis indicates that the risk of conflict between democracies has increased as the world has become more democratic.6 Studies using tools of network analysis also indicate systemic effects of democracy. Dorussen & Ward (2010) and Lupu & Traag (2013) find support for the democratic peace while accounting for the pacifying impact of trade networks. Maoz (2006) finds that large ‘democratic cliques’ in networks dampen conflicts, but Cranmer & Desmarais (2011) conclude that the support for this claim is weak when using a more appropriate statistical method. The internal democratic peace A number of studies find empirical confirmation of an ‘inverted-U’ relationship between level of democracy and the probability of onset of internal armed conflict. Semidemocratic regimes have a higher risk of internal conflict than consistent autocracies or democracies (Boswell & Dixon, 1990; Muller & Weede, 1990; Hegre et al., 2001; Fearon & Laitin, 2003). The existence of this ‘inverted U’ has been challenged, however (Elbadawi & Sambanis, 2002; Collier & Hoeffler, 2004; Vreeland, 2008).7 In any case, very few studies find traces of a monotonic effect of democracy. When controlling for GDP per capita or other indicators of socio-economic development, democratically governed countries have no lower risk of internal armed conflict than autocratic ones.8 Buhaug (2006) finds that semi-democracies have a higher risk of wars over government than autocracies and democracies, but that democracies are more likely to experience conflicts over territory than the other two regime types. Cederman, Hug & Krebs (2010) find democratization to affect conflicts over government, but not over territory. Although democratic institutions by themselves are ineffective in reducing risk of internal conflict onset, several studies find that they affect how internal conflicts evolve. Lacina (2006) and Gleditsch, Hegre & Strand (2009) show that internal wars in democracies are less lethal. Democratic governments make use of less violence against civilians (Eck & Hultman, 2007) and engage in less repression (Davenport, 2007b; Colaresi & Carey, 2008),9 but rebel groups tend to make more extensive use of violence against civilians when fighting democratic regimes (Eck & Hultman, 2007). Possibly because of the stronger constraints on the use of violence against insurgents, democracies tend to have longer internal wars (Gleditsch, Hegre & Strand, 2009).10 Some studies, such as Mukherjee (2006), find that post-conflict democracies have a lower risk of conflict recurrence. Other studies report contrasting results (Walter, 2004; Quinn, Mason & Gurses, 2007; Collier, Hoeffler & So¨derbom, 2008).

### Democracy solves growth

#### Democracy is directly correlated with economic growth

Silva, MA International Relations, 11 [Shanila De, MA International Relations, Department of Politics & International Studies, University of Warwick, https://www.academia.edu/1139228/Facilitating\_Peace\_Democracy\_Building\_Following\_Violent\_Conflict] Schloss

Rodrick and Wacziarg show that democratization is not bad for economic performance and that, in fact, democracies have positive effects on growth. 60 They conclude that the idea that political reforms should wait until a country is ‘mature enough’ for democracy, or the idea that growth should precede democracy, is not supported by evidence. 61 The assumption that autocracies are better equipped to grow the economy presupposes that autocracies deliver better performance than democracy, which, in their analysis, is shown to be false. 62 A market system may reduce the tendency towards corruption by providing higher standards of living and alternative pathways for advancement. 63 However, in a market economy there are winners and losers, and while growth, overall, may be a stabilizing factor, inequalities can be destabilizing. 64 Wittman explains that in a democracy, it is in the interest of policy makers to create policies that result in a more equitable distribution of the gains from growth the gains from growth. 65 A more even distribution, including higher investment in human capital, enhances overall stability. 66 Democracy can maintain the high standards of living and substantial economic growth that are required for long term stability. 67 Besley and Kudamatsu show that autocracies that achieve high levels of growth are those which constrain the behaviour of their leader, meaning that it is not the case that all dictatorships benefit from growth. 68 Growth seems to be correlated with constrained leaders. 69 Liberal democracies have constraints built in, through the ability of voters to discipline politicians. 70 They also make sure that political change, in the event of inadequate leadership, is regular and stable rather than irregular and unstable. This regular-change effect has further positive impacts on growth. 71 Democracy and growth are mutually reinforcing. 72 While democracy can have a positive effect on post-conflict stability, this effect is more pronounced when a country’s income is higher. 73 Overall, “countries whose citizens enjoy high levels of economic well being and have access to a more open political system are significantly less likely to experience multiple civil wars than autocratic countries with low levels of individual welfare.” 74 An appropriately moulded democratic system, combined with effective institutions results in stable, growth oriented states. 75 Effective institutions highlight the importance of governance, which is the next condition necessary for stability and is as important as economic management. 76

### Democracy solves terrorism

#### Democracies are significantly less susceptible to terrorist attacks--- political freedom, counter terrorist measures, less incentives

Li, Political Science Professor, 15 [Quan, Department of Political Science The Pennsylvania State University, Does Democracy Promote or Reduce Transnational Terrorist Incidents?, http://jcr.sagepub.com/content/49/2/278.full.pdf+html] Schloss

One argument in the democracy-terrorism literature posits that aspects of democracy reduce terrorism. In nondemocratic societies, the lack of opportunities for political participation induces political grievances and dissatisfaction among dissenters, motivating terrorism (Crenshaw 1981, 383). In contrast, in democratic societies, free and fair elections ensure that rulers can be removed and that desirable social changes can be brought about by voters, reducing the need to resort to violence (Schmid 1992). Democratic rules enable nonviolent resolution of political conflict. Democracies permit dissenters to express their policy preferences and seek redress (Ross 1993). Different social groups are able to participate in the political process to further their interest through peaceful means, such as voting and forming political parties (Eubank and Weinberg 1994, 2001). Since democracy lowers the cost of achieving political goals through legal means, groups find costly illegal terrorist activities less attractive (Ross 1993; Eyerman 1998). Wide democratic participation also has beneficial consequences that remain largely unnoticed in the literature. To the extent that democratic participation increases political efficacy of citizens, terrorist groups will be less successful recruiting new members in democracy than in autocracy. This may reduce the number of terrorist attacks in democracy. Within the context of transnational terrorism, wide democratic participation helps to reduce incentives of domestic groups to engage in terrorist activities against foreign targets in a country. When citizens have grievances against foreign targets, greater political participation under a democratic system allows them to exert more influence on their own government so that they can seek favorable policy changes or compensation more successfully. Joining a terrorist group and attacking the foreign target become less appealing options. To the extent that democratic participation leads to public tolerance of counterterrorist efforts, a democratic government will be more effective stopping a variety of terrorist attacks, including those by domestic terrorists against foreign targets as well as those committed by foreign terrorists in the country.

## Data Localization Scenario

### Uniqueness – Localization increasing

#### Global data localization now

Donohue 15 – Professor of Law, Georgetown Law and Director, Center on National Security and the Law, Georgetown Law (Lauren, HIGH TECHNOLOGY, CONSUMER PRIVACY, AND U.S. NATIONAL SECURITY, Symposium Articles, 4 Am. U. Bus. L. Rev. 11 p.20-23, 2015, Hein Online)//JJ

C. Data Localization and Data Protection

Over the past eighteen months, countries around the world have increasingly adopted data localization laws, restricting the storage, analysis, and transfer of digital information to national borders.45 To some extent, the use of barriers to trade as a means of incubating tech-based industries predated the Snowden releases.46 In the aftermath of the leaks, the dialogue has gained momentum. The asserted purpose is to protect government data and consumer privacy. As of the time of writing, China, Greece, Malaysia, Russia, South Korea, Venezuela, Vietnam, Iran, and others have already implemented local data server requirements. Turkey has introduced new privacy regulations preventing the transfer of personal data (particularly locational data) overseas. Others, such as Argentina, India, and Indonesia are actively considering new laws, even as Brazilian president, Dilma Rousseff, has been promoting a law that would require citizens' personal data to be stored within domestic bounds. Germany and France are considering a Schengen routing system, retaining as much online data in the European Union as possible. As a regional matter, the European Union (EU) Commission's Vice President, Viviane Reding, is pushing for Europe to adopt more expansive privacy laws. In March 2014, the European Parliament passed the Data Protection Regulation and Directive, imposing strict limits on the handling of EU citizens' data. Reding announced, "The message the European Parliament is sending is unequivocal: This reform is a necessity, and now it is irreversible. Europe's directly elected parliamentarians have listened to European citizens and European businesses and, with this vote, have made clear that we need a uniform and strong European data protection law, which will... strengthen the protection of our citizens." Regardless of where the information is based, those handling the data must obtain the consent of the data subjects to having their personal information processed. They also retain the right to later withdraw consent. Those violating the directive face steep fines, including up to five percent of revenues. Apart from the new directive, the Civil Liberties, Justice, and Home Affairs Committee of the European Parliament passed a resolution calling for the end of the US/EU Safe Harbor agreement. Some 3000 U.S. companies rely on this framework to conduct business with the EU.

### Surveillance causes data localization

#### Surveillance overreach is the driving force of global data localization

Castro and McQuinn 15 – \* Vice President of the Information Technology and Innovation Foundation and Director of the Center for Data Innovation, B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University, AND \*\* Research Assistant with the Information Technology and Innovation Foundation, B.S. in Public Relations and Political Communications from the University of Texas (Daniel and Alan, Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness, Information Technology and Innovation Foundation, June 2015, http://www2.itif.org/2015-beyond-usa-freedom-act.pdf?\_ga=1.33178294.940386433.1435342104)//JJ

