# NSA NEGATIVE

## NSA Overreach Advantage Answers

### Internet freedom Take-outs

#### Corporate surveillance wrecks internet freedom

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, Ch. 6)//AK

Most of the big US defense contractors, such as Raytheon, Northrop Grumman, and Harris Corporation, build cyberweapons for the US military. And many big IT companies help build surveillance centers around the world. The French company Bull SA helped the Libyan government build its surveillance center. Nigeria used the Israeli firm Elbit Systems. Syria used the German company Siemens, the Italian company Area SpA, and others. The Gadhafi regime in Libya purchased telephone surveillance technology from China’s ZTE and South Africa’s VASTech. We don’t know who built the Internet surveillance systems used in Azerbaijan and Uzbekistan, but almost certainly some Western companies helped them. There are few laws prohibiting this kind of technology transfer, and the ones that exist are easily bypassed. These are not only specially designed government eavesdropping systems; much government surveillance infrastructure is built for corporate use. US-based Blue Coat sells monitoring and content filtering systems for corporate networks, which are also used for government surveillance in countries like Burma, China, Egypt, Indonesia, Nigeria, Qatar, Saudi Arabia, Turkey, and Venezuela. Netsweeper is a Canadian corporate filtering product used for censorship by governments in Qatar, Yemen, the UAE, Somalia, and Pakistan. Filtering software from the US company Fortinet is used to censor the Internet in Burma; SmartFilter, from the US company McAfee and normally used in schools, helps the governments of Tunisia and Iran censor the Internet in their countries. Commercial security equipment from the UK company Sophos has been used by Syria and other oppressive regimes to surveil and arrest their citizens. Technology is value neutral. You can use your phone to call 911 or to plan a bank robbery. There’s no technical difference between a government’s using a tool to identify criminals or using it to identify dissidents. There’s no technical difference between corporate and government uses. Legitimate corporate tools for blocking employees from e-mailing confidential data can be used by repressive governments for surveillance and censorship. Conversely, the same anti-censorship tools that Saudi and Iranian dissidents use to evade their governments can be used by criminals to distribute child porn. Encryption allows the good guys to communicate without being eavesdropped on by the bad guys, and also allows the bad guys to communicate without being eavesdropped on by the good guys. And the same facial recognition technology that Disney uses in its theme parks to pick out photos its patrons might want to buy as souvenirs can identify political protesters in China, and Occupy Wall Street protesters in New York.

#### Collapse of Internet freedom inevitable

VARA 14 [Vauhini Vara, the former business editor of newyorker.com, lives in San Francisco and is a business and technology correspondent for the New Yorker. “The World Cracks Down on the Internet”, 12-4-14, http://www.newyorker.com/tech/elements/world-cracks-internet, msm]

In September of last year, Chinese authorities announced an unorthodox standard to help them decide whether to punish people for posting online comments that are false, defamatory, or otherwise harmful: Was a message popular enough to attract five hundred reposts or five thousand views? It was a striking example of how sophisticated the Chinese government has become, in recent years, in restricting Internet communication—going well beyond crude measures like restricting access to particular Web sites or censoring online comments that use certain keywords. Madeline Earp, a research analyst at Freedom House, the Washington-based nongovernmental organization, suggested a phrase to describe the approach: “strategic, timely censorship.” She told me, “It’s about allowing a surprising amount of open discussion, as long as you’re not the kind of person who can really use that discussion to organize people.”¶ On Thursday, Freedom House published its fifth annual report on Internet freedom around the world. As in years past, China is again near the bottom of the rankings, which include sixty-five countries. Only Syria and Iran got worse scores, while Iceland and Estonia fared the best. (The report was funded partly by the Dutch Ministry of Foreign Affairs, the United States Department of State, Google, and Yahoo, but Freedom House described the report as its “sole responsibility” and said that it doesn’t necessarily represent its funders’ views.)¶ China’s place in the rankings won’t come as a surprise to many people. The notable part is that the report suggests that, when it comes to Internet freedom, the rest of the world is gradually becoming more like China and less like Iceland. The researchers found that Internet freedom declined in thirty-six of the sixty-five countries they studied, continuing a trajectory they have noticed since they began publishing the reports in 2010.¶ Earp, who wrote the China section, said that authoritarian regimes might even be explicitly looking at China as a model in policing Internet communication. (Last year, she co-authored a report on the topic for the Committee to Protect Journalists.) China isn’t alone in its influence, of course. The report’s authors even said that some countries are using the U.S. National Security Agency’s widespread surveillance, which came to light following disclosures by the whistle-blower Edward Snowden, “as an excuse to augment their own monitoring capabilities.” Often, the surveillance comes with little or no oversight, they said, and is directed at human-rights activists and political opponents.¶ China, the U.S., and their copycats aren’t the only offenders, of course. In fact, interestingly, the United States was the sixth-best country for Internet freedom, after Germany—though this may say as much about the poor state of Web freedom in other places as it does about protections for U.S. Internet users. Among the other countries, this was a particularly bad year for Russia and Turkey, which registered the sharpest declines in Internet freedom from the previous year. In Turkey, over the past several years, the government has increased censorship, targeted online journalists and social-media users for assault and prosecution, allowed state agencies to block content, and charged more people for expressing themselves online, the report noted—not to mention temporarily shutting down access to YouTube and Twitter. As Jenna Krajeski wrote in a post about Turkey’s Twitter ban, Prime Minister Recep Tayyip Erdoğan vowed in March, “We’ll eradicate Twitter. I don’t care what the international community says. They will see the power of the Turkish Republic.” A month later, Russian President Vladimir Putin, not to be outdone by Erdoğan, famously called the Internet a “C.I.A. project,” as Masha Lipman wrote in a post about Russia’s recent Internet controls. Since Putin took office again in 2012, the report found, the government has enacted laws to block online content, prosecuted people for their Internet activity, and surveilled information and communication technologies. Among changes in other countries, the report said that the governments of Uzbekistan and Nigeria had passed laws requiring cybercafés to keep logs of their customers, and that the Vietnamese government began requiring international Internet companies to keep at least one server in Vietnam.¶ What’s behind the decline in Internet freedom throughout the world? There could be several reasons for it, but the most obvious one is also somewhat mundane: especially in countries where people are just beginning to go online in large numbers, governments that restrict freedom offline—particularly authoritarian regimes—are only beginning to do the same online, too. What’s more, governments that had been using strategies like blocking certain Web sites to try to control the Internet are now realizing that those approaches don’t actually do much to keep their citizens from seeing content that the governments would prefer to keep hidden. So they’re turning to their legal systems, enacting new laws that restrict how people can use the Internet and other technologies.¶ “There is definitely a sense that the Internet offered this real alternative to traditional media—and then government started playing catch-up a little bit,” Earp told me. “If a regime has developed laws and practices over time that limit what the traditional media can do, there’s that moment of recognition: ‘How can we apply what we learned in the traditional media world online?’ ”¶ There were a couple of hopeful signs for Internet activists during the year. India, where authorities relaxed restric­tions that had been imposed in 2013 to help quell rioting, saw the biggest improvement in its Internet-freedom score. Brazil, too, notched a big gain after lawmakers approved a bill known as the Marco Civil da Internet, which protects net neutrality and online privacy. But, despite those developments, the report’s authors didn’t seem particularly upbeat. “There might be some cautious optimism there, but I do not want to overstate that because, since we started tracking this, it’s been a continuous decline, unfortunately,” Sanja Kelly, the project director for the report, told me. Perhaps the surprising aspect of Freedom House’s findings isn’t that the Internet is becoming less free—it’s that it has taken this long for it to happen.

#### As internet use increases, internet freedom will inevitably decrease – it’s zero-sum

Kelly and Cook 11 [Sanja Kelly, managing editor, and Sarah Cook, assistant editor, at Freedom House produced "Freedom on the Net: A Global Assessment of Internet and Digital Media," a 2011 report. “Internet freedom”, 4-17-11, http://www.sfgate.com/opinion/openforum/article/Internet-freedom-declining-as-use-grows-2375021.php, msm]

Indeed, as more people use the Internet to freely communicate and obtain information, governments have ratcheted up efforts to control it. Today, more than 2 billion people have access to the Internet, a number that has more than doubled in the past five years. Deepening Internet penetration is particularly evident in the developing world, where declining subscription costs, government investments in infrastructure, and the rise of mobile technology has allowed the number of users to nearly triple since 2006.¶ In order to better understand the diverse, rapidly evolving threats to Internet freedom, Freedom House, a Washington, D.C., NGO that conducts research on political freedom, has undertaken an analysis - the first of its kind - of the ways in which governments in 37 key countries create obstacles to Internet access, limit digital content and violate users' rights. What we found was that Internet freedom in a range of countries, both democratic and authoritarian, is declining. Emboldened governments and their sympathizers are increasingly using technical attacks to disrupt political activists' online networks, eavesdrop on their communications and debilitate their websites. Such attacks were reported in at least 12 countries, ranging from China to Russia, Tunisia to Burma, Iran to Vietnam. In Belarus, at the height of controversial elections, the authorities created mirror versions of opposition websites, diverting users to the new ones, where deliberately false information on the times and locations of protests were posted. In Tunisia, in the run-up to the January 2011 uprising that drove the regime from power, the authorities regularly broke into the e-mail, Facebook and blogging accounts of opposition and human rights activists, either deleting specific material or simply collecting intelligence about their plans.¶ Governments around the world increasingly are establishing mechanisms to block what they deem to be undesirable information. In many cases, the restrictions apply to content involving illegal gambling, child pornography, copyright infringement or the incitement of hatred or violence. However, a large number of governments are also engaging in deliberate efforts to block access to information related to politics, social issues and human rights. In Thailand, tens of thousands of websites critical of the monarchy have been blocked. In China - in addition to blocking dissident websites - user discussions and blog postings revealing tainted-milk products, pollution or torture are deleted.¶ Centralized government control over a country's connection to international Internet traffic also emerged as one significant threat to online free expression. In one-third of the states examined, authorities have exploited their control over infrastructure to limit access to politically and socially controversial content or, in extreme cases, cut off access to the Internet entirely, as Hosni Mubarak's government did in Egypt during the height of the protests there.¶ Until recently, the conventional assumption has been that Internet freedom would inexorably improve, given the technology's diffuse and open structure. But this assumption was premature. Our findings should serve as an early warning sign to defenders of free expression.¶