U.S. SURVEILLANCE POWERS ARE THE JUSTIFICATION FOR FOREIGN PROTECTIONISM The ability of companies — both tech and traditional — to easily share data across borders has brought a vast array of benefits to countries, companies, consumers, and economies through increased efficiency, decreased costs, and improved services. 26 And yet nations have continued to erect barriers to cloud computing and cross - border data flows, much to their own detriment. 27 While some defenders of these policies have asserted that they are designed to increase the privacy or security of their citizens’ data, it is clear that they are also motivated by misguided self - interest . By creating rules that advantage domestic firms over foreign firms, many countries believe they will build a stronger domestic tech industry or gain short - term economic value , such as jobs in domestic dat a centers . In reality, these policies unwittingly limit the ability of a country’s own firms to innovate by shielding them from international competition. 28 These policies not only limit the number of services that a country’s citizens and businesses can en joy, but also harm that country’s productivity and competitiveness. Some countries used U.S. surveillance laws to justify data protectionism even before Snowden’s NSA revelations. For example, when Rackspace built data centers in Australia in 2012, an Australian competitor stirred up fears that the United States would use the Patriot Act to track Australian citizens as a means to force Rackspace out of Australia. 29 In addition, this same Australian company funded a report calling on Australian policymakers to impose additional regulations designed to put foreign cloud computing competitors at a disadvantage. 30 However, since the recent NSA revelations, the use of privacy concerns to justify protectionist barriers has grown significantly. Amid growing anti - U . S . sentiment, Europe has seen calls for data localization requirements, procurement preferences for European providers, and even a “Schengen area for data” — a system that keeps as much data in Europe as possible — as ways to promote deployment of cloud services entirely focused on the European market. 31 France and Germany have even started to create dedicated national networks: “Schlandnet” for the former and the “Sovereign Cloud” for the latter. 32 The French government has gone so far as to put € 150 million ($200 million) into two start - ups, Numergy and Cloudwatt, to create a domestic infrastructure independent of U.S. tech giants. 33 Furthermore, some groups have invoked U.S. cyber espionage to argue that European citizens are n ot adequately protected and are call ing for the removal of the “safe harbor” agreement — an agreement that allows Internet companies to store data outside of the European Union . Yet if this were removed it would cut Europeans off from many major Internet services There is also an increasingly distressing trend of countries, such as Australia, China, Russia , and India, passing laws that prevent their citizens’ personal information from leaving the country’s borders — effectively mandating that cloud computing firms build data centers in those countries or risk losing access to their markets. For example, in 201 4 Russian implemented and Indonesia began considering policies that would require Internet - based companies to set up local data centers. 35 These policies are often a veiled attempt to spur short term economic activity by creating data - center jobs. However, this benefit is often outweighed by the substantial cost of building unnecessary data centers, a cost that is eventually passed along to the country’s citizens. Several U.S. tech giants, such Apple and Salesforce, have already started to build their data c enters abroad to appease foreign watchdogs and privacy advocates. 36 For example, Amazon started running Internet services and holding data in Germany for its European business partners in an effort to downplay threats of online spying.

#### That will collapse the global internet

**Chandler and Le, 15** - \* Director, California International Law Center, Professor of Law and Martin Luther King, Jr. Hall Research Scholar, University of California, Davis; A.B., Harvard College; J.D., Yale Law School AND \*\*Free Speech and Technology Fellow, California International Law Center; A.B., Yale College; J.D., University of California, Davis School of Law (Anupam and Uyen, “DATA NATIONALISM” 64 Emory L.J. 677, lexis)

The era of a global Internet may be passing. Governments across the world are putting up barriers to the free flow of information across borders. Driven by concerns over privacy, security, surveillance, and law enforcement, governments are erecting borders in cyberspace, breaking apart the World Wide Web. The first generation of Internet border controls sought to keep information out of a country - from Nazi paraphernalia to copyright infringing material. n1 The new generation of Internet border controls seeks not to keep information out but rather to keep data in. Where the first generation was relatively narrow in the information excluded, the new generation seeks to keep all data about individuals within a country. Efforts to keep data within national borders have gained traction in the wake of revelations of widespread electronic spying by United States intelligence agencies. n2 Governments across the world, indignant at the recent disclosures, have cited foreign surveillance as an argument to prevent data from leaving their borders, allegedly into foreign hands. n3 As the argument [\*680] goes, placing data in other nations jeopardizes the security and privacy of such information. We define "data localization" measures as those that specifically encumber the transfer of data across national borders. These measures take a wide variety of forms - including rules preventing information from being sent outside the country, rules requiring prior consent of the data subject before information is transmitted across national borders, rules requiring copies of information to be stored domestically, and even a tax on the export of data. We argue here that data localization will backfire and that it in fact undermines privacy and security, while still leaving data vulnerable to foreign surveillance. Even more importantly, data localization increases the ability of governments to surveil and even oppress their own populations. Imagine an Internet where data must stop at national borders, examined to see whether it is allowed to leave the country and possibly taxed when it does. While this may sound fanciful, this is precisely the impact of various measures undertaken or planned by many nations to curtail the flow of data outside their borders. Countries around the world are in the process of creating Checkpoint Charlies - not just for highly secret national security data but for ordinary data about citizens. The very nature of the World Wide Web is at stake. We will show how countries across the world have implemented or have planned dramatic steps to curtail the flow of information outside their borders. By creating national barriers to data, data localization measures break up the World Wide Web, which was designed to share information across the globe. n4 The Internet is a global network based on a protocol for interconnecting computers without regard for national borders. Information is routed across this network through decisions made autonomously and automatically at local routers, which choose paths based largely on efficiency, unaware of political borders. n5 Thus, the services built on the Internet, from email to the World [\*681] Wide Web, pay little heed to national borders. Services such as cloud computing exemplify this, making the physical locations for the storage and processing of their data largely invisible to users. Data localization would dramatically alter this fundamental architecture of the Internet. Such a change poses a mortal threat to the new kind of international trade made possible by the Internet - information services such as those supplied by Bangalore or Silicon Valley. n6 Barriers of distance or immigration restrictions had long kept such services confined within national borders. But the new services of the Electronic Silk Road often depend on processing information about the user, information that crosses borders from the user's country to the service provider's country. Data localization would thus require the information service provider to build out a physical, local infrastructure in every jurisdiction in which it operates, increasing costs and other burdens enormously for both providers and consumers and rendering many of such global services impossible. While others have observed some of the hazards of data localization, especially for American companies, n7 this Article offers three major advances over earlier work in the area. First, while the earlier analyses have referred to a data localization measure in a country in the most general of terms, our Article provides a detailed legal description of localization measures. Second, by examining a variety of key countries around the world, the study allows us to see the forms in which data localization is emerging and the justifications offered for such measures in both liberal and illiberal states. Third, the Article works to comprehensively refute the various arguments for data localization offered around the world, showing that data localization measures are in fact likely to undermine security, privacy, economic development, and innovation where adopted. [\*682] Our paper proceeds as follows. Part I describes the particular data localization measures in place or proposed in different countries around the world, as well as in the European Union. Part II then discusses the justifications commonly offered for these measures - such as avoiding foreign surveillance, enhancing security and privacy, promoting economic development, and facilitating domestic law enforcement. We appraise these arguments, concluding that, in fact, such measures are likely to backfire on all fronts. Data localization will erode privacy and security without rendering information free of foreign surveillance, while at the same time increasing the risks of domestic surveillance.

### Data localization causes war

#### Data localization will end globalization, cause war

Schwartz, 2014 Peter, co-founder of the Global Business Network, (Peter, “WARNING: The Internet Might End in December”, September 22, 2014 <http://www.huffingtonpost.com/peter_schwartz/end-of-internet_b_5856168.html//DM>)

**THE GEO-DIGITAL WORLD ORDER**

Among the most important battlefields is the one for control of the world's information networks, especially the Internet. The Internet was designed to facilitate the easy movement of information, and it has succeeded brilliantly. For anyone with access to it, the Internet makes available a vast amount of the world's knowledge. Money flashes all over the world in a globally integrated marketplace. The Internet has eliminated friction from almost every market and transaction. The rapidly growing concerns about privacy, government spying and hacking, have set in motion a cascade that may be unstoppable, having created an alliance of both our friends and challengers. The next battle will be fought in Busan, Korea in a few weeks at the meeting of the International Telecommunications Union, a body chartered to technically regulate the interconnection standards of telephone and telegraph networks and assign parking spots in Earth orbit for communications satellites. At that meeting the challenger countries will once again, as they tried to do last December in Dubai, try to wrest control from the multi-stakeholder coalition that has been governing the Internet under a contract with the U.S. government. **THE END OF THE WORLD AS WE KNOW IT** If they succeed, it very well may lead to the end of the world as we know it. There will be no Internet. There will be many nets: ChinaNet, Euronet, maybe Deutsche Net and France net and Brazil Net and Russia Net. It will resemble the world before the Internet with many private networks and a constant challenge of interconnection. I remember carrying around all the devices I needed to use to connect to the early Internet because of a variety of technical standards. The Internet was created to take the friction out of digital communications, whether those borders were university boundaries or national borders. The digital borders will begin to rise and with it the cost of doing everything will begin to grow. The nations of the world will once again begin to diverge. Economies of scale will disappear. **A HIGH FRICTION FUTURE** As we disconnect, nationalism is likely to grow. We will be in a high friction world with the opportunities for conflict growing fast. It is a recipe for poverty and war. Just as Smoot-Hawley was a staggeringly self-destructive act that made the Great Depression much worse, so the fragmentation of the Internet driven by the desire for national control will accelerate the end of the second era of globalization

### Data localization kills global economy

#### NSA surveillance leaks are spurring data localization measures—that undermines the global economy

**Kornbluh 14** - senior fellow for digital policy at the Council on Foreign Relations (Karen, “Beyond Borders: Fighting Data Protectionism”, Democracy, Fall 2014, [http://www.democracyjournal.org/pdf/34/beyond\_borders\_fighting\_data\_protectionism.pdf)//DBI](http://www.democracyjournal.org/pdf/34/beyond_borders_fighting_data_protectionism.pdf%29//DBI)

Preserving the ability of information to flow through the pipes of the Internet should be a major U.S. foreign and international economic policy priority. According to the National Foreign Trade Council, a business organization, "goods, services, and content flowing through the Internet" were responsible for 15 percent of U.S. GDP growth from 2007 to 2012. Products and services that rely on cross-border data flows were expected to add an estimated $1 trillion in value to the U.S. economy annually over the next ten years. Globally, the Organization for Economic Cooperation and Development (OECD) calls the Internet a technological enabler likely to generate more growth than electricity, the internal combustion engine, the steam engine, or railways-and an astonishing 60 percent of the planet has yet to come online. And, as we've been reminded these last few years, the Internet's power to generate innovation and growth is rivaled only by its potential to help people realize their rights and democratic aspirations. All this was put in serious jeopardy by Snowden's revelations of National Security Agency (NSA) surveillance. Countries already harboring mercantilist fears that U.S. Internet companies are undermining their commerce and culture are now more openly considering protectionist measures. The effect of these various government incursions could be to clog the pipes of the Internet, or even to create, as Google's law enforcement and information security director has warned, a "splinter net." U.S. entrepreneurs and Silicon Valley giants alike would have a hard time reaching customers, and those seeking information, expression, and association in repressive societies would have fewer options to do so safely. The United States has championed the open, rules-based trading system since World War II. But as a number of governments have attempted to control the flow of digital goods, services, and information into and out of their countries, U.S. efforts have been hamstrung-first by the lack of successful foreign Internet companies, then by the lack of foreign participation in global Internet governance mechanisms, and finally by the surveillance revelations. In addition, a disconnect between U.S. Internet "geek" policy-makers (at the Federal Communications Commission, the White House Office of Science and Technology Policy, the Commerce Department's National Telecommunications and Information Administration, and the State Department's Internet and telecommunications units) and national security and economic policy "wonks" (at the National Security Council, National Economic Council, Treasury, and the Office of the U.S. Trade Representative) has kept the issue at the margins of policy-making.