#### Reject their ahistorical idealism – the internet accelerates the worst parts of humanity

**Morozov, 2012**– Contributing editor at The New Republic and author of two books ; has written for The New York Times, The Economist, The Wall Street Journal, Financial Times, London Review of Books, Times Literary Supplement (Evgeny, The Net Delusion: The Dark Side of Internet Freedom, p. 256)//TT

Even worse, the supposed lawlessness and networked anarchy enabled by the Internet have resulted in greater social pressure to tame the Web. In a sense, the more important the Internet becomes, the greater the onus to rein in its externalities. Promoting the freedom to connect will be a tricky proposal to sell to voters, many of whom actually want the government to promote the freedom to disconnect—at least for particular political and social groups. If the last decade is anything to judge by, the pressure to regulate the Web is as likely to come from concerned parents, environmental groups, or various ethnic and social minorities as it is from authoritarian governments. The truth is that many of the opportunities created by a free-for-all anonymous Internet culture have been creatively exploited by people and networks that undermine democracy. For instance, it’s almost certain that a Russian white supremacist group that calls itself the Northern Brotherhood would have never existed in the pre-Internet era. It has managed to set up an online game in which participants—many of them leading a comfortable middleclass existence—are asked to videotape their violent attacks on migrant guest workers, share them on YouTube, and compete for cash awards. Crime gangs in Mexico have also become big fans of the Internet. Not only do they use YouTube to disseminate violent videos and promote a climate of fear, but they are also reportedly going through social networking sites hunting for personal details of people to kidnap. It doesn’t help that the offspring of Mexico’s upper classes are all interconnected on Facebook. Ghaleb Krame, a security expert at Alliant International University in Mexico City, points out that “criminals can find out who are the family members of someone who has a high rank in the police. Perhaps they don’t have an account on Twitter or Facebook, but their children and close family probably do.” It’s hard to imagine Mexican police officers becoming braver as a result. And social networking can also help to spread fear: In April 2010, a series of Facebook messages warning of impending gang wars paralyzed life in Cuernavaca, a popular resort, with only a few brave people daring to step outside (it proved to be a false alarm). The leaders of al-Shabab (“The Lads”), Somalia’s most prominent Islamist insurgency group, use text messaging to communicate with their subordinates, avoiding any face-to-face communication and the risks it entails. It’s not a particularly contentious conclusion that they have become more effective—and thus more of a menace—as a result. Plenty of other less notorious (and less violent) cases of networked harm barely receive any global attention. According to a 2010 report from the Convention on International Trade in Endangered Species, an international intergovernmental organization, the Internet has created a new market for trade in extinct species, allowing buyers and sellers to find each other more easily and trade more effectively. Kaiser’s spotted newt, found only in Iran, may be the first real victim of the Twitter Revolution. According to reports in the Independent, more than ten companies are selling wild-caught specimens over the Internet. Not surprisingly, the newt’s population was reduced 80 percent between 2001 and 2005 alone. Another informal market the Internet has boosted is organ trading. Desperate individuals in the developing world are bypassing any intermediaries and are offering their organs directly to those who are willing to pay up. Indonesians, for example, use a website called iklanoke.com, a local alternative to Craigslist, where their postings usually go unmonitored by police. A typical ad from Iklanoke reads, “16-year-old male selling a kidney for 350 million rupiah or in exchange for a Toyota Camry.” Text messaging has been used to spread hate in Africa, most recently in Muslim-Christian squabbles that erupted in the central Nigerian city of Jos in early 2010 that took the lives of more than three hundred people. Human rights activists working in Jos identified at least 145 such messages. Some instructed the recipients how to kill, dispose of, and burn bodies (“kill before they kill you. Dump them in a pit before they dump you”); others spread rumors that triggered even more violence. According to Agence France-Presse, one such message urged Christians to avoid food sold by Muslim hawkers, as it could have been poisoned; another message claimed political leaders were planning to cut water supplies to dehydrate members of one faith. Two years earlier Kenya lived through an eerily similar tumultuous period. The political crisis that followed Kenya’s disputed election that took place on December 27, 2007, showed that the networks fostered by mobile technology, far from being “net goods,” could easily escalate into uncontrollable violence. “If your neighbor is kykuyu, throw him out of his house. No one will hold you responsible,” said a typical message sent at the peak of the violence; another one, also targeting Kykuyus, said, “Let’s wipe out the Mt. Kenya mafia,” adding, “Kill 2, get 1 free.” But there was also a more disturbing effort by some Kykuyus to use text messaging to first collect sensitive information about members of particular ethnic groups and then distribute that information to attack and intimidate them. “The blood of innocent Kykuyus will cease to flow! We will massacre them right here in the capital. In the name of justice put down the names of all the Luos and Kaleos you know from work, your property, anywhere in Nairobi, not forgetting where and how their children go to school. We will give you a number on where to text these messages,” said one such message. At one point, the Kenyan authorities were considering shutting down mobile networks to avoid any further escalation of violence (between 800 and 1,500 people died, and up to 250,000 were displaced). Even though text messaging also proved instrumental in setting up a system that helped to track how violence spread around Kenya—a success story that gained far more attention in the media—one can’t just disregard the fact that text messaging also helped to mobilize hate. In fact, text messages full of hatred and highly intimidating death threats kept haunting witnesses who agreed to testify to the high-level Waki Commission set up to investigate the violence two years after the clashes. (“You are still a young man and you are not supposed to die, but you betrayed our leader, so what we shall do to you is just to kill you” was the text of a message received by one such witness.) The bloody Uighur-Han clashes that took place in China’s Xinjiang Province in the summer of 2009 and resulted in a ten-month ban on Internet communications appear to have been triggered by a provocative article posted to the Internet forum www.sg169.com. Written by an angry twenty-three-year-old who had been laid off by the Xuri Toy Factory in China’s Guangdong Province, 3,000 miles from Xinjiang, the article asserted that “six Xinjiang boys raped two innocent girls at the Xuri Toy Factory.” (China’s official media stated that the rape accusations were fake, and foreign journalists could not find any evidence to substantiate such claims either.) Ten days later, the Uighur workers at the toy factory were attacked by a group of angry Han people (two Uighurs were killed, and over a hundred were injured). That confrontation, in turn, triggered even more rumors, many of which overstated the number of people who had been killed, and the situation got further out of control soon thereafter, with text messaging and phone calls helping to mobilize both sides (the authorities eventually turned off all phone communications soon thereafter). A gruesome video that showed several Uighur workers being beaten by a mob armed with metal pipes quickly went viral as well, only adding to the tensions. Even countries with a long democratic tradition have not been sparred some of the SMS-terror. In 2005, many Australians received text messages urging attacks on their fellow citizens of Lebanese descent (“This Sunday every Fucking Aussie in the shire, get down to North Cronulla to help support Leb and wog bashing day. . . . Bring your mates down and let’s show them this is our beach and they’re never welcome back”), sparking major ethnic fights in an otherwise peaceful country. Ethnic Lebanese got similar messages, only calling for attacks on non-Lebanese Australians. More recently, right-wing extremists in the Czech Republic have been aggressively using text messaging to threaten local Roma communities. Of course, even if text messaging had never been invented, neo-Nazis would still hate the Roma with as much passion; to blame their racism on mobile phones would be yet another manifestation of focusing on technology at the expense of political and social factors. But the ease, scale, and speed of communications afforded by text messaging makes the brief and previously locally contained outbursts of neo-Nazi anger resonate in ways that they could have never resonated in an era marked by less connectedness. Perhaps, the freedom to connect, at least in its current somewhat abstract interpretation, would be a great policy priority in a democratic paradise, where citizens have long forgotten about hate, culture wars, and ethnic prejudice. But such an oasis of tolerance simply does not exist. Even in Switzerland, commonly held up as a paragon of decentralized democratic decision making and mutual respect, the freedom to connect means that a rather small and marginalized fraction of the country’s population managed to tap the power of the Internet to mobilize their fellow citizens to ban building new minarets in the country. The movement was spearheaded by right-wing blogs and various groups on social networking sites (many of them featuring extremely graphic posters—or “political Molotov cocktails,” as Michael Kimmelman of the New York Times described them—suggesting Muslims are threatening Switzerland, including one that showed minarets rising from the Swiss flag like missiles), and even peace-loving Swiss voters could not resist succumbing to the populist networked discourse. Never underestimate the power of Twitter and Photoshop in the hands of people mobilized by prejudice.

#### Internet freedom inhibits rational policymaking

**Morozov, 2012**– Contributing editor at The New Republic and author of two books ; has written for The New York Times, The Economist, The Wall Street Journal, Financial Times, London Review of Books, Times Literary Supplement (Evgeny, The Net Delusion: The Dark Side of Internet Freedom, p. 266)//TT

As the Internet mediates more and more of our foreign policy, we are poised to surrender more and more control over it. Of course, the era when diplomats could take the time to formulate deep and extremely careful responses to events was already over with the arrival of the telegraph, which all but killed the autonomy of the foreign corps. As far as thoughtful foreign policy is concerned, it’s all been downhill from there. It’s hardly surprising that John Herz, the noted theorist of international relations, observed in 1976 that “where formerly more leisurely but also cooler and more thoroughly thought-out action was possible, one now must act or react immediately.” The age of Internet politics deprives the diplomats of more than just autonomy. It’s also the end of rational policymaking, as policymakers are bombarded with information they cannot process, while a digitally mobilized global public demands an immediate response. Let’s not kid ourselves: Policymakers cannot craft effective policies under the influence of blood-curling videos of Iranian protesters dying on the pavement. By 1992 George Kennan, the don of American diplomacy and author of the famous “Long Telegram” from Moscow, which shaped much of American thinking during the Cold War and helped to articulate the policy of containment, had come to believe that the media killed America’s ability to develop rational foreign policy. Back then viral political videos were still the bread and butter of network television. After he watched the gruesome footage of several dead U.S. Army rangers being dragged through the streets of Mogadishu on CNN, Kennan made the following bitter note in his diary, soon republished as an op-ed in the New York Times: “If American policy from here on out . . . is to be controlled by popular emotional impulses, and particularly ones invoked by the commercial television industry, then there is no place—not only for myself but for what have traditionally been regarded as the responsible deliberative organs of our government, in both executive and legislative branches.” Kennan’s words were soon seconded by Thomas Keenan, the director of the Human Rights Project at Bard College, who believes that “the rational consideration of information, with a view to grounding what one does in what one knows, now seems overtaken and displaced by emotion, and responses are now somehow controlled or, better, remote-controlled by television images.” Now that television images have been superseded by YouTube videos and angry tweets, the threshold of intervention has dropped even lower. All it took to get the U.S. State Department to ask Twitter to put off their maintenance was a high number of tweets of highly dubious provenance. When the whole world expects us to react immediately—and the tweets are piling up in the diplomats’ in-boxes—we are not likely to rely on history, or even our own experiences and earlier mistakes, but instead decide that tweets + young Iranians holding mobile phones = a Twitter Revolution. William Scheuerman, a political theorist who studies the role of speed in international affairs, is right to worry that “the historical amnesia engendered by a speed-obsessed society invites propagandistic and fictional retellings of the past, where political history is simply recounted to the direct advantage of presently dominant political and economic groups.” Apparently, it’s also fictional retellings of the most recent present that a speed-obsessed society should be concerned about. When facts no longer shape their reactions, policymakers are likely to produce wrong responses. The viral aspect of today’s Internet culture is hardly exerting a positive influence on diplomats’ ability to think clearly. Back in the 1990s, many pundits and policymakers liked to denigrate (and a select few worship) the so-called “CNN effect,” referring to the power of modern media to exert pressure on decision makers by streaming images from the scene of a conflict, eventually forcing them to make decisions they may not have otherwise made. CNN’s supposed—but mostly unproven—influence on foreign policy in the 1990s could at least be justified by the fact that it was speaking on behalf of some idealistic and even humanistic position; we knew who was behind CNN, and we knew what their (mostly liberal) biases were. The humanism of a bunch of Facebook groups is harder to verify. Who are these people, and what do they want? Why are they urging us to interfere or withdraw from a given conflict? Where the optimists see democratization of access, the realists may see the ultimate victory of special interests over agenda setting. Governments, of course, are not stupid. They are also taking advantage of this tremendous new opportunity to cover their own attempts to influence global public opinion in the cloth of vox populi, either directly or through the work of proxies. Take Megaphone, a technology developed by a private Israeli firm. It keeps track of various online polls and surveys, usually run by international newspapers and magazines, that ask their readers questions about the future of the Middle East, Palestine, the legitimacy of Israeli policies, etc. Whenever a new poll is found, the tool pings its users, urging them to head to a given URL and cast a pro-Israel vote. Similarly, the tool also offers to help mass-email articles favorable to Israel, with the objective of pushing such articles to the “most emailed” lists that are available on many newspaper websites. But it’s not only nimble guerilla-like Web experiments like Megaphone that are influencing global public opinion. The truth is that Russia and China have created their own CNNs, which aim to project their own take on the world news. Both have vibrant websites. As American and British news media are experimenting with paywalls to remain afloat, it’s government-owned English-language media from Russia and China that stand to benefit the most. They would even pay people to read them! For all intents and purposes, navigating the new “democratized” public spaces created by the Internet is extremely difficult. But it’s even more difficult to judge whether the segments that we happen to see are representative of the entire population. It’s never been easier to mistake a few extremely unrepresentative parts for the whole. This in part ex plains why our expectations about the transformative power of the Internet in authoritarian states are so inflated and skewed toward optimism: The people we usually hear from are those who are already on the frontlines of using new media to push for democratic change in authoritarian societies. Somehow, the Chinese bloggers who cover fashion, music, or pornography—even though those subjects are much more popular in the Chinese blogosphere than human rights or rule of law—never make it to congressional hearings in Washington. The media is not helping either. Assuming they speak good English, those blogging for the Muslim Brotherhood in Egypt may simply have no intention of helping BBC or CNN to produce yet another report about the power of the blogosphere. That’s why the only power Western media cover is usually secular, liberal, or pro-Western. Not surprisingly, they tell us what we wanted to hear all along: Bloggers are fighting for secularism, liberalism, and Western-style democracy. This is why so many Western politicians fall under the wrong impression that bloggers are natural allies, even harbingers, of democracy. “If it’s true that there are more bloggers per head of population in Iran than any other country in the world, that makes me optimistic about the future of Iran,” said then UK’s foreign minister, David Miliband, while visiting Google’s headquarters. Why this should be the case—given that Iran’s conservative bloggers, who are often more hard-line than the government and are anything but a force for democracy, equality, and justice, are a formidable and rapidly expanding force in the Iranian blogosphere—is unclear. Chances are that Miliband’s advisors simply never ventured beyond a handful of pro-Western Iranian blogs that dominate much of the media coverage of the country. It’s hard to say what Miliband would make of certain groups of Chinese nationalists who, when they’re not making anti-Western or anti-CNN videos, are busy translating books by Western philosophers like Leibniz and Husserl. Things get worse when Western policymakers start listening to bloggers in exile. Such bloggers often have a grudge against their home country and are thus conditioned to portray all domestic politics as an extension of their own struggle. Their livelihoods and careers often depend on important power brokers in Washington, London, and Brussels making certain assumptions about the Internet. Many of them have joined various new media NGOs or even created a few of their own; should the mainstream assumptions about the power of blogging shift, many of these newly created NGOs are likely to go under. Not surprisingly, people who get grants to harness the power of the Internet to fight dictators are not going to tell us that they are not succeeding. It’s as if we’ve produced a few million clones of Ahmed Chala - bi, that notoriously misinformed Iraqi exile who gave a highly inaccurate picture of Iraq to those who were willing to listen, and hired them to tell us how to fix their countries. Of course, the influence of exiles on foreign policy is a problem that most governments have had to deal with in the past, but bloggers, perhaps thanks to the inevitable comparisons to Soviet dissidents and the era of samizdat, are often not subjected to the level of scrutiny they deserve.

### No Democracy Impact

#### Democratic peace empirically false and fails due to backsliding

John J. Mearsheimer, R. Wendell Harrison Distinguished Service Professor of political science at the University of Chicago and co-director of the Program on International Security Policy, The Tragedy of Great Power Politics, 2001, pp. 367-368

As challenges to realism go, democratic peace theory is among the strongest. Still, it has serious problems that ultimately make it unconvincing. The theory’s proponents maintain that the available evidence shows that democracies do not fight other democracies. But other scholars who have examined the historical record dispute this claim. Perhaps the most telling evidence against the theory is Christopher Layne’s careful analysis of four crises in which rival democracies almost went to war with each other.14 When one looks at how the decision not to fight was reached in each case, the fact that both sides were democracies appears to have mattered little. There certainly is no evidence that the rival democracies had benign intentions toward each other. In fact, the outcome each time was largely determined by balance-of-power considerations. Another reason to doubt democratic peace theory is the problem of backsliding. No democracy can be sure that another democracy will not someday become an authoritarian state, in which case the remaining democracy would no longer be safe and secure.15 Prudence dictates that democracies prepare for that eventuality, which means striving to have as much power as possible just in case a friendly neighbor turns into the neighborhood bully. But even if one rejects these criticisms and embraces democratic peace theory, it is still unlikely that all the great powers in the system will become democratic and stay that way over the long term. It would only take a non-democratic China or Russia to keep power politics in play, and both of those states are likely to be non-democratic for at least part of the twenty-first century.16

#### More empirical examples disprove DPT.

Nisley 8 (Thomas Jay Nisley, Prof. of International Studies, Southern Polytechnic State University, “The Pugnacious and the Pacific: Why Some Democracies Fight Wars” International Politics (2008) 45, 168–181)

There is a clear and sharp difference in the use of international violence among democracies. When examining the involvement in militarized interstates disputes (defined as use of force or war) among the continuously democratic states between the years 1950 and 2001, an interesting finding emerges. 'Of the 283 discrete involvements by these stable democracies, just four countries carried out 75.6% of these (19% of the whole group): Israel, the United States, India, and the United Kingdom' ([Müller, 2004](http://www.palgrave-journals.com/ip/journal/v45/n2/full/8800225a.html#bib25), 495). These four states accounted for 214 of the militarized interstate disputes over the period of observation. In contrast, the remaining 18 states only accounted for 69 militarized interstate disputes with three states (Luxemburg, Finland, and Austria) not having engaged in a single militarized interstate dispute during the 51-year period. A likely counter argument is that small states have little chance to get involved militarily. However, in an age of coalition warfare, military involvement by small states is relatively easy as they can join with larger states as they project power. President Bush's 'coalition of the willing' included many small states such as El Salvador and the Dominican Republic in the military involvement in Iraq. How do we make sense of this discrepancy in the pugnacity of democracies? To get to the heart of Müller's explanation, we must look at the identified causes of the democratic peace and Müller's evaluation of these explanations.