#### Economic decline causes great power instability

**Green and Schrage 09** - Senior Advisor and Japan Chair at the Center for Strategic and International Studies (CSIS) and Associate Professor at Georgetown University, CSIS Scholl Chair in International Business and a former senior official with the US Trade Representative's Office, State Department and Ways & Means Committee (Michael and Steven, “It's not just the economy”, Asia Times Online, 03/26/09, http://www.atimes.com/atimes/Asian\_Economy/KC26Dk01.html)

Facing the worst economic crisis since the Great Depression, analysts at the World Bank and the US Central Intelligence Agency are just beginning to contemplate the ramifications for international stability if there is not a recovery in the next year. For the most part, the focus has been on fragile states such as some in Eastern Europe. However, the Great Depression taught us that a downward global economic spiral can even have jarring impacts on great powers. It is no mere coincidence that the last great global economic downturn was followed by the most destructive war in human history. In the 1930s, economic desperation helped fuel autocratic regimes and protectionism in a downward economic-security death spiral that engulfed the world in conflict. This spiral was aided by the preoccupation of the United States and other leading nations with economic troubles at home and insufficient attention to working with other powers to maintain stability abroad. Today's challenges are different, yet 1933's London Economic Conference, which failed to stop the drift toward deeper depression and world war, should be a cautionary tale for leaders heading to next month's London Group of 20 (G-20) meeting. There is no question the US must urgently act to address banking issues and to restart its economy. But the lessons of the past suggest that we will also have to keep an eye on those fragile threads in the international system that could begin to unravel if the financial crisis is not reversed early in the Barack Obama administration and realize that economics and security are intertwined in most of the critical challenges we face. A disillusioned rising power? Four areas in Asia merit particular attention, although so far the current financial crisis has not changed Asia's fundamental strategic picture. China is not replacing the US as regional hegemon, since the leadership in Beijing is too nervous about the political implications of the financial crisis at home to actually play a leading role in solving it internationally. Predictions that the US will be brought to its knees because China is the leading holder of US debt often miss key points. China's currency controls and full employment/export-oriented growth strategy give Beijing few choices other than buying US Treasury bills or harming its own economy. Rather than creating new rules or institutions in international finance, or reorienting the Chinese economy to generate greater long-term consumer demand at home, Chinese leaders are desperately clinging to the status quo (though Beijing deserves credit for short-term efforts to stimulate economic growth). The greater danger with China is not an eclipsing of US leadership, but instead the kind of shift in strategic orientation that happened to Japan after the Great Depression. Japan was arguably not a revisionist power before 1932 and sought instead to converge with the global economy through open trade and adoption of the gold standard. The worldwide depression and protectionism of the 1930s devastated the newly exposed Japanese economy and contributed directly to militaristic and autarkic policies in Asia as the Japanese people reacted against what counted for globalization at the time. China today is similarly converging with the global economy, and many experts believe China needs at least 8% annual growth to sustain social stability. Realistic growth predictions for 2009 are closer to 5%. Veteran China hands were watching closely when millions of migrant workers returned to work after the Lunar New Year holiday last month to find factories closed and jobs gone. There were pockets of protests, but nationwide unrest seems unlikely this year, and Chinese leaders are working around the clock to ensure that it does not happen next year either. However, the economic slowdown has only just begun and nobody is certain how it will impact the social contract in China between the ruling communist party and the 1.3 billion Chinese who have come to see President Hu Jintao's call for "harmonious society" as inextricably linked to his promise of "peaceful development". If the Japanese example is any precedent, a sustained economic slowdown has the potential to open a dangerous path from economic nationalism to strategic revisionism in China too. Dangerous states It is noteworthy that North Korea, Myanmar and Iran have all intensified their defiance in the wake of the financial crisis, which has distracted the world's leading nations, limited their moral authority and sown potential discord. With Beijing worried about the potential impact of North Korean belligerence or instability on Chinese internal stability, and leaders in Japan and South Korea under siege in parliament because of the collapse of their stock markets, leaders in the North Korean capital of Pyongyang have grown increasingly boisterous about their country's claims to great power status as a nuclear weapons state. The junta in Myanmar has chosen this moment to arrest hundreds of political dissidents and thumb its nose at fellow members of the 10-country Association of Southeast Asian Nations. Iran continues its nuclear program while exploiting differences between the US, UK and France (or the P-3 group) and China and Russia - differences that could become more pronounced if economic friction with Beijing or Russia crowds out cooperation or if Western European governments grow nervous about sanctions as a tool of policy. It is possible that the economic downturn will make these dangerous states more pliable because of falling fuel prices (Iran) and greater need for foreign aid (North Korea and Myanmar), but that may depend on the extent that authoritarian leaders care about the well-being of their people or face internal political pressures linked to the economy. So far, there is little evidence to suggest either and much evidence to suggest these dangerous states see an opportunity to advance their asymmetrical advantages against the international system.

###

# Tech Leadership Extensions

### Surveillance kills competitiveness

#### The perception of NSA overreaching wrecks global trust in the US tech sector – that wrecks the US economy and competitiveness

**Kehl, 14** – Policy Analyst at New America’s Open Technology Institute (Danielle, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

“It is becoming clear that the post-9/11 surveillance apparatus may be at cross-purposes with our high-tech economic growth,” declared Third Way’s Mieke Eoyang and Gabriel Horowitz in December 2013. “The economic consequences [of the recent revelations] could be staggering.”25 A TIME magazine headline projected that “NSA Spying Could Cost U.S. Tech Giants Billions,” predicting losses based on the increased scrutiny that economic titans like Google, Microsoft, Facebook, and Yahoo have faced both at home and abroad since last June.26 The NSA’s actions pose a serious threat to the current value and future stability of the information technology industry, which has been a key driver of economic growth and productivity in the United States in the past decade.27 In this section, we examine how emerging evidence about the NSA’s extensive surveillance apparatus has already hurt and will likely continue to hurt the American tech sector in a number of ways, from dwindling U.S. market share in industries like cloud computing and webhosting to dropping tech sales overseas. The impact of individual users turning away from American companies in favor of foreign alternatives is a concern. However, the major losses will likely result from diminishing confidence in U.S. companies as trustworthy choices for foreign government procurement of products and services and changing behavior in the business-to-business market. Costs to the U.S. Cloud Computing Industry and Related Business Trust in American businesses has taken a significant hit since the initial reports on the PRISM program suggested that the NSA was directly tapping into the servers of nine U.S. companies to obtain customer data for national security investigations.28 The Washington Post’s original story on the program provoked an uproar in the media and prompted the CEOs of several major companies to deny knowledge of or participation in the program.29 The exact nature of the requests made through the PRISM program was later clarified,30 but the public attention on the relationship between American companies and the NSA still created a significant trust gap, especially in industries where users entrust companies to store sensitive personal and commercial data. “Last year’s national security leaks have also had a commercial and financial impact on American technology companies that have provided these records,” noted Representative Bob Goodlatte, a prominent Republican leader and Chairman of the House Judiciary Committee, in May 2014. “They have experienced backlash from both American and foreign consumers and have had their competitive standing in the global marketplace damaged.”31 Given heightened concerns about the NSA’s ability to access data stored by U.S. companies, it is no surprise that American companies offering cloud computing and webhosting services are among those experiencing the most acute economic fallout from NSA surveillance. Within just a few weeks of the first disclosures, reports began to emerge that American cloud computing companies like Dropbox and Amazon Web Services were starting to lose business to overseas competitors.32 The CEO of Artmotion, one of Switzerland’s largest offshore hosting providers, reported in July 2013 that his company had seen a 45 percent jump in revenue since the first leaks,33 an early sign that the country’s perceived neutrality and strong data and privacy protections34 could potentially be turned into a serious competitive advantage.35 Foreign companies are clearly poised to benefit from growing fears about the security ramifications of keeping data in the United States. In a survey of 300 British and Canadian businesses released by PEER 1 in January 2014,36 25 percent of respondents indicated that they were moving data outside of the U.S. as a result of the NSA revelations. An overwhelming number of the companies surveyed indicated that security and data privacy were their top concerns, with 81 percent stating that they “want to know exactly where their data is being hosted.” Seventy percent were even willing to sacrifice performance in order to ensure that their data was protected.37 It appears that little consideration was given over the past decade to the potential economic repercussions if the NSA’s secret programs were revealed.38 This failure was acutely demonstrated by the Obama Administration’s initial focus on reassuring the public that its programs primarily affect non-Americans, even though non-Americans are also heavy users of American companies’ products. Facebook CEO Mark Zuckerberg put a fine point on the issue, saying that the government “blew it” in its response to the scandal. He noted sarcastically: “The government response was, ‘Oh don’t worry, we’re not spying on any Americans.’ Oh, wonderful: that’s really helpful to companies [like Facebook] trying to serve people around the world, and that’s really going to inspire confidence in American internet companies.”39 As Zuckerberg’s comments reflect, certain parts of the American technology industry are particularly vulnerable to international backlash since growth is heavily dependent on foreign markets. For example, the U.S. cloud computing industry has grown from an estimated $46 billion in 2008 to $150 billion in 2014, with nearly 50 percent of worldwide cloud-computing revenues coming from the U.S.40 R Street Institute’s January 2014 policy study concluded that in the next few years, new products and services that rely on cloud computing will become increasingly pervasive. “Cloud computing is also the root of development for the emerging generation of Web-based applications—home security, outpatient care, mobile payment, distance learning, efficient energy use and driverless cars,” writes R Street’s Steven Titch in the study. “And it is a research area where the United States is an undisputed leader.”41 This trajectory may be dramatically altered, however, as a consequence of the NSA’s surveillance programs. Economic forecasts after the Snowden leaks have predicted significant, ongoing losses for the cloud-computing industry in the next few years. An August 2013 study by the Information Technology and Innovation Foundation (ITIF) estimated that revelations about the NSA’s PRISM program could cost the American cloud computing industry $22 to $35 billion over the next three years.42 On the low end, the ITIF projection suggests that U.S. cloud computing providers would lose 10 percent of the foreign market share to European or Asian competitors, totaling in about $21.5 billion in losses; on the high-end, the $35 billion figure represents about 20 percent of the companies’ foreign market share. Because the cloud computing industry is undergoing rapid growth right now—a 2012 Gartner study predicted global spending on cloud computing would increase by 100 percent from 2012 to 2016, compared to a 3 percent overall growth rate in the tech industry as a whole43—vendors in this sector are particularly vulnerable to shifts in the market. Failing to recruit new customers or losing a competitive advantage due to exploitation by rival companies in other countries can quickly lead to a dwindling market share. The ITIF study further notes that “the percentage lost to foreign competitors could go higher if foreign governments enact protectionist trade barriers that effectively cut out U.S. providers,” citing early calls from German data protection authorities to suspend the U.S.-EU Safe Harbor program (which will be discussed at length in the next section).44 As the R Street Policy Study highlights, “Ironically, the NSA turned the competitive edge U.S. companies have in cloud computing into a liability, especially in Europe.”45 In a follow up to the ITIF study, Forrester Research analyst James Staten argued that the think tank’s estimates were low, suggesting that the actual figure could be as high as $180 billion over three years.46 Staten highlighted two additional impacts not considered in the ITIF study. The first is that U.S. customers—not just foreign companies—would also avoid US cloud providers, especially for international and overseas business. The ITIF study predicted that American companies would retain their domestic market share, but Staten argued that the economic blowback from the revelations would be felt at home, too. “You don’t have to be a French company, for example, to be worried about the US government snooping in the data about your French clients,” he wrote.47 Moreover, the analysis highlighted a second and “far more costly” impact: that foreign cloud providers, too, would lose as much as 20 percent of overseas and domestic business because of similar spying programs conducted by other governments. Indeed, the NSA disclosures “have prompted a fundamental re-examination of the role of intelligence services in conducting coordinated cross-border surveillance,” according to a November 2013 report by Privacy International on the “Five Eyes” intelligence partnership between the United States, the United Kingdom, Canada, Australia, and New Zealand.48 Staten predicts that as the surveillance landscape around the world becomes more clear, it could have a serious negative impact on all hosting and outsourcing services, resulting in a 25 percent decline in the overall IT services market, or about $180 billion in losses.49 Recent reports suggest that things are, in fact, moving in the direction that analysts like Castro and Staten suggested.50 A survey of 1,000 “[Information and Communications Technology (ICT)] decision-makers” from France, Germany, Hong Kong, the UK, and the USA in February and March 2014 found that the disclosures “have had a direct impact on how companies around the world think about ICT and cloud computing in particular.”51 According to the data from NTT Communications, 88 percent of decision-makers are changing their purchasing behavior when it comes to the cloud, with the vast majority indicating that the location of the data is very important. The results do not bode well for recruitment of new customers, either—62 percent of those currently not storing data in the cloud indicated that the revelations have since prevented them from moving their ICT systems there. And finally, 82 percent suggested that they agree with proposals made by German Chancellor Angela Merkel in February 2014 to have separate data networks for Europe, which will be discussed in further detail in Part III of this report. Providing direct evidence of this trend, Servint, a Virginia-based webhosting company, reported in June 2014 that international clients have declined by as much as half, dropping from approximately 60 percent of its business to 30 percent since the leaks began.52 With faith in U.S. companies on the decline, foreign companies are stepping in to take advantage of shifting public perceptions. As Georg Mascolo and Ben Scott predicted in a joint paper published by the Wilson Center and the New America Foundation in October 2013, “Major commercial actors on both continents are preparing offensive and defensive strategies to battle in the market for a competitive advantage drawn from Snowden’s revelations.”53 For example, Runbox, a small Norwegian company that offers secure email service, reported a 34 percent jump in customers since June 2013.54 Runbox markets itself as a safer email and webhosting provider for both individual and commercial customers, promising that it “will never disclose any user data unauthorized, track your usage, or display any advertisements.”55 Since the NSA revelations, the company has touted its privacy-centric design and the fact that its servers are located in Norway as a competitive advantage. “Being firmly located in Norway, the Runbox email service is governed by strict privacy regulations and is a safe alternative to American email services as well as cloud-based services that move data across borders and jurisdictions,” company representatives wrote on its blog in early 2014.56 F-Secure, a Finnish cloud storage company, similarly emphasizes the fact that “its roots [are] in Finland, where privacy is a fiercely guarded value.”57 Presenting products and services as ‘NSA-proof’ or ‘safer’ alternatives to American-made goods is an increasingly viable strategy for foreign companies hoping to chip away at U.S. tech competiveness.58

#### **U.S. surveillance programs are crushing U.S. tech industry competitiveness – collapse the economy and inflames foreign protectionism – surveillance reforms key to solve**

Castro and McQuinn 15 – \* Vice President of the Information Technology and Innovation Foundation and Director of the Center for Data Innovation, B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University, AND \*\* Research Assistant with the Information Technology and Innovation Foundation, B.S. in Public Relations and Political Communications from the University of Texas (Daniel and Alan, Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness, Information Technology and Innovation Foundation, June 2015, <http://www2.itif.org/2015-beyond-usa-freedom-act.pdf?_ga=1.33178294.940386433.1435342104)//JJ>

Almost two years ago, ITIF described how revelations about pervasive digital surveillance by the U.S. intelligence community could severely harm the competitiveness of the United States if foreign customers turned away from U.S. - made technology and services. 1 Since then, U.S. policymakers have failed to take sufficient action to address these surveillance concerns ; in some cases, they have even fanned the flames of discontent by championing weak information security practices . 2 In addition, other countries have used anger over U .S. government surveillance as a cover for implementing a new wave of protectionist policies specifically targeting information technology . The combined result is a set of policies both at home and abroad that sacrifices robust competitiveness of the U.S. tech sector for vague and unconvincing promises of improved national security. The failure of U.S. policymakers to address surveillance concerns over the last few years has buoyed foreign protectionism and hurt American businesses ITIF estimated in 2013 that even a modest drop in the expected foreign market share for cloud computing stemming from concerns about U.S. surveillance could cost the United States between $21.5 billion and $35 billion by 2016. 3 Since then , it has become clear that the U.S. tech industry as a whole, not just the cloud computing sector , has under - performed as a result of t he Snowden revelations . Therefore, the economic impact of U.S. surveillance practices will likely far exceed ITIF’s initial $35 billion estimate. This report catalogues a wide range of specific examples of the economic harm that has been done to U.S. busin esses . In short, foreign customers are shunning U.S. companies . The policy implication of this is clear: Now that Congress has reformed how the National Security Agency ( NSA ) collects bulk domestic phone records and allowed private firms — rather than the government — to collect and store approved data, it is time to address other controversial digital surveillance activities by the U.S. intelligence community. The U.S. government’s failure to reform many of the NSA’s surveillance programs has damaged the competitiveness of the U.S. tech sector and cost it a portion of the global market share . 5 This includes programs such as PRISM — the controversial program authorized by the FISA Amendments Act , which allows for warrantless access to private - use r data on popular online services both in the United States and abroad — and Bullrun — the NSA’s program to undermine encryption standards both at home and abroad . Foreign companies have seized on these controversial policies to convince their customers that keeping data at home is safer than sending it abroad, and foreign governments have pointed to U.S. surveillance as justification for protectionist policies that require data to be kept within their national borders . In the most extreme cases, such as in China, foreign governments are using fear of digital surveillance to force companies to surrender valuable intellectual property, such as source code. In the short term, U.S. companies lose out on contracts, and over the long term, other countries create protectionist policies that lock U.S. businesses out of foreign markets. This not only hurt s U.S. technology companies , but costs American jobs and weakens the U.S. trade balance. To reverse this trend, ITIF recommend s that policymakers:  Increase transparency about U.S. surveillance activities both at home and abroad.  S trengthen information security by opposing any government efforts to introduce backdoors in software or weaken encryption.  Strengthen U.S. mutual legal assistance treaties (MLATs) .  Work to establish international legal standards for government access to data.  Complete trade agreements like the Trans Pacific Partnership that ban digital protectionism, and pressure nations that seek to erect protectionist barriers to abandon those efforts .

### Perception key

#### The widespread perception that the NSA is acting beyond the established legislative framework is destroying the reputation of U.S. tech companies

**Eoyang and Bishai, 15** - \*Mieke Eoyang is the Director of the National Security Program at Third Way, a center-left think tank. She previously served as Defense Policy Advisor to Senator Edward M. Kennedy, and a subcommittee staff director on the House Permanent Select Committee on Intelligence, as well as as Chief of Staff to Rep. Anna Eshoo (D-Palo Alto); \*\*Chrissy Bishai is a Fellow at Third Way (“Restoring Trust between U.S. Companies and Their Government on Surveillance Issues” 3/19, <http://www.thirdway.org/report/restoring-trust-between-us-companies-and-their-government-on-surveillance-issues>

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

### Tech leadership key to hegemony

#### \*Tech leadership underpins hegemony

Weiss 14 – Fellow of the Academy of the Social Sciences in Australia, Professor Emeritus in Government and International Relations at the University of Sydney, Honorary Professor of Political Science at Aarhus University. (Linda, America Inc.?: Innovation and Enterprise in the National Security State, Cornell University Press, 4/1/14, p. 1-3)//JJ

Bill Gates's "state-less" depiction of America's high-tech economy perfectly captures the prevailing understanding of U.S. techno-industrial preeminence. Both at home and abroad, the United States is widely portrayed as the quintessential free-market economy. In this reputedly freewheeling entrepreneurial setting, robust antistatism combines with weak State capacity to ensure that the U.S. government contributes little more to America's global technology leadership than a business-friendly environment. This book tells a different story, one that links high technology with national security and (antistatist) political norms. 1 It proposes that there is more to American capitalism and the American state than meets the free-market eye. In getting to this "something more," we start from the substantive observation that the U S. has an unmatched capacity for transformative innovation. For half a century and more, the United States has been the uncontested high-technology hegemon, leading the world in virtually all the major technologies that drive the modern economy and underpin its prosperity. Think of innovations such as communications satellites, micro- electronics, computers, software, biotechnology, the internet—the list goes on. More striking still is that every one of these breakthrough innovations emanated from the United States precisely in the period since World War Il, giving rise to entirely new industries. My main argument focuses on the role of what I call the national security state or NSS (though I use the term in an unusual sense; more on this shortly). Since World War Il, the NSS has dominated in high-risk, break- through technologies and emerging industries; this pursuit has established, and continues to secure, the foundations for a high-technology commercial sector. Nevertheless, the NSS pursues technology leadership in order to sustain U.S. military-political primacy, not to achieve commercial advantage. To do so it has to rely on the private sector to advance its technology goals. After all, the days when the military could source all it needed from its arsenals are long gone. But as leading-edge capabilities came to reside less and less within the pool of large defense contractors (core of what is traditionally described as the military-industrial complex), and more and more within high-tech firms reluctant to work on security related projects, the NSS was compelled to retool its incentive system. As I explain in more detail below, increasingly since the 1980s the NSS has had to reach outside the traditional pool of large Contractors to attract the most innovative companies, by building commercial goals into its programs. By placing greater emphasis on commercializalion opportunities, some of these incentives seek to sweeten collaboration with the Department of Defense (DoD) and other security-related agencies, and thus to increase NSS influence over the direction of technology. In this manner, commercialization becomes the sine qua non of technological- cum-military primacy. Far from being mutually exclusive, security and com- merce have become closely entwined in NSS policy and practice. At one level then, this is a story about how the geopolitics of threat perception has generated a vast state machinery geared to perpetual innovation in the quest for technological superiority. At another level, it is a story about the domestic challenges and political obstacles that have reshaped the NSS and its relationship with the private sector, not only by integrating the goals of security with those of commerce but also by merging public and private resources in distinctive ways.