### Data Localization Take-outs

#### Surveillance is a proxy for larger disputes with US internet hegemony – and the alt causes matter more

**Hill 14\*** Technology policy consultant at Monitor 360, fellow of the Global Governance Futures 2025 program at the Brookings Institution (Jonah, “THE GROWTH OF DATA LOCALIZATION POST-SNOWDEN: ANALYSIS AND RECOMMENDATIONS FOR U.S. POLICYMAKERS AND BUSINESS LEADERS” p.19-20)//GK

Upon first glance, the preceding case studies present a consistent narrative: for the nations now considering localization for data, the Snowden revelations exposed an NSA that had overstepped the boundaries of acceptable surveillance, violated citizen privacy, and catalyzed public and government opinion in favor of forceful action in response. For policymakers, data localization offers a seemingly simple and effective solution. Under closer examination, however, a more complicated picture emerges. The localization movement is in fact a complex and multilayered phenomenon, with the objective not only—or even primarily—of protecting privacy. Depending on the country in which it is being advanced, localization also serves to protect domestic businesses from foreign competition, to support domestic intelligence and law enforcement ambitions, to suppress dissent and to stir up populist enthusiasms for narrow political ends. Direct evidence of these other objectives for which privacy seems to be a pretext is by its nature difficult to uncover: rarely to policy-makers admit to seeking protectionist goals, to spying on their populations, to suppressing dissent or to exploiting populist emotions. Yet, by viewing the localization movement in the context of other state and corporate interests and activities, it is possible to uncover these other, less exalted ends. Powerful business interests undoubtedly see data localization as an effective and convenient strategy for gaining a competitive advantage in domestic IT markets long dominated by U.S. tech firms. To localization proponents of this stripe, the NSA programs serve as a powerful and politically expedient excuse to pursue policies protective of domestic businesses. As an illustration, data localization in Germany presents clear economic benefits for a most powerful industry advocate for localization, Deutsche Telekom (DT). Whether by way of its “email made in Germany” system or the Schengen area routing arrangement, DT looks poised to gain from efforts to reduce the prominence of American tech firms in Europe. It is no wonder that the company has been spearheading many of the localization proposals in that country. As telecommunications law expert Susan Crawford has noted, DT has been seeking to expand its cloud computing services for years, but has found its efforts to appeal to German consumers stifled by competition from Google and other American firms. 79 T-Systems International GmbH, DT’s 29,000-employee distribution arm for information-technology solutions, has been steadily losing money as a result.80 Moreover, Crawford suggests that DT would not be content with gaining a greater share of the German market; she points out that through a Schengen routing scheme, “Deutsche Telekom undoubtedly thinks that it will be able to collect fees from network operators in other countries that want their customers’ data to reach Deutsche Telekom’s customers.”81 Similarly, companies and their allies in government in Brazil and India look to profit from data localization proposals. Indeed, the governments of both nations have for years sought to cultivate their own domestic information technology sectors, at times by protecting homegrown industries with import tariffs and preferential taxation. Brazilian President Rousseff has on numerous occasions stated that her government intends to make Brazil a regional technology and innovation leader; in recent years the government has proposed measures to increase domestic Internet bandwidth production, expand international Internet connectivity, encourage domestic content production, and promote the use of domestically produced network equipment.82 India, more controversially, has at times required foreign corporations to enter into joint ventures to sell e- commerce products, and has compelled foreign companies to transfer proprietary technology to domestic firms after a predetermined amount of time.83 Brazil and India are, of course, not alone in this respect. Indonesian firms are constructing domestic cloud service facilities with the help of government grants, 84 while Korea is offering similar support to its own firms. For the governments and corporations of these nations, long frustrated by their inability to develop a domestic IT industry that can compete on an even playing field with the U.S. technology giants, data localization is one means to confront, and perhaps overcome, the American Internet hegemony. 85

#### No risk of data localization – encryption solves mistrust.

Otto 14 (Greg Otto, Tech Reporter at FedScoop, Can encryption stop the 'balkanizing' of the Internet?” FedScoop, 26 September 2014, <http://fedscoop.com/encryption-internet-data-localization/>, *\*fc*)

Mulvenon later said he believes trust will be restored when encryption eventually becomes standard for the majority of Internet users. "The basis for trust in my daily life is robust, transparent encryption," he said. "But it also has to be easy enough for my mother to use. It can't be that you can only be a crypto-paranoid if you run GPG on the command line. It has to be something that is baked in to a basic level of what we are doing." Even with countries and companies wringing their hands over how data moves across borders, U.S. Coordinator for International Communications & Information Policy Daniel Sepulveda doesn't see the Internet fragmenting into something different than what it is today. "At the end of the day, there is literally not a country that has chosen to not connect to the global Internet," Sepulveda said. "There is a discussion by some politicians in some countries about constructing intranets inside their country and disassociating themselves from the global internet. That is actually not happening."

#### Localization is driven by the desire for surveillance and freedom from American dependence

**Hill 14\*** Technology policy consultant at Monitor 360, fellow of the Global Governance Futures 2025 program at the Brookings Institution (Jonah, “THE GROWTH OF DATA LOCALIZATION POST-SNOWDEN: ANALYSIS AND RECOMMENDATIONS FOR U.S. POLICYMAKERS AND BUSINESS LEADERS” p.21-22)//GK

If a government already has a sophisticated communications surveillance capacity, it would not be surprising that that it would want to enhance that capacity – certainly, that is what the United States has done. It would seem naïve to suppose that other governments would act differently. Data localization in both German and India and elsewhere, would offer just such enhancement, through two important intelligence functions. First, it allows domestic intelligence agencies to better monitor domestic data by either forcing data to be stored in local servers (indeed, India has previously required two international firms, Research in Motion and Nokia, to locate servers and data domestically91 for intelligence collection purposes), or by requiring that data to be held by local firms over which domestic intelligence and law enforcement agencies may have greater coercive power. Second, in light of the often-overlooked fact that many intelligence services, such as the BND, cooperate with the NSA in a variety of information sharing programs,92 governments may view localization as a tactic to gain additional bargaining power with the NSA in negotiations over how much information the American spy agency will share.93 Moreover, domestic law enforcement agencies (to the extent that, in most democratic countries, law enforcement is administratively and actually separate from intelligence services) surely have reason to view data localization as a potentially valuable evidence gathering tool, useful in identifying and then prosecuting conventional criminal activities. In connection with investigations and prosecutions, foreign law enforcement often complain that the process by which they request data from U.S. firms (the rules of which are generally negotiated between the United States and foreign governments and then ratified in a Mutual Legal Assistance Treaty) is slow and cumbersome, and that American firms and the U.S. Justice Department are too often uncooperative. The President’s Review Group on Intelligence and Communication Technologies estimated that the average time from request to delivery is 10 months, and sometimes years pass before a response arrives.94 There is uncertainty about when data can be shared, with whom, and on what terms; and it all happens with very little transparency.95 This process presents annoying and seemingly unjustified interference to foreign law enforcement officials who want to apprehend criminals. The Brazilian government, for example, has requested information from Google for several pending cases in the Brazilian Supreme Court, but has yet to receive it.96 Similarly, India has often asked the U.S. to serve summonses upon Google, as well as on Facebook, Twitter, and others, for failing to prevent the dissemination of speech prohibited under Indian Law, but has been rejected due to U.S. civil liberties sensibilities.97 Data localization, for frustrated and impatient law enforcement agencies and their political allies, looks like a straightforward mechanism to free themselves from some of this bothersome dependence on Americans.

#### Data localization is motivated by external factors – surveillance is only a public excuse

**Hill 14** - technology and international affairs consultant, formerly worked in the Office of the Cybersecurity Coordinator on the National Security Staff at the White House (Jonah, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders”, Conference on the Future of Cyber Governance, 5/1/14)//DBI

The problem for U.S. tech companies is that there are actually a wide variety of forces and interest groups driving the data localization movement, and many of these forces and groups have objectives beyond the professed goals of data protection and counter-NSA surveillance. One can easily discern in foreign governments’ interest in data localization a combination of anti-American populism, a desire for greater ease of foreign (and domestic) surveillance, and a sense among policymakers and business that the Snowden backlash presents an opportunity to cultivate domestic cloud and other tech services industries, industries that have long been outcompeted by American tech companies in their home markets—old-fashioned protectionism tailored for the digital age.