### Soft power

#### Surveillance overreach spills over to gut overall US global legitimacy

**Kehl, 14** – Policy Analyst at New America’s Open Technology Institute (Danielle, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

Broader Foreign Policy Costs

Beyond Internet Freedom, the NSA disclosures “have badly undermined U.S. credibility with many of its allies,” Ian Bremmer argued in Foreign Policy in November 2013.214 Similarly, as Georg Mascolo and Ben Scott point out about the post-Snowden world, “the shift from an open secret to a published secret is a game changer… it exposes the gap between what governments will tolerate from one another under cover of darkness and what publics will tolerate from other governments in the light of day.”215 From stifled negotiations with close allies like France and Germany to more tense relations with emerging powers including Brazil and China, the leaks have undoubtedly weakened the American position in international relations, opening up the United States to new criticism and political maneuvering that would have been far less likely a year ago.216

U.S. allies like France, Israel, and Germany are upset by the NSA’s actions, as their reactions to the disclosures make clear.217 Early reports about close allies threatening to walk out of negotiations with the United States—such as calls by the French government to delay EU-U.S. trade talks in July 2013 until the U.S. government answered European questions about the spying allegations218—appear to be exaggerated, but there has certainly been fallout from the disclosures. For months after the first Snowden leaks, German Chancellor Angela Merkel would not visit the United States until the two countries signed a “no-spy” agreement—a document essentially requiring the NSA to respect German law and rights of German citizens in its activities. When Merkel finally agreed come to Washington, D.C. in May 2014, tensions rose quickly because the two countries were unable to reach an agreement on intelligence sharing, despite the outrage provoked by news that the NSA had monitored Merkel’s own communications.219 Even as Obama and Merkel attempted to present a unified front while they threatened additional sanctions against Russia over the crisis in the Ukraine, it was evident that relations are still strained between the two countries. While President Obama tried to keep up the appearance of cordial relations at a joint press conference, Merkel suggested that it was too soon to return to “business as usual” when tensions still remain over U.S. spying allegations.220 The Guardian called the visit “frosty” and “awkward.”221 The German Parliament has also begun hearings to investigate the revelations and suggested that it is weighing further action against the United States.222

Moreover, the disclosures have weakened the United States’ relationship with emerging powers like Brazil, where the fallout from NSA surveillance threatens to do more lasting damage. Brazilian President Dilma Rousseff has seized on the NSA disclosures as an opportunity to broaden Brazil’s influence not only in the Internet governance field, but also on a broader range of geopolitical issues. Her decision not to attend an October 2013 meeting with President Barack Obama at the White House was a direct response to NSA spying—and a serious, high-profile snub. In addition to cancelling what would have been the first state visit by a Brazilian president to the White House in nearly 20 years, Rousseff’s decision marked the first time a world leader had turned down a state dinner with the President of the United States.223 In his statement on the postponement, President Obama was forced to address the issue of NSA surveillance directly, acknowledging “that he understands and regrets the concerns disclosures of alleged U.S. intelligence activities have generated in Brazil and made clear that he is committed to working together with President Rousseff and her government in diplomatic channels to move beyond this issue as a source of tension in our bilateral relationship.”224

Many observers have noted that the Internet Freedom agenda could be one of the first casualties of the NSA disclosures. The U.S. government is fighting an uphill battle at the moment to regain credibility in international Internet governance debates and to defend its moral high ground as a critic of authoritarian regimes that limit freedom of expression and violate human rights online. Moreover, the fallout from the NSA’s surveillance activities has spilled over into other areas of U.S. foreign policy and currently threatens bilateral relations with a number of key allies. Going forward, it is critical that decisions about U.S. spying are made in consideration of a broader set of interests so that they do not impede—or, in some cases, completely undermine—U.S. foreign policy goals.

#### Legitimacy is key to international leadership – solves all global problems

**Stanley, 7 (**Elizabeth Stanley, Ass Prof @ Georgetown, 7 “International Perceptions of US Nuclear Policy” Sandia Report, http://www.prod.sandia.gov/cgi-bin/techlib/access-control.pl/2007/070903.pdf)

How important is soft power, anyway? Given its vast conventional military power, does the United States even need soft power? Some analysts argue that US military predominance is both possible and desirable over the long term, and thus soft power is not important. But a growing consensus disagrees. These analysts argue that soft power is critical for four reasons. First, soft power is invaluable for keeping potential adversaries from gaining international support, for “winning the peace” in Afghanistan and Iraq, and for convincing moderates to refrain from supporting extremist terrorist groups. Second, soft power helps influence neutral and developing states to support US global leadership. Third, soft power is also important for convincing allies and partners to share the international security burden.14 Finally, and perhaps most importantly, given the increasing interdependence and globalization of the world system, soft power is critical for addressing most security threats the United States faces today. Most global security threats are impossible to be countered by a single state alone. Terrorism, weapons of mass destruction (WMD) proliferation, failed and failing states, conflicts over access to resources, are not confined to any one state. In addition, disease, demographic shifts, environmental degradation and global warming will have negative security implications as well.15 All of these potential threats share four traits: (1) they are best addressed proactively, rather than after they develop into full-blown crises; (2) they require multi-lateral approaches, often under the umbrella of an international institution; (3) they are not candidates for a quick fix, but rather require multi-year, or multi-decade solutions; and, (4) they are “wicked” problems. Given these four traits, soft power is critical for helping to secure the international, multi-lateral cooperation that will be necessary to address such threats effectively.

### Hegemony impact – China

#### Maintaining US hegemony is key to counter China rise – causes the world to descend into great power politics which breed conflict

**Roloff 14** – Writer of a thesis submitted to Johns Hopkins University in conformity with the requirements for∂ the degree of Master of Arts in Global Security Studies. (Luke, “PATTERNS OF INSTABILITY: THE CAUSES AND CONSEQUENCES OF STRUCTURAL INSECURITY AND POWER POLITICS IN THE ASIA-PACIFIC SPHERE”, May 2014, <https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/37219/ROLOFF-THESIS-2014.pdf?sequence=1//DM>)

Since the end of the Cold War, the international environment has been a∂ historical anomaly in which the traditional strategies and motivations for interstate∂ rivalries and zero-sum power politics were subdued. As the United States emerged as the∂ world’s sole superpower and hegemon, so too did the current unipolar system. The era of∂ Pax Americana, coupled with the proclaimed victories of democracy and liberal market,∂ ushered out a 20th century marred by interstate wars and welcomed a new millennium∂ heralded as an era of cooperation and collective prosperity. It soon became a common∂ refrain that peace in the post-Cold War era would be founded upon multinational∂ organizations, international norms, and the linkages of a globalized economy. This was a∂ drastic and marked departure from the great power politics of alliance blocs, deterrence∂ and arms races that had dominated mainstream strategic rationale during the Cold War∂ and most of history. Under the new Pax Americana, these concepts of international∂ power contests were deemed obsolete and understandably became dormant in a time∂ when the most imminent threats ranged from terrorism and pandemics to rouge states and∂ rising tides. However, the supposed passing of great power politics was prematurely∂ based upon a benign power distribution and not a fundamental change in the structure of∂ the global order. The cyclical calculus of power politics is rapidly resurfacing in an∂ increasingly multipolar Asia-Pacific Sphere due to the rise of China, the forthcoming∂ response of the United States, and the insecurity of regional actors.1 Future stability of∂ the Asia-Pacific is contingent upon how the relationship between the U.S. and China will∂ evolve in a new multipolar environment. History cautions that rising powers and the∂ status quo rarely enjoy a frictionless relationship, but why does this occur? What are the∂ unstable dynamics of the international system that plague great power politics with such∂ frequency that some even term it the ‘tragedy’ of great powers? The answer to both∂ questions resides in the very structure of the international order and the instability∂ inherent therein. The goal of this thesis is to identify the systemic causes for structural instability,∂ which are again emerging to drive a new regional power rivalry between the U.S. and∂ China and transform the Asia-Pacific into a region governed by power rivalries and∂ brinkmanship. There are no new explanations or theories offered here. Instead, what is∂ unique is the revival of previously discarded explanations of world politics to address the∂ remerging symptoms of great power conflicts. The strategic value of a state’s relative∂ power in comparison to potential rivals may resemble Bismarkian Europe, but the∂ following chapters will show that this thinking has a very real and immediate place in∂ modern strategic planning. It may seem that this historically grounded analysis is too∂ abstract or notional and cannot offer much strategic guidance in the current Asia-Pacific.∂ However, by identifying the root causes of power rivalries and incorporating structural∂ influences into operational doctrine, modern strategies can benefit by accurately∂ deciphering an adversary’s geopolitical decision and predict the outcome based upon∂ historical precedence. An understanding of great power politics and history allows for∂ preemptive actions rather than a reactive posture, which only invites further∂ misunderstandings and escalation. An analytical framework that asks why China is∂ pursuing a seemingly destabilizing posture or assesses the impact of the U.S.’s own∂ rebalancing actions can prevent the region from continuing to slide towards a more ∂ 4∂ hostile, militarized and volatile future. Nowhere is the need for accurate information and∂ sound engagements more critical than in the evolving geopolitical postures between the∂ reigning U.S. and an emerging China. This outlook hypothesizes that if current strategies fail to account for the∂ underlying structural influences driving geopolitical struggles, future Sino-U.S.∂ exchanges will succumb to the same historical cycle of conflict based upon mutual∂ apprehension, distrust and spiraling insecurity. The specter of China as a prospective∂ regional challenger against American power rekindles the possibility that great power∂ rivalries will soon preoccupy both sides’ interactions and jeopardize the stability of the∂ region. This trajectory is incumbent upon China’s expanding military prowess and∂ economic clout, which threatens to upset the current regional status quo underwritten by∂ American preponderance in the region. China’s growing capabilities suggest that the∂ region will be soon become a tense bipolar or even more treacherous and unbalanced∂ multipolar structure. The prospect of competing powers and a structural shift away from a clear∂ hegemonic power will drive the calculated cycle of power politics, which manifests itself∂ in the international arena as security dilemmas, entangling alliances and militarization.∂ However, China’s military growth is not the result of tyrannical or irrational opponents.∂ This instability is the consequence of the present international structure. The global∂ commons is still an anarchic environment where each nation must ensure its own∂ survival. Consequently, state strategies are driven by an intrinsic insecurity stemming∂ from misperceptions of other state’s intentions and relative military capabilities. China’s∂ rise is an ongoing issue, but the underlying tensions are symptomatic of enduring ∂ 5∂ geopolitical sensitivities that have long fueled national fears, thwarted peace, and bred∂ conflict. To demonstrate how structural instability within the global system subsists in∂ emerging strategies and force postures, the following chapters will present three∂ overarching ‘hazards’ that are commonly associated with great power politics and∂ regional instability: security dilemmas, balance of power dynamics and an overreliance∂ upon economic interdependence. Each chapter will identify how the hazard can∂ negatively influence state strategies and each chapter follows a similar pattern of∂ analysis. First, a brief, but comprehensive, literature review explains the definition of∂ each hazard, traces the theoretic lineage and outlines the current scholarship. Second, a∂ historical case study with similar characteristics to today’s operating environment will∂ demonstrate how each of these elements contributed to and intensified past power∂ rivalries. Third, the lessons from the case study will be juxtaposed against current∂ strategies or regional posturing in the modern Pacific to demonstrate how these structural∂ hazards are increasingly weighing upon today’s strategic calculus.

#### A US-China confrontation will escalate

**Roloff 14** – Writer of a thesis submitted to Johns Hopkins University in conformity with the requirements for∂ the degree of Master of Arts in Global Security Studies. (Luke, “PATTERNS OF INSTABILITY: THE CAUSES AND CONSEQUENCES OF STRUCTURAL INSECURITY AND POWER POLITICS IN THE ASIA-PACIFIC SPHERE”, May 2014, https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/37219/ROLOFF-THESIS-2014.pdf?sequence=1//DM)

The existence and possible consequences of a Sino-American security dilemma∂ will be discussed in the context of both China and the United States’ nascent operational∂ strategies: China’s anti-access/area-denial (A2/AD) doctrine and the United States’ Joint∂ Operational Access Concept (JOAC). I argue that neither strategy will effectively ∂ dissuade opposing forces and instead inflame an escalating security dilemma between the∂ two principal powers of the 21st century. Both strategies seek to gain operational control∂ of the western Pacific. China’s maturing A2/AD strategy seeks to bypass conventional∂ balancing metrics and instead relies upon specific technology and regional advantages to∂ create an operating environment that is too dangerous to risk United States’ forces. In∂ response, the United States’ JOAC mandates assured access in A2/AD environments will∂ be a key operational requirement for future military plans and force posture. Previous∂ security dilemmas have occurred due to the insecurity inherent within an anarchic∂ international order in which the security preparations of one state will inevitable create∂ insecurity within surrounding states. Often historical security dilemmas manifest themselves as arms races, competing coalitions, or even outright war. If further∂ implemented, China’s A2/AD and the United States’ JOAC will generate an atmosphere∂ ripe for the development of regional arms races and military tensions within the guise of∂ a larger Sino-American security dilemma. I maintain that the operational characteristics of A2/AD and JOAC are indicative∂ of a classical security dilemma due to three inherent conditions shared by both strategies:∂ the primacy of preemptive offensive strikes, misperceptions surrounding new A2/AD∂ weapon technology and finally, the uncertainty created by a lack of discernable∂ information about China’s ultimate strategic goals in the Pacific. There is no standard∂ list of ingredients for security dilemmas but preemption, misperception, and uncertainty∂ were chosen because of the frequency these factors appeared in security dilemma∂ literature. These three accelerants combine to create chronic insecurity that is∂ reminiscent of past security dilemmas and only serve to foster an operational ∂ environment that impedes future stability. To demonstrate the emerging structural∂ instability within the Asia-Pacific, this chapter will utilize a historical case study method∂ that compares how preemption, misperception and uncertainty drove the Cold War-era∂ security dilemma between the Soviet Union and the United States to analogous patterns∂ emerging in the Sino-U.S. relationship. To demonstrate the structural instability of∂ preemptive attack, I will compare the Cold War’s first strike nuclear doctrine and the∂ offensive long-range first-strike that are favored in both Chinese and United States∂ strategic literature. For examining how misperceptions of military capabilities and∂ technology exacerbate regional insecurity, I will compare the paranoia surrounding early∂ Soviet intercontinental ballistic missiles (ICBMs) to the nascent fear surrounding China’s∂ anti-ship ballistic missile (ASBM). Finally, I will liken the misperception surrounding∂ Soviet grand intentions and the ensuing strategic uncertainty with a similar lack of∂ understanding and information when attempting to decipher China’s long-term strategic∂ goals.

### Multipolarity increases conflict

#### Multipolarity is bad – insecurities cause security dilemmas, proliferation, and escalatory measures

**Roloff 14** – Writer of a thesis submitted to Johns Hopkins University in conformity with the requirements for∂ the degree of Master of Arts in Global Security Studies. (Luke, “PATTERNS OF INSTABILITY: THE CAUSES AND CONSEQUENCES OF STRUCTURAL INSECURITY AND POWER POLITICS IN THE ASIA-PACIFIC SPHERE”, May 2014, https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/37219/ROLOFF-THESIS-2014.pdf?sequence=1//DM)

The security dilemma concept is a theoretical foundation in realist school∂ interpretations of security problems and especially relevant within the defense realism∂ and offense-defense realist subsets. A realist interpretation of the world maintains that∂ anarchy, or the lack of any overarching authority to protect individual states, defines the∂ international order. Therefore, as noted realist scholar John Mearsheimer predicts, there∂ are certain “bedrock assumptions” that exist in an anarchic international system. 7∂ Some∂ of Mearsheimer expectations are: states will develop offensive military capabilities; states∂ are never sure of another actor’s intention; and every state is a rational actor that seeks to∂ survive in such a Hobbesian atmosphere.8 Professor Shiping Tang, in his work The Security Dilemma: A Conceptual∂ Analysis, builds upon Mearsheimer’s ‘bedrock’ and constructs a theoretical roadmap∂ demonstrating the causal linkages, which explicate how an anarchic world order leads to∂ security dilemmas and conflict. Tang shares many of Mearsheimer’s assumptions and∂ draws connections between the self-help anarchic structure that creates a high level of∂ “uncertainty about each other intentions and fear, states resort to the accumulation of∂ power and capabilities as a means of defense, and these capabilities inevitably contain∂ some offensive capabilities”.9∂ This uncertainty and resulting armament generate the∂ security dilemma, whereas stated, other states begin to arm themselves in response. Tang∂ believes that this cycle of “actions and reactions” when mixed with national psychologies∂ and material estimations, entrenches each state into a self-propelled pattern of heightened∂ tensions and escalatory measures- often referred to as a security spiral.∂ 10 The unfortunate∂ outcome being that the security dilemma often results in war, deteriorating relations, or∂ arms races. According to the security dilemma, this creates a self-defeating paradox∂ because a state’s attempts for increased security will regularly result in a less stable and∂ increasingly hostile environment.

####

# Solvency Extensions

### Solvency – 702 Exclusivity Good

#### 702 is a stronger limit on domestic surveillance than 12333

Bedoya 14 - Executive Director of the Center on Privacy and Technology at Georgetown Law (Alvaro Bedoya, “Executive Order 12333 and the Golden Number”, Just Security, 10/9/2014, http://justsecurity.org/16157/executive-order-12333-golden-number/)//MBB

More importantly, Litt’s explanation overlooks the fact that 12333 is a bulk collection authority – while section 702 is not. Yes, 702 data pass through the United States. But at the end of the day, while section 702 collection may seem “bulky,” it is nonetheless an exclusively targeted collection authority. Section 702 can be used only to collect on communications to, from or (controversially) about a specific target. There aren’t an infinite number of targets. In 2013, there were 89,138 of them. Executive Order 12333, by contrast, allows for pure bulk collection of overseas electronic communications. There is no requirement that electronic surveillance under 12333 be targeted at a particular individual, organization or facility. A recent directive from the President (PPD-28) explains: References to signals intelligence collected in “bulk” mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.). (Emphasis mine.) Indeed, 12333 lets the government conduct any electronic surveillance, so long as it does so from a location abroad, so long as it does not affirmatively target a U.S. person, and so long as it is done for a “foreign intelligence or counterintelligence purpose.” The resultant difference in scale of collection is significant. In his 2011 opinion, Judge Bates stated that NSA acquired over 250 million Internet communications annually under section 702; the Washington Post revealed that a single program under 12333 collected nearly 5 billion cellphone location records every day. This may be a bit of an apples-to-oranges comparison, but it’s an instructive one nonetheless. The untargeted nature and massive scope of 12333 collection strongly suggest that it may be used to collect far more U.S. person communications than are collected under section 702. Moreover, because 12333 allows for bulk collection, it would seem to stand a high chance of capturing Americans’ communications that are, in fact, entirely unrelated to foreign intelligence – precisely the category of protected communications that Judge Bates found so problematic. Curiously, the new report on 12333 from the NSA’s Civil Liberties and Privacy Office explicitly excludes bulk collection from its analysis. It would be great if Judge Bates could ask these questions. But he can’t. The FISC lacks jurisdiction over 12333 collection. And so it is on Congress – and on us – to fill in the gap. For section 702, the sponsors of the USA FREEDOM Act succeeded in adding a modest but nonetheless incrementally positive provision that would require the Director of National Intelligence to either annually disclose an estimate of the number of Americans affected by section 702 programs, or to provide a detailed, public explanation of why he or she cannot provide that figure (see subsection “(e)(4)” of section 603 of the bill).