### No Economy Impact

#### All events prove *market resiliency*- it proved our safety nets work

Geewax 7/8— national economics correspondent for NPR website (Marilyn, “A Day Filled With Market Jitters, But Not Panic,” NPR, JULY 08, 2015, <http://www.npr.org/sections/thetwo-way/2015/07/08/421223972/a-day-filled-with-market-jitters-but-not-panic>). WM

If you were looking for reasons to be nervous, Wednesday provided lots of them, like these: — Chinese stocks plunged again, with the Shanghai Composite Index falling another 5.9 percent. — The Greek debt crisis remained unresolved, with European officials still scrambling for a solution. — Many raw-material prices continued their slide — with the Bloomberg Commodity Index down 26 percent from last year. And then came a thunderbolt. A "technical issue" forced the shutdown of the New York Stock Exchange (NYSE) for most of the day. The world's largest stock exchange stood silent from 11:32 a.m. until 3:10 p.m. ET. NYSE officials said they needed the downtime to untangle a malfunction of some sort. Despite this daunting collection of financial-market problems, optimists could take heart: Investors did not panic. In the end, it was a tough day, but not a disastrous one. By the 4 p.m. closing bell, the NYSE was returning to normal. The Dow Jones Industrial Average closed down about 261 to 17,515, and while that's lousy, it was no stampede. Analysts generally attributed the NYSE's calm close to the market redundancies that allowed traders to do business. Investors were not trapped. They could continue buying and selling shares via NASDAQ or BATS or dozens of other exchanges and private trading venues. So you could recap events this way: Wednesday ended up being a good day because, even with disruptions and fears, free markets functioned around the world. Yes, Chinese stocks were dropping, but the recent plunge is no surprise after a super-fast run up over the past year. And even though the Greek situation is awful, it is not generating panic outside of Greece. In fact, the rest of the eurozone is seeing many economic indicators turning up. And even without the NYSE functioning, investors had the freedom to continue going about their business. So maybe we are actually seeing a world that is becoming more stable, thanks to trading-platform redundancies. And after learning from the financial crisis of 2008-09, central bankers and regulators everywhere are better equipped to roll with the disruptions related to Greek debt and Chinese stocks. Bottom line: good for us. While there are serious trouble spots and plenty of pain for some individuals, the overall global financial markets are more stable and mature. Or you could recap the day this way: yikes! Just because we haven't seen panic yet, the planet is piling up lots of oily rags and kindling. Sooner or later, a spark could be struck somewhere, starting a global bonfire and melting down asset prices. No matter what happens, some day, economic historians will be able to look back and see clearly where we were heading. For now, let's just say these are interesting times.

#### Economic decline doesn’t cause war

Robert Jervis, Professor of International Politics in the Department of Political Science at Columbia University, 2011

(Force in Our Times, Saltzman Working Paper No. 15, July 2011, http://www.siwps.com/news.attachment/saltzmanworkingpaper15-842/SaltzmanWorkingPaper15.PDF)

Even if war is still seen as evil, the security community could be dissolved if severe conflicts of interest were to arise. Could the more peaceful world generate new interests that would bring the members of the community into sharp disputes? 45 A zero-sum sense of status would be one example, perhaps linked to a steep rise in nationalism. More likely would be a worsening of the current economic difficulties, which could itself produce greater nationalism, undermine democracy, and bring back old-fashioned beggar-thy-neighbor economic policies. While these dangers are real, it is hard to believe that the conflicts could be great enough to lead the members of the community to contemplate fighting each other. It is not so much that economic interdependence has proceeded to the point where it could not be reversed – states that were more internally interdependent than anything seen internationally have fought bloody civil wars. Rather it is that even if the more extreme versions of free trade and economic liberalism become discredited, it is hard to see how without building on a pre-existing high level of political conflict leaders and mass opinion would come to believe that their countries could prosper by impoverishing or even attacking others. Is it possible that problems will not only become severe, but that people will entertain the thought that they have to be solved by war? While a pessimist could note that this argument does not appear as outlandish as it did before the financial crisis, an optimist could reply (correctly, in my view) that the very fact that we have seen such a sharp economic down-turn without anyone suggesting that force of arms is the solution shows that even if bad times bring about greater economic conflict, it will not make war thinkable.

##

## Tech Leadership Advantage Answers

### Tech leadership Take-outs

#### Chinese technological leadership inevitable – not possible for the US to reclaim

Sharif 15 – Associate Professor in the Division of Social Science at the Hong Kong University of Science and Technology (Naubahar, Global Technology Leadership: The Case of China, Hong Kong University of Science and Technology Institute for Emerging Market Studies, February, http://iems.ust.hk/wp-content/uploads/2015/02/IEMSWP2015-11.pdf)//JJ

However, such skepticism overlooks several important factors that have positioned China to compete for global technological leadership. We see three distinct sources of competitive advantage that we believe China will leverage in developing its capacity for technological innovation. One of these factors — a large and rapidly growing domestic market — is no secret, while the other two — a firm government hand in industrial policy and globalization — complement the first factor, market size, in providing China with a path to global technological leadership. China’s rapidly growing domestic market — now the second largest in the world — will continue to grow and is likely to surpass the US market around 2020. As market size is an important determinant of innovation activities, burgeoning demand will drive Chinese companies to continuously advance their technological capabilities to profit from successful innovation, providing a global advantage such as no other economy enjoys. In spite of China’s openness to market forces, however, Beijing’s autocratic system of governance largely persists, providing ample room for the Chinese government to enact and implement industrial and innovation policy to enhance the technological capabilities of Chinese companies to an extent that mature Western market - oriented economies and democratic governments cannot match. This represents the second advantage we discuss here. Able to enact policy facing little or no opposition, Beijing can steer economic development as it sees fit. Benefiting from 7 China’s so - called ‘indigenous innovation’ strategy, Chinese companies enjoy government support of R&D, enabling them to develop technologies independently and to own intellectual property rights. Large - scale government grants and low - interest loans from state - owned banks under the framework of the indigenous innovation strategy provide Chinese firms with strong incentives to become global technological leaders. Finally, intensified globalization will continue to benefit Chinese companies in the coming decades, providing a third advantage in its drive to become a worldwide force in technology. On the one hand, Chinese firms need not develop every advanced technology on their own in a globalized world. Backed by the government’s ‘goglobal’ strategy, they can acquire such technologies through mergers and acquisitions abroad. On the other hand, as the economy grows and indigenous companies move up the technological ladder, foreign multinational corporations will be increasingly tempted, or perhaps feel compelled, to bring their advanced products to China, eventually even patenting their cutting - edge techno ogies there. This will in turn generate demonstration, labor mobility, and competition effects — or ‘spillovers’ — to benefit local firms. With all these opportunities looming on the horizon, Chinese companies are sparing no effort to seize them in an effort to possibly assume global leadership in technology and innovation. After tracing the trajectory of global technological leadership as indicated in the economics and innovation literature, we subsequently consider each of the three factors we have identified as competitive advantages for China — market size, governmental power, and globalization — in greater depth.

#### Alt causes to decreasing military primacy – defense cuts, foolish spending, and bad planning.

Forbes and Colby 14 (J. Randy Forbes, Chairman of the Seapower and Projection Forces Subcommittee of the House Armed Services Committee, and Elbridge Colby, Senior Fellow at the Center for a New American Security, “We're Losing Our Military Edge Over China. Here's How to Get It Back,” The National Interest, March 27 2014, <http://nationalinterest.org/commentary/were-losing-our-military-edge-over-china-heres-how-get-it-ba-10134>, \*fc)

While China’s buildup is a leading reason for this challenge to our military superiority, it is not the only one. Rather, we also find ourselves at this juncture through a combination of a foolishly constricting approaches to defense planning manifested by five years of defense cuts, including sequestration; a two-decade sanguinity about the true challenge to our military edge posed by China’s impressive military modernization; and, a refusal to ensure that our capabilities within the U.S. defense portfolio are militarily sufficient in quantity and diversity to maintain asymmetric superiority for full-spectrum warfare. Together, this lack of focus and indiscipline has helped allow countries like China to begin materially closing the once-yawning gap in military capability.

### No Hege Impact

#### Hege doesn’t solve war – no real threats, can’t solve irrational actors, and no credibility

Friedman, et al, ’13. Benjamin H. Friedman is a Research Fellow in Defense and Homeland Security Studies at the Cato Insti- tute. Brendan Rittenhouse Green is the Stanley Kaplan Postdoctoral Fellow in Political Science and Leader- ship Studies at Williams College. Justin Logan is Director of Foreign Policy Studies at the Cato Institute. “Debating American Engagement: The Future of U.S. Grand Strategy.” International Security, Volume 38, Number 2, Fall 2013, pp. 181-199 (Article). http://muse.jhu.edu/login?auth=0&type=summary&url=/journals/international\_security/v038/38.2.craig.html – clawan.

Brooks et al.’s case, however, is flawed. We dissect it in three parts. First, we show that primacy is unlikely to produce the main security benefit they ascribe to it: dimin- ished third-party security competition. Second, Brooks et al. understate primacy’s danger—specifically, its tendency to lead the United States into imprudent wars. Third, they misunderstand primacy’s nonsecurity consequences. the questionable security benefits of primacy Brooks et al. argue that the specter of U.S. power eliminates some of the most baleful consequences of anarchy, producing a more peaceful world. U.S. security guarantees deter aggressors, reassure allies, and dampen security dilemmas (p. 34). “By supplying reassurance, deterrence, and active management,” Brooks et al. write, primacy “re- duces security competition and does so in a way that slows the diffusion of power away from the United States” (pp. 39–40). There are three reasons to reject this logic: security competition is declining anyway; if competition increases, primacy will have difficulty stopping it; and even if competition occurred, it would pose little threat to the United States. an increasingly peaceful world. An array of research, some of which Brooks et al. cite, indicates that factors other than U.S. power are diminishing interstate war and se- curity competition.2 These factors combine to make the costs of military aggression very high, and its benefits low.3 A major reason for peace is that conquest has grown more costly. Nuclear weapons make it nearly suicidal in some cases.4 Asia, the region where future great power com- petition is most likely, has a “geography of peace”: its maritime and mountainous regions are formidable barriers to conflict.5 Conquest also yields lower economic returns than in the past. Post-industrial econo- mies that rely heavily on human capital and information are more difficult to exploit.6 Communications and transport technologies aid nationalism and other identity politics that make foreigners harder to manage. The lowering of trade barriers limits the returns from their forcible opening.7 Although states are slow learners, they increasingly appreciate these trends. That should not surprise structural realists. Through two world wars, the international sys- tem “selected against” hyperaggressive states and demonstrated even to victors the costs of major war. Others adapt to the changed calculus of military aggression through socialization.8 managing revisionist states. Brooks et al. caution against betting on these positive trends. They worry that if states behave the way offensive realism predicts, then secu- rity competition will be fierce even if its costs are high. Or, if nonsecurity preferences such as prestige, status, or glory motivate states, even secure states may become ag- gressive (pp. 36–37).9 These scenarios, however, are a bigger problem for primacy than for restraint. Offen- sive realist security paranoia stems from states’ uncertainty about intentions; such states see alliances as temporary expedients of last resort, and U.S. military commit- ments are unlikely to comfort or deter them.10 Nonsecurity preferences are, by defini- tion, resistant to the security blandishments that the United States can offer under primacy. Brooks et al.’s revisionist actors are unlikely to find additional costs sufficient reason to hold back, or the threat of those costs to be particularly credible. The literature that Brooks et al. cite in arguing that the United States restrains allies actually suggests that offensive realist and prestige-oriented states will be the most re- sistant to the restraining effects of U.S. power. These studies suggest that it is most difficult for strong states to prevent conflict between weaker allies and their rivals when the restraining state is defending nonvital interests; when potential adversaries and allies have other alignment options;11 when the stronger state struggles to mobilize power domestically12; when the stronger state perceives reputational costs for non- involvement;13 and when allies have hawkish interests and the stronger state has only moderately dovish interests.14 In other words, the cases where it would be most important to restrain U.S. allies are those in which Washington’s efforts at restraint would be least effective. Highly moti- vated actors, by definition, have strong hawkish interests. Primacy puts limits on U.S. dovishness, lest its commitments lack the credibility to deter or reassure. Such credibil- ity concerns create perceived reputational costs for restraining or not bailing out allies. The United States will be defending secondary interests, which will create domestic ob- stacles to mobilizing power. U.S. allies have other alliance options, especially in Asia. In short, if states are insensitive to the factors incentivizing peace, then the United States’ ability to manage global security will be doubtful. Third-party security competition will likely ensue anyway. costs for whom? Fortunately, foreign security competition poses little risk to the United States. Its wealth and geography create natural security. Historically, the only threats to U.S. sovereignty, territorial integrity, safety, or power position have been po- tential regional hegemons that could mobilize their resources to project political and military power into the Western Hemisphere. Nazi Germany and the Soviet Union ar- guably posed such threats. None exist today. Brooks et al. argue that “China’s rise puts the possibility of its attaining regional he- gemony on the table, at least in the medium to long term” (p. 38). That possibility is re- mote, even assuming that China sustains its rapid wealth creation. Regional hegemony requires China to develop the capacity to conquer Asia’s other regional powers. India lies across the Himalayas and has nuclear weapons. Japan is across a sea and has the wealth to quickly build up its military and develop nuclear weapons. A disengaged United States would have ample warning and time to form alliances or regenerate forces before China realizes such vast ambitions.

#### There’s no correlation between hegemony and stability

Fettweis, ’10 [Christopher J. Fettweis, Assistant Professor of Political Science at Tulane University, “Threat and Anxiety in US Foreign Policy,” Survival, 52:2, 59-82, March 25th 2010, <http://dx.doi.org/10.1080/00396331003764603>]

One potential explanation for the growth of global peace can be dismissed fairly quickly: US actions do not seem to have contributed much. The limited evidence suggests that there is little reason to believe in the stabilising power of the US hegemon, and that there is no relation between the relative level of American activism and international stability. During the 1990s, the United States cut back on its defence spending fairly substantially. By 1998, the United States was spending $100 billion less on defence in real terms than it had in 1990, a 25% reduction.29 To internationalists, defence hawks and other believers in hegemonic stability, this irresponsible ‘peace dividend’ endangered both national and global security. ‘No serious analyst of American military capabilities’, argued neo-conservatives William Kristol and Robert Kagan in 1996, ‘doubts that the defense budget has been cut much too far to meet America’s responsibilities to itself and to world peace’.30 And yet the verdict from the 1990s is fairly plain: the world grew more peaceful while the United States cut its forces. No state seemed to believe that its security was endangered by a less-capable US military, or at least none took any action that would suggest such a belief. No militaries were enhanced to address power vacuums; no security dilemmas drove insecurity or arms races; no regional balancing occurred once the stabilising presence of the US military was diminished. The rest of the world acted as if the threat of international war was not a pressing concern, despite the reduction in US military capabilities. Most of all, the United States was no less safe. The incidence and magnitude of global conflict declined while the United States cut its military spending under President Bill Clinton, and kept declining as the George W. Bush administration ramped the spending back up. Complex statistical analysis is unnecessary to reach the conclusion that world peace and US military expenditure are unrelated.

####

## Solvency Answers

### SQ Protections Enough

#### Existing oversight checks NSA overreach

Cordero, 14- Carrie F. Cordero is the Director of National Security Studies at Georgetown University Law Center (“Fear vs. Facts: Exploring the Rules the NSA Operates Under” 6/13, <http://www.cato-unbound.org/2014/06/13/carrie-f-cordero/fear-vs-facts-exploring-rules-nsa-operates-under>

There is no doubt the Snowden disclosures have launched a debate that raises significant issues regarding the extent of U.S. government national security surveillance authorities and activities. And Julian Sanchez’s essay Snowden: Year One raises a number of these issues, including whether the surveillance is too broad, with too few limits and too little oversight. But an overarching theme of Sanchez’s essay is fear – and fear of what might be overshadows what actually is, or is even likely. Indeed, he suggests that by just “tweaking a few lines of code” the NSA’s significant capabilities could be misdirected from targeting valid counterterrorism suspects to Americans involved in the Tea Party or Occupy movements. So really, what would it take to turn NSA’s capabilities inward, to the dark corner of monitoring political activity and dissent? It turns out, quite a lot. So much, in fact, that after a considered review of the checks and balances in place, it may turn out to be not worth fearing much at all. First, a little history. Prior to 1978, NSA conducted surveillance activities for foreign intelligence purposes under Executive authority alone. In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA), which distinguished between surveillance that occurred here at home and that which occurred overseas. FISA requires that when electronic surveillance is conducted inside the United States, the government seek an order from the Foreign Intelligence Surveillance Court (FISC or the Court) based on probable cause. So, if the government wants to conduct surveillance targeting a foreign agent or foreign power here in the United States, it must obtain FISC approval to do so. By law, the Court may not issue an order targeting an American based solely on activities protected by the First Amendment to the Constitution. The Attorney General is required to report on the full range of activities that take place under FISA to four congressional committees: both the intelligence and judiciary committees in Congress. The law requires that the committees be “fully informed” twice each year. There have been a number of amendments to FISA over the years. In 1994, the statute was amended to require that physical searches for national security purposes conducted inside the United States also happen by an order from the FISC. The USA-PATRIOT Act of 2001 amended several provisions of FISA, one of which enabled better sharing of information between terrorism and criminal investigators. And in 2008, FISA was amended to provide a statutory framework for certain approvals by the Attorney General, Director of National Intelligence, and FISC regarding the targeting of non-U.S. persons reasonably believed to be outside the United States for foreign intelligence purposes, when the cooperation of a U.S. communications service provider is needed. So how do we know that this system of approvals is followed? Is the oversight over NSA’s activities meaningful, or “decorative,” as Sanchez suggests? It is worth exploring. Here is how oversight of the Section 702 surveillance works, as one example, since it has been the subject of a significant part of the debate of the past year. Section 702 was added to FISA by the FISA Amendments Act of 2008. It authorizes the NSA to acquire the communications, for foreign intelligence purposes, of non-U.S. persons reasonably believed to be outside the United States. These are persons with no Constitutional protections, and yet, because the acquisition requires the assistance of a U.S. electronic communications provider, there is an extensive approval and oversight process. There is a statutory framework. Specifically, the Attorney General and Director of National Intelligence jointly approve certifications. According to declassified documents, the certifications are topical, meaning, the way the statute is being implemented, the certifications are not so specific that they identify individual targets; but they are not so broad that they cover any and everything that might be foreign intelligence information. The certifications are filed with the FISC, along with targeting and minimization procedures. Targeting procedures are the rules by which NSA selects valid foreign intelligence targets for collection. Minimization procedures are rules by which NSA handles information concerning U.S. persons. The FISC has to approve these procedures. If it does not approve them, the government has to fix them. The Court reviews these procedures and processes annually. The Court can request a hearing with government witnesses (like senior intelligence officials, even the NSA Director, if the judge wanted or needed to hear from him personally) or additional information in order to aid in its decisionmaking process. Information about the 702 certifications is reported to the Congressional intelligence committees. Once the certifications are in effect, attorneys from the Department of Justice’s (DOJ) National Security Division and attorneys and civil liberties officials from the Office of the Director of National Intelligence (ODNI) review the NSA’s targeting decisions and compliance with the rules. They conduct reviews at least every 90 days. During that 90-day period, oversight personnel are in contact with NSA operational and compliance personnel. Compliance incidents can be discovered in one of at least two ways: the NSA can self-report them, which it does; or the DOJ and ODNI oversight personnel may discover them on their own. Sometimes the NSA does not report a compliance incident in the required timeframe. Then the time lag in reporting may become an additional compliance incident. The DOJ and ODNI compliance teams write up semi-annual reports describing the results of their reviews. The reports are approved by the Attorney General and Director of National Intelligence and provided to the FISC and to Congress. According to the one report that has been declassified so far, in August 2013, for a six-month period in 2012, the rate of error for the NSA’s compliance under Section 702 collection was .49% - less than half of one percent. If we subtract the compliance incidents that were actually delays in reporting, then the noncompliance rate falls to between .15-.25% - less than one quarter of one percent. Hardly an agency run amok.