#### FISA isn’t a rubber stamp – its approval rate is due to executive internal compliance

**Sievert 14** \* Professor, Bush School of Government and U.T. Law School, author of three editions of Cases and Materials on US Law and National Security (Ronald, “Time to Rewrite the Ill-Conceived and Dangerous Foreign Intelligence Surveillance Act of 1978”, National Security Law Journal Vol. 3, Issue 1 – Fall 2014)//GK

The public claim that the FISA Court is somehow a rubber stamp because most applications are eventually approved, is completely ludicrous. This view does not reflect the real difficulty of obtaining a FISA order.152 When the defense made a “rubber stamp” objection before the Ninth Circuit in United States v. Cavanaugh, the court noted that the lack of rejections was “consistent with a practice of careful compliance with statutory requirements on the part of the government.”153 Royce Lamberth, a former Chief Judge of the FISA Court, attributed the government’s perfect record to the “superb internal review process created within DOJ,” 154 which requires personal approval of both the Attorney General and the head of the requesting agency for each FISA application. This often results in the submission of forty to fifty page affidavits at a minimum to FISA judges. 155 Judge Lamberth also stated that far from granting automatic approval of FISA requests, the Court often comes back to the government with questions and comments about their requests and often requires intelligence agencies to modify them to meet the Court’s standards.156 In 2013, Reggie Walton, current FISA Court presiding judge, said that “the court alters numerous government requests for data collection or even refuses some of them, even though that may not be reflected in the final statistics that the court sends to Congress.”157 In the opinion of Judge Richard Posner, the positive statistics are a reflection of the fact that the government is actually far too conservative in seeking surveillance orders. He believes that in our legalistic culture the FBI tries to avoid violating the law and does not want to sail anywhere close to the wind. “The analogy is to a person who has never missed a plane in his life because he contrives always to arrive at the airport eight hours before the scheduled departure time.”158

#### 702 has multiple layers of oversight – only .1% of cases are errors

**PCLOB 14** - independent, bipartisan agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act (“Report on the Surveillance Program Operated Pursuant to Sec7on 702 of the Foreign Intelligence Surveillance Act”, 07/02/14, [https://www.pclob.gov/library/702-Report.pdf)//GK](https://www.pclob.gov/library/702-Report.pdf%29//GK) p. 71

In enacting Section 702, Congress mandated additional external layers of oversight, each resulting in reports made to Congress and the FISC. This Section describes the targeting and minimization reviews conducted by the DOJ’s National Security Division (“NSD”) and the ODNI, the reports issued by the inspectors general, and additional oversight activities conducted by the FISC and the Congressional Committees. A. NSD/ODNI Targeting Reviews As is discussed above, the NSA is required under its targeting procedures to document every targeting decision made under its targeting procedures. The record of each targeting decision, known as a tasking sheet, includes (1) the specific selector to be tasked,312 (2) citations to the specific documents and communications that led the NSA to determine that the target is reasonably believed to be located outside the United States,313 (3) a narrative describing the contents of these specific documents and communications, (4) a statement regarding the assessed U.S. person status of the target, and (5) a statement identifying the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired.314 The NSD conducts a post-tasking review of every tasking sheet provided by the NSA;315 the ODNI reviews a sample of these sheets. In addition to evaluating whether the tasking complied with the targeting procedures, the NSD and ODNI review the targeting for overall compliance with the statutory limitations, such as the prohibition against reverse targeting. If the NSD or ODNI is unable to determine whether the tasking sheet is sufficient, the NSD and ODNI will require the NSA to provide the cited documents and communications that underlie the NSA’s foreignness determination at a bimonthly onsite review.316 The NSD and ODNI also engage with the NSA compliance and legal personnel to ask follow-up questions regarding the foreignness and foreign intelligence purpose determinations.317 As needed, the NSD and ODNI also seek additional information from the CIA and FBI regarding selectors that they have nominated.318 The NSD and ODNI’s review of foreign intelligence purpose determinations is more limited than its review of foreignness determinations insofar as the NSA analysts are required to document the basis for their foreignness determination (i.e., they must show their work), whereas the analyst need only identify a foreign intelligence purpose. The results of each NSD/ODNI bimonthly review are required by statute to be provided to the Congressional Committees.319 Historically, the NSD and ODNI’s bimonthly reviews have determined that approximately 0.1% of all the NSA taskings did not meet the requirements of the NSA targeting procedures.320 Additionally but separately, the NSD and ODNI also conduct approximately monthly reviews of the FBI’s application of its own targeting procedures.321 The NSD currently reviews every instance in which the FBI’s evaluation of foreignness revealed any information regarding the target, regardless of whether the information confirms or rebuts the NSA's foreignness determination. Follow-up questions regarding the FBI’s evaluation of this information are discussed with FBI analysts and supervisory personnel.322 Like the NSA reviews, the results of the NSD/ODNI monthly reviews regarding FBI targeting are documented in a report that must be sent to the Congressional Committees.323 The NSD and ODNI have not reported the historical percentage of tasking incidents that have been discovered as a result of these reviews. For the period of June through November 2012, the overall FBI tasking incident error rate, which would include incidents discovered by the NSD/ODNI reviews, was 0.04%.

#### Section 702 means only non-US persons can be targeted – incidental collection about US persons requires court approval and minimization

**Cordero, 15 -** Director of National Security Studies, Georgetown University Law Center, Adjunct Professor of Law(Carrie, “Focusing on 702: A Brief Reply to the Brennan Center’s Liza Goitein and Faiza Patel” Lawfare, 4/10, <http://www.lawfareblog.com/focusing-702-brief-reply-brennan-centers-liza-goitein-and-faiza-patel>

On the intended purpose of the 2008 amendment, I don’t think that a review of the legislative record would show that the “primary purpose” of Section 702 - that is, the reason the legislative amendment was sought - was to collect on U.S. persons (and/or persons in the United States, which includes both U.S. and non-U.S. persons.) A review of the statements for the record from DOJ and DNI officials in 2007 and 2008 would reveal that the purpose was to facilitate acquisition directed at non-U.S. persons reasonably believed to be outside the United States, for foreign intelligence purposes. Perhaps some think that those arguments were simply subterfuge for a behind-the-scenes goal of collecting on U.S. persons, but that impression is not supported by the record. Nor does it square with my own experience working on these issues in government during that time period. Moreover, to the extent that those type of concerns were held by some members of Congress at the time, the final, enacted version of the FISA Amendments Act of 2008 included a specific prohibition on reverse targeting (targeting a non-U.S. person for collection with the actual goal of collecting the communications of a U.S. person), as well as court approval of the targeting and minimization procedures. Incidental collection of U.S. persons was foreseen and expected; that’s why there are minimization procedures that provide rules for how those communications must be handled. But when the government sought 702 authority, it did so for the purpose of facilitating the targeting of non-U.S. persons outside the United States for foreign intelligence purposes. As to effect, Section 702 does not “remove the requirement for an individualized order for the acquisition of communications between foreign targets and U.S. persons,” as Liza and Faiza describe it, in circumstances when the target of the collection is a U.S. person, or, any person in the U.S. Instead, if the U.S. government seeks to target for collection a U.S. person anywhere in the world (including the U.S., of course), or a non-U.S. person inside the United States, the government must obtain a probable cause based order from the Foreign Intelligence Surveillance Court.

### Solvency – FISA Effective

#### Curtailing NSA authority under FISA is the most effective action the US can take

**Donohue, 14** - Professor of Law, Georgetown University Law Center (Laura, “HIGH TECHNOLOGY, CONSUMER PRIVACY, AND U.S. NATIONAL SECURITY”, Georgetown University Law Center, 17 September 2014, http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1119&context=cong)//gg

Numerous steps could be taken by Congress to address the situation in which U.S. industry currently finds itself. The most effective and influential decision that legislators could take would be to curb the NSA’s authorities under the Foreign Intelligence Surveillance Act. This action has two components: first, ending the telephony metadata collection program and, second, restricting the use of to/from, or about collection under upstream interceptions. Both programs would further benefit from greater transparency, to make it clear that their aim is to prevent foreign aggression and to prevent threats to U.S. national security—not to engage in the interception of trade secrets or to build dossiers on other countries’ populations. The second most effective change that could be undertaken would be to introduce stricter privacy controls on U.S. companies, in the process bringing the United States into closer line with the principles that dominate in the European Union. The two entities are not as far apart as the dialogue might have one assume, and so changes required in this sphere would be minimal. Together, these two alterations—curbing the NSA surveillance programs and providing increased consumer protections for privacy—would allow U.S. industry to argue changed circumstance to allow companies to again become competitive for contracts and markets to which they seek access. A third alteration that would make a substantial difference over the longer term relates to the national security infrastructure. The current failure of the United States to integrate economic concerns creates a vulnerability for the country in terms of the breadth and depth of programs subsequently adopted. New thought needs to be given to how to take on board—and mitigate—potentially devastating economic consequences of government surveillance efforts.

#### FISA reforms that change PRISM and upstream are key to restoring US credibility

**Donohue, 14** - Professor of Law, Georgetown University Law Center (Laura, “HIGH TECHNOLOGY, CONSUMER PRIVACY, AND U.S. NATIONAL SECURITY”, Georgetown University Law Center, 17 September 2014, <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1119&context=cong)//gg>

In addition to the economic impact of NSA telephony metadata collection (discussed, infra), the program runs contrary to Congressional intent in introducing the Foreign Intelligence Surveillance Act, contradicts the statutory language, and violates the Fourth Amendment.94 In 2014 the Privacy and Civil Liberties Oversight Board came to a similar conclusion,95 as did the President’s own appointed Review Group, charged with considering the telephony metadata collection program, in 2013.96 Accordingly, the President announced on January 17, 2014 that he was “ordering a transition that will end the Section 215 bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk metadata.”97 The alternative approach was to be developed by March 28, 2014. Nine months later, on September 13, 2014, the Foreign Intelligence Surveillance Court approved DOJ’s request to extend the program for another 90 days—without any transition program in place. Although the President issued a new presidential directive in January 2014 for U.S. signals intelligence activities both at home and abroad, the classified nature of parts of the document, international skepticism about the Administration’s commitment to privacy, and the failure of the Administration to make good on its promise of transition to a new program meant that the global community, with good reason, has questioned whether anything has really changed. No new legislation is in place that would provide limits on the Executive Branch beyond those that operated for the duration of the bulk collection program. As a matter of Section 702 and the interception of international content, both PRISM and upstream collection present global concerns—neither of which have been addressed through any legislative change. The existence of these programs, while perhaps statutorily consistent with the FISA Amendments Act, as well as constitutionally sufficient with regard to the interception of non-U.S. persons communications, where the individual is reasonably believed to be located outside the United States, as a policy matter, goes some way towards undermining international confidence in U.S. companies. The Fourth Amendment does not reach non-U.S. persons based overseas who lack a substantial connection to the United States.98 Writing for the Court in United States v. Verdugo-Urquidez, Chief Justice Rehnquist concluded that “the people” referred to in the Fourth Amendment indicate a particular group—not merely people qua people.99 His reading stems from a deeply Aristotelian approach: i.e., one that emphasizes membership in the polis ( ), or political community, as a concomitant of forming a structure of government.100 As members of the polis, U.S. persons, both distributively and collectively, obtain the protections of the constitution. Looked at in this regard, the Constitution itself embodies the collective organization of “the people” into one entity. “U.S. persons” and “the people” are therefore one and the same. The “right of the people” thus refers to a collective group of individuals “who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community.”101 Very few cases address precisely what constitutes sufficient contact with the United States to satisfy the “substantial connections” aspect of the majority’s decision. Those that do point in seemingly different directions.102 At a minimum, however, it would be extraordinary to assume that simply because an individual uses a U.S. company, he or she thereby gains the protections of the Fourth Amendment. This was the basic argument underlying the “modernization” of FISA in the first place, to take account of bad actors, communicating overseas, who would suddenly fall within the more protective FISA regime merely because their communications happened to come within U.S. territory by nature of the carrier in question. Even recognizing, however, that few constitutional barriers may apply to the programmatic use of Section 702 insofar as it is applied to non-U.S. persons (leaving aside the questions that accompany the incidental collection of U.S. persons’ information, as well as entirely domestic conversations), as a matter of policy, certainly both PRISM and the use of to/from or about collection in upstream gathering has dramatically undermined U.S. industry. As a matter of policy, therefore, greater restrictions, more transparency, and more effective oversight of the international collection of content may help to alter the situation with regard to the skepticism expressed towards U.S. companies.