#### Squo Congressional oversight prevents abuse and oversight reform is better than scaling back

**Cordero, 14** - Carrie F. Cordero is the Director of National Security Studies at Georgetown University Law Center (“Fear vs. Facts: Exploring the Rules the NSA Operates Under” 6/13, <http://www.cato-unbound.org/2014/06/13/carrie-f-cordero/fear-vs-facts-exploring-rules-nsa-operates-under>

Generally, however, Congressional committees charged with oversight of the Intelligence Community do their job. The Intelligence Committees of Congress have professional staff, often with deep experience in national security matters. The Committees conduct substantive hearings, although, due to the sensitive and operational nature of the topics discussed, often in classified session. Congressional staff also receive briefings. During the debate surrounding the passage of the FISA Amendments Act of 2008, many members of Congress and their staffs visited the NSA and received dozens of briefings regarding its details and subsequent implementation. Decorative? Returning to the question implicitly posed by Sanchez’s argument: what would it take to turn this system inside out? Most likely, it would take either a conspiracy of the highest order, or the complete incompetence of everyone involved in the process – from operators to leadership inside the Intelligence Community, from lawyers to senior officials at the Justice Department, from legal advisors to judges of the FISC, from staff to members of Congress. Here’s what happens in the real world: people make mistakes; technological implementation goes awry; bureaucracy gets in the way of getting down to the bottom line. The adequacy and rigor of Congressional oversight waxes and wanes based, at times, on the quality of the leadership of the various committees at any time. Government employees also sometimes do the wrong thing, such as the twelve cases in ten years that the NSA has explained to Congress, and then they are held accountable. Oversight and compliance systems sometimes fail, too, such as the delay in recognizing the problems in the technical implementation of the phone metadata program that was subsequently brought to the Court’s attention. These are all valid reasons to work on improving auditing, compliance, oversight and accountability mechanisms. They are not valid reasons for adopting reforms that would dramatically scale back important national security capabilities that keep the nation safe.

#### XO12333 has the same minimization procedures as FISA – no abuse

**Joel, 14 -**  Alexander W. Joel is the civil liberties protection officer for the Office of the Director of National Intelligence and reports directly to Director of National Intelligence James R. Clapper (“The Truth About Executive Order 12333” Politico, 8/18, http://www.politico.com/magazine/story/2014/08/the-truth-about-executive-order-12333-110121.html#.VYomBfl4pyg

Under EO 12333, intelligence agencies may collect, retain, and disseminate information about Americans “only in accordance with procedures … approved by the Attorney General … after consultation with the Director [of National Intelligence].” Tye noted that he is not familiar with the details of these procedures, but nonetheless said that Americans should be troubled by “the collection and storage of their communications” under the executive order. As the civil liberties protection officer for the director of national intelligence (DNI), I work with intelligence agencies on these procedures, and would like to describe how they safeguard privacy and civil liberties. But first I want to commend Tye for raising his concerns through the processes established for that purpose. Using those processes, he has been able to review his concerns with intelligence oversight bodies as well as with the public, all while continuing to protect classified information. At the outset, remember that FISA, with very limited exceptions, requires the government to seek an individualized court order before it can intentionally target a United States person anywhere in the world to collect the content of his or her communications. The FISA court must be satisfied, based on a probable cause standard, that the United States person target is an agent of a foreign power, or, as appropriate, an officer or employee of a foreign power. But even when the government targets foreign nationals overseas in response to valid foreign intelligence requirements, it will inevitably collect some communications about Americans. As the Privacy and Civil Liberties Oversight Board noted in its examination of Section 702 of FISA, “[t]he collection of communications to and from a target inevitably returns communications in which non-targets are on the other end, some of whom will be U.S. persons.” Indeed, when Congress first enacted FISA in 1978, it required the government to follow what are called “minimization procedures.” These procedures, which must be approved by the FISA court, restrict what the government can do with collected information about U.S. persons (such as for how long that information may be retained, and under what circumstances it may be shared). Similarly, EO 12333 requires procedures to minimize how an agency collects, retains or disseminates U.S. person information. These procedures must be approved by the attorney general, providing an important additional check. The National Security Agency’s procedures are reflected in documents such as United States Signals Intelligence Directive SP0018 (USSID 18), issued in 1993 and updated in 2011. These procedures generally provide that communications may not be retained for more than five years. In addition, NSA personnel may not use U.S. person “selection terms” (such as names, phone numbers or email addresses) to retrieve communications from its collection under EO 12333 without a finding by the attorney general that the U.S. person is an agent of a foreign power (or in other similarly narrow circumstances). And even if the NSA determines that information about an American constitutes foreign intelligence, it routinely uses a generic label like “U.S. Person 1” in intelligence reporting to safeguard the person’s identity. The underlying identity may be provided only in a very limited set of circumstances, such as if it’s necessary to understand the particular foreign intelligence being conveyed. Oversight is extensive and multi-layered. Executive branch oversight is provided internally at the NSA and by both the Department of Defense and the Office of the DNI by agency inspectors general, general counsels, compliance officers and privacy officers (including my office and the NSA’s new Civil Liberties and Privacy Office). The Department of Justice also provides oversight, as do the Privacy and Civil Liberties Oversight Board and the president’s Intelligence Oversight Board. In addition, Congress has the power to oversee, authorize and fund these activities.

#### The NSA collects a miniscule amount of info

**Dickerson, 15 -** Julie Dickerson is currently a 3L at Harvard Law School, and previously served as Senior Editor for the Harvard National Security Journal (“Meaningful Transparency: The Missing Numbers the NSA and FISC Should Reveal” Harvard National Security Journal, <http://harvardnsj.org/2015/02/meaningful-transparency-the-missing-numbers-the-nsa-and-fisc-should-reveal/>

Under § 702 of the USA-PATRIOT Act, the NSA uses information from U.S. electronic communication service providers to target non-Americans outside the United States for documented foreign intelligence purposes. The NSA collects more than 250 million internet communications under this power each year. While a large absolute number, it is unclear what percent of total internet communications these § 702 communications constitute. The NSA has revealed that the internet carries 1,826 Petabytes of information per day, the NSA touches 1.6% of that data in its foreign intelligence mission, and the NSA only selects 0.025% of that data for review. The net result is that NSA analysts look at a mere 0.00004% of the world’s traffic. These percentages of total data traffic, though indicative that the percent of § 702 communications collected is likely miniscule, do not map perfectly onto percentages of total communications.

### Not Enough

#### Plan doesn’t restore trust – too small, NSA hacking, and metadata exemptions

**Wheeler, 14** – PhD, independent journalist specializing in national security and civil liberties; former senior policy analyst at The Intercept (Marcy, “A Radical Proposal of Following the Law” 11/24,

https://www.emptywheel.net/2014/11/24/a-radical-proposal-of-following-the-law/

Mieke Eoyang, the Director of Third Way’s National Security Program, has what Ben Wittes bills as a “disruptive” idea: to make US law the exclusive means to conduct all surveillance involving US companies.

But reforming these programs doesn’t address another range of problems—those that relate to allegations of overseas collection from US companies without their cooperation.

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.

[snip]

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.

Now, I have nothing against this proposal. It seems necessary but wholly inadequate to restoring trust between the government and (some) Internet companies. Indeed, it represents what should have been the practice in any case.

Let me first take a detour and mention a few difficulties with this. First, while I suspect this might be workable for content collection, remember that the government was not just collecting content from Google and Yahoo overseas — they were also using their software to hack people. NSA is going to still want the authority to hack people using weaknesses in such software, such as it exists (and other software companies probably still are amenable to sharing those weaknesses). That points to the necessity to start talking about a legal regime for hacking as much as anything else — one that parallels what is going on with the FBI domestically.

Also, this idea would not cover the metadata collection from telecoms which are domestically covered by Section 215, which will surely increasingly involve cloud data that more closely parallels the data provided by FAA providers but that would be treated as EO 12333 overseas (because thus far metadata is still treated under the Third Party doctrine here). This extends to the Google and Yahoo metadata taken off switches overseas. So, such a solution would be either limited or (if and when courts domestically embrace a mosaic theory approach to data, including for national security applications) temporary, because some of the most revealing data is being handed over willingly by telecoms overseas.

And before we institute this, we ought to know why the government was stealing overseas anyway. Was it to get around already broadly defined FISA Amendments Act certifications, including a Foreign Government one that can and apparently has been used for other purposes? Was it to collect on Americans who otherwise couldn’t be picked up via a legitimate target? I’ve been told the government was stealing algorithms, as much as content. That raises real questions about whether it is proper for the government to demand that kind of proprietary analysis done by Internet companies, one that would also need to be resolved in any such law.

Finally, one other problem with this is the criminal counterpart, the fact that DOJ is demanding Microsoft respond to domestic warrants for content stored in Ireland. What will restore other countries’ trust — and therefore the international viability of these companies — is sovereignty, which is something the government has been assiduously chipping away at even in the criminal context. Thus, while a lot of intelligence people poo poo the notion of sovereignty in spying, until you solve that on the overt stuff, you’re still going to be killing your tech base. So again, this only solves part of the problem, and even since the Snowden leaks started, DOJ seems intent only to double down.

Moreover, I don’t think this is the sphere in which the response to NSA’s theft overseas will play out, it will be the technological sphere, at least in the near term. What no one within the National Security establishment wants to admit is how badly NSA already shat the bed by stealing Google’s data overseas. Google is a worthy technical adversary to NSA (which is not to say it’s not a voracious spy in its own right, serving its own needs). And it will take a lot — far more than simply agreeing to what should have been the practice in any case — to get Google to not treat the government as an technical adversary, at least insofar as protecting its own networks generally. That’s as it should be, frankly. If NSA can steal from Google, so can, in the medium term, China.