### Solvency – Warrant Requirement

#### Fourth Amendment warrant requirement essential to addresses public trust

Heymann, 15 [Philip B, former Deputy Attorney General in the Clinton administration and currently a law professor at Harvard Law School, AN ESSAY ON DOMESTIC SURVEILLANCE, [file:///C:/Users/Jonah/Downloads/Lawfare-Philip-Heymann-SURVEILLANCE-for-publ-10-May-2015.pdf](file:///C%3A/Users/Jonah/Downloads/Lawfare-Philip-Heymann-SURVEILLANCE-for-publ-10-May-2015.pdf)] Schloss4

The way the 4th Amendment works is straightforward; comprehensible to Americans who would distrust a secret reliance merely on search terms; and surprisingly useful. To search any place, record, or communication which is not freed, by Supreme Court doctrine, of the 4th Amendment obligations of probable cause and a warrant to search any place, record, or communication which is not excepted by Supreme Court doctrine from 4th Amendment obligations of a probable cause and a warrant (with some exceptions) requires a factual basis for thinking it probable (or, in some cases, by reasonably suspecting) that evidence of either a crime or a specified national danger will be found in a particular place (or in a particular communication). A court, having satisfied itself of such a “predicate,” must certify that fact and authorize a search or electronic surveillance and specify the conditions under which it may take place. The attributes and advantages of this system are immense. Consider six wonders of the 4th Amendment: (1) The system is entirely comprehensible and makes perfect sense to a very high percentage of Americans who would never understand or trust the neutrality of government officials furnishing secret search terms to technicians at the NSA. (2) The way it works makes unnecessary any substantial effort to establish that the costs in terms of privacy of a particular search are less than benefits to law enforcement or national security. It does not require an extraordinarily complicated balancing of the amount of damage a search does to privacy versus the amount of value it adds in terms of reduced crime or reduced danger to national security. While we would like to allow only those searches whose cost in terms of citizen insecurity are outweighed by the benefits in terms of solving or preventing a crime, the cost of making that judgment in the case of each individual search would be immense. Consider how difficult it would be to weigh each of the categories – costs and benefits – to determine where the balance falls. The cost to citizens’ sense of privacy depends on, among other things, the fears of government misuse of the power to search and that itself depends on whether the subject of the search was known or anonymous when the search took place, how sensitive the information to be acquired was, how private was the location where the information was found, how much was learned about a single individual, and how carefully the information was retained and not disseminated. On the other side of the balance, the benefits of surveillance are equally fact-dependent. They depend in each case on how dangerous is the activity that is subject to surveillance, what alternative ways there are to learn about it, how useful (or alternatively unnecessary) the information likely to be found is in ending that danger, the inability of targets to find out about the manner of surveillance and thereby avoid it, and the likely promptness of discovery of evidence. Any such costly analysis of the trade-off between cost and benefits of a particular case is replaced under the 4th Amendment by simply requiring a showing that evidence of a crime or of a grave future threat would be found in the place or communication and at the time of the search or electronic surveillance. The police can quickly know what they are allowed and forbidden to do. The cost of this radically simplified balance is merely that a search is allowed even when the benefits of solving the crime may be relatively unimportant. Yet this does not detract greatly from the security individuals can feel under the 4th Amendment. (3) Use of 4th Amendment standards provides assurance of privacy to the vast majority of citizens who are likely to know whether there is probable cause to search their places or surveil their communications. (4) At the same time, it prevents foolish or abusive government searches, an important check on the efficiency and excesses of law enforcement. (5) The system of the 4th Amendment, unlike a grand jury subpoena for documents, does not tip off the suspect that he is about to be searched (and thus should hide or destroy any evidence). The suspect takes no part in the decision of the court to issue a warrant. (6) The 4th Amendment manages to do these things without making known to the suspect, even after a search or an arrest, the identity of any informant who has decided to subject a dangerous suspect to the risk of a search or electronic surveillance of his communications. The informant’s identity may and will be kept secret.

### AT: Foreign servers

#### Plan reverses incentives for companies to shift to foreign subsidiaries

**Eoyang and Bishai, 15** - \*Mieke Eoyang is the Director of the National Security Program at Third Way, a center-left think tank. She previously served as Defense Policy Advisor to Senator Edward M. Kennedy, and a subcommittee staff director on the House Permanent Select Committee on Intelligence, as well as as Chief of Staff to Rep. Anna Eshoo (D-Palo Alto); \*\*Chrissy Bishai is a Fellow at Third Way (“Restoring Trust between U.S. Companies and Their Government on Surveillance Issues” 3/19, <http://www.thirdway.org/report/restoring-trust-between-us-companies-and-their-government-on-surveillance-issues>

The move by certain U.S. companies to place subsidiaries in foreign ownership to resist requests by the U.S. government presents an interesting twist on this idea. In shifting the balance back to increased protections for U.S. companies, this legislation would change the incentives so that claiming U.S. law would have operational advantages in giving companies uniformity of law for all their data. This would also encourage the use of a single choice of law for all data governed by a company—that of the nationality of incorporation—rather than encouraging a choice of law patchwork to govern the data as it flows around the world.

### AT: Circumvention

#### NSA will comply

**De 14** - General Counsel, National Security Agency (Rajesh, “The NSA and Accountability in an Era of Big Data”, JOURNAL OF NATIONAL SECURITY LAW & POLICY, 2014, p.8-10//DM)

Finally, NSA traditionally has maintained a strong culture of compliance among its workforce. Employees receive basic mandatory training on NSA’s legal authorities and the procedures that ensure the protection of privacy rights. Personnel also must receive refresher training throughout their career at NSA. Follow-on training can include highly specialized legal and compliance training focused on the specific requirements of the employee’s assigned mission. NSA has also proactively established a corporate Director of Compliance to help ensure that legal, technical, and operational requirements of the mission remain aligned. NSA’s compliance efforts draw from best practices across industry (such as IT security and other heavily regulated industries like healthcare). NSA is actively engaging with the broader compliance community to partner, to share best practices, and to understand emerging trends.

#### NSA is invested in the perception of compliance

Schlanger 15 [Margo, Professor of Law at the University of Michigan Law School, and the founder and director of the Civil Rights Litigation Clearinghouse., Intelligence Legalism and the National Security Agency’s Civil Liberties Gap, [file:///C:/Users/Jonah/Downloads/Intelligence%20Legalism%20and%20the%20National%20Security%20Agency-s%20Civil%20Li%20(2).pdf](file:///C%3A/Users/Jonah/Downloads/Intelligence%20Legalism%20and%20the%20National%20Security%20Agency-s%20Civil%20Li%20%282%29.pdf)] Schloss3

In total, more than a few hundred people spend all or a substantial part of their work weeks on NSA compliance and oversight. This enormous staffing commitment itself demonstrates real commitment to abiding by the FISA and 12,333 rules. (In other topic areas, one might suspect that the commitment is to being seen to abide by the rules—but the IC’s secrecy undercuts that cynical interpretation.) Nonetheless, inevitably, the agency is far from perfectly compliant. On occasion, compliance errors have been extremely widespread: In 2009, the government disclosed a series of significant compliance failures to the FISA Court affecting both the internet and telephony metadata programs. These included systemic failures to comply with the reasonable articulable suspicion standard, by use of less strictly vetted alert lists and seed accounts; unauthorized sharing of unminimized query results with other agency personnel; and collection of fields of metadata beyond what was allowed by court order on nearly all the internet metadata records.91 In addition, in 2011, the government reported that the “upstream” methods it was using to surveil American internet communications abroad were incapable of confining NSA access to only communications that met the standard for collection.92 These were extremely significant failures, and they prompted some moderately robust responses— creation of the current NSA compliance office,93 augmentation of the Justice Department oversight role, 94 and some stern (though for years secret) lectures by the FISA Court judges. It is surely reasonable to expect better than these low points. But it would be unrealistic to demand either perfect compliance or perfect detection of noncompliance. Both are unattainable for an organization as complex as the NSA, governed by rulesets as complex as the Foreign Intelligence Surveillance Act, Executive Order 12,333, and their related procedural documents. Error, after all, has many causes. Sometimes the rules are misunderstood or miscommunicated. 96 Sometimes someone who understands the rules makes a mistake—enters a typo, for example, 97 or seeks approval later than the rules require.98 Sometimes, one can imagine, systems fail—a computer algorithm that is supposed to distinguish among people with different statuses might miscategorize a new status, for example. And sometimes people try to defeat the rules.99 In a system as massive and complicated as the NSA’s signals intelligence program, even an extremely low rate of error can add up.100 (Although because most of the information collected does not involve persons in the U.S. or Americans abroad, these errors frequently do not violate anyone’s constitutional rights, under current doctrine.) Of course, each type of error can be reduced. But compliance errors are often hydraulic—pushing out errors in one place is likely to introduce at least some errors in another place.101 The goal, then, is not zero errors, but rather, as the NSA’s Director of Compliance puts it, to “assure compliance at a reasonable level.” 102 NSA has not always achieved that goal—but it musters substantial effort to do so.