Google, Apple, and Facebook have the heft and resources that a lot of the countries reacting to the NSA disclosures don’t have. They also have an urgent market need to respond, or at least create a credible illusion of responding. Few in DC seem to get that yet. That the proposed solutions to the damage NSA did to Google are so modest (effectively throwing table scraps to a wounded lion) is, in my mind, evidence that the NatSec world doesn’t yet grasp how badly NSA’s hubris has already hurt the Agency.

#### The perception of illegality under international law prevents solvency

**Rubinstein and Hoboken 14** – \*Senior Fellow at the Information Law Institute (ILI) and NYU School of Law, AND \*\*Microsoft Research Fellow in the Information Law Institute at New York University, PhD from the University of Amsterdam (Ira and Joris Van, PRIVACY AND SECURITY IN THE CLOUD: SOME REALISM ABOUT TECHNICAL SOLUTIONS TO TRANSNATIONAL SURVEILLANCE IN THE POST- SNOWDEN ERA, 66 Maine L. Rev. 488, September 2014, [http://ssrn.com/abstract=2443604](http://ssrn.com/abstract%3D2443604))//JJ

If anything, the Snowden leaks clearly illustrate that global cloud service providers are facing a new class of threats from intelligence agencies across the world. The revelations are many and diverse in nature. This Article proposes that, from the perspective of the cloud industry, the threats can be generally distinguished in terms of front-door versus backdoor access to data and communications handled by cloud providers. Revelations of front-door access in the U.S. context include PRISM and the widely discussed telephone metadata program.13 The PRISM program is conducted on the basis of Section 702 of the FISA Amendments Act 2008 (FAA), under which the U.S. intelligence community has successfully gained access to data from U.S. cloud services related to non-U.S. persons reasonably believed to be outside the U.S.14 Under this program, the NSA gains access by demanding cloud and communication service providers hand over customer information and content, requiring annual certification, and with targeting and minimization procedures reviewed by the Foreign Intelligence Surveillance Court.15 What is most striking about these programs is the structural basis and scale on which access takes place. In addition, many have raised doubts about the statutory and constitutional basis of these programs under U.S., international, as well as foreign law.16 Observers and stakeholders from outside of the United States are especially troubled by the fact that Section 702 would clearly violate the Fourth Amendment if it were designed to intercept the communications of U.S. persons.17

### 702 Exclusivity Fails

#### 702 won’t solve perception – the problem is the programs 702 authorized

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.37, 2015, Hein Online)//JJ

As a matter of Section 702 and the interception of international content, PRISM and Upstream collection present global concerns. Neither program has yet to be 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, goes some way towards undermining international confidence in U.S. companies.

#### Section 702 limit doesn’t resolve perception problems – the primary fear is what 702 authorizes

**Granick, 13** – civil liberties director for the Center for Internet and Society at Stanford Law School (Jennifer, “REFORMING FISA: A CRITICAL LOOK AT THE WYDEN/UDALL PROPOSAL AND FOREIGN SURVEILLANCE” 9/30, http://cyberlaw.stanford.edu/publications/reforming-fisa-critical-look-wydenudall-proposal-and-foreign-surveillance

Rather than focus on section 215, I want to focus in this post on the bill’s proposed reforms to section 702 of the FISA Amendments Act, or FAA. This is the provision underlying the PRISM program—and its use to obtain the content of phone calls and Internet messages, which Glenn Greenwald revealed based on Edward Snowden’s documentation. There’s been less discussion of the problems with section 702 than of those with section 215, even as we’ve learned some worrisome things about the way the NSA uses this legal authority. The new bill would address some, but by no means all, of these problems. In my opinion, it needs to be broader. I. Bacgkround First, some legal and technological background is in order. Traditional FISA required the government to show probable cause that the target of the underlying foreign intelligence surveillance was an agent of a foreign power and would use the facilities at which the government planned to direct surveillance before conducting electronic surveillance. This probable cause requirement had the practical effect of limiting surveillance to communications to or from individuals who are reasonably believed to be working for another government or a terrorist group. In addition to the expansions created in 2001 by the USA PATRIOT Act (including section 215), section 702 of the FAA created a new source of authority for conducting warrantless electronic surveillance. If the Attorney General and the Director of National Intelligence certify that the purpose of the monitoring is to collect foreign intelligence information about any non­American individual or entity not known to be in the United States, the Foreign Intelligence Surveillance Court (FISC) can require companies to provide access to Americans’ international communications. The court does not approve the target or the facilities to be monitored, nor does it assess whether the government is doing enough to minimize the intrusion, correct for collection mistakes, and protect privacy. Once the court approves the certification, the government can issue top-secret directives to Internet companies like Google and Facebook to turn over calls, e-mails, video and voice chats, photos, voice­over IP calls (like Skype), and social networking information. Enter, PRISM. PRISM surveillance is technologically complicated, involving both the aforementioned directives demanding that companies turn over the contents of user Internet messages, as well as upstream surveillance conducted directly on the fiber optic cables carrying telecommunications and Internet traffic. Pulling the right stuff off the cables as it travels is a technological challenge. Reports suggest that one way the NSA has accomplished this surveillance is via the XKeyScore tool, which appears to copy and temporarily store almost everything that flows over the network, filter that traffic based on various selection criteria, and store the subset in different databases for longer periods of time. No one has yet identified the legal authority under which the NSA justifies XKeyScore. It cannot be the FAA because that law does not authorize copying everything, even for a short period of time. Leaving that question aside for now, I want to highlight several pernicious results of the FISA Amendments Act or FAA. Americans’ communications with targets overseas are subject to warrantless interception. Once those communications are collected, current rules allow the NSA to search the trove for U.S. person identifiers, which Wyden has referred to as the “back door searches loophole”. The non-U.S. targets include regular people, not just those who are agents of foreign powers. While analysts provide their foreign intelligence purpose when selecting the target, the rationale is just one short sentence. By untethering surveillance from facilities that the target uses, the FAA greatly increased the opportunity for the NSA to collect information about rather than just to or from the target. As an example, if I monitor a network for “Jennifer Granick” and Jennifer Granick uses that network, I’ll get her communications, and maybe some messages about her. If I can monitor any facility for “Jennifer Granick”, I’m going to pull only messages about, but not to or from her. II. The Wyden/Udall Proposal Enter the new bill. The fact sheet says the Intelligence Oversight and Surveillance Reform Act would reform section 702 to: Close the “back door searches” loophole; Prohibit the government from collecting communications that are “about the target”, in non-terrorism contexts; Strengthen the prohibition against “reverse targeting,” or targeting a foreigner in order to warrantlessly acquire the communications of an American who is known to be communicating with that foreigner; and Place stronger statutory limits on the use of unlawfully collected information. These are critical reforms. I would like to see the bill further include a higher standard of care with regards to ensuring that people inside the U.S. are not targeted. As Professor Christopher Sprigman and I argued in the New York Times, PRISM is designed to produce at least 51 percent confidence in a target’s “foreignness” — as John Oliver of “The Daily Show” put it, “a coin flip plus 1 percent.” In other words, 49 percent of the time the NSA may be acquiring information it is not allowed to have, even under the terrifyingly broad auspices of the FAA. More fundamentally, though, the Wyden/Udall bill does not fully address a fundamental problem with the FAA, which is that it authorizes surveillance of average citizens of other countries for reasons that are not necessarily related to the security of the United States. Senator Udall acknowledged in the press conference announcing the bill (at 30:17) that the NSA’s unfettered spying has had and will continue to have an adverse economic effect on U.S.-based businesses, and that this is one of the motivations behind the bill. Prohibiting “about the target” collection is one giant step forward. That would mean that non-targets outside the U.S. could not be subject to surveillance under this law just because they talk about a target, unless their conversation is related to terrorism. Depending on the details of the targeting and minimization procedures, if my British friend in London and I email about our dismay over the Kenya attacks, that would be fair game, but our conversation about the policies of Brazilian President Dilma Roussef would be off limits. However, targets still need not be agents of foreign powers so long as a significant purpose of the collection is foreign intelligence. Foreign intelligence is broad, and includes any information that “relates to” the conduct of U.S. foreign affairs. For example, DNI James Clapper affirmed that the U.S. collects information about economic and financial matters to “provide the United States and our allies early warning of international financial crises which could negatively impact the global economy … or to provide insight into other countries’ economic policy or behavior which could affect global markets.” Monitoring economic and financial matters is in the United States’ national interest. However, routine eavesdropping upon common foreigners to discover information about these matters is a bad idea. First, foreigners have privacy rights, too. Freedom from arbitrary interference with one’s privacy is part of the Universal Declaration of Human Rights. Next, this monitoring is detrimental to U.S. companies and to the United States’ long-term interests in promoting democratic ideals. As Sprigman and I argue, although it may be legal, unfettered U.S. spying on foreigners will cause serious collateral damage to America’s technology companies, to our Internet-fueled economy, and to human rights and democracy the world over. Since our Atlantic article on June 28th, and the disclosure that the NSA targeted both Petrobras and President Dilma Roussef, Brazil has announced that it will look into requiring Internet companies to store its citizens’ data locally, and take other steps that threaten to balkanize the global Internet. When Brazil takes these steps, it gives comfort and cover to authoritarian countries who will do the same, so that they can better censor, spy on, and control Internet access within their own borders.

#### Empirically – NSA over-collection is because of the FISC

**Sommer, 14** - The author is with ZwillGen PLLC in Washington, D.C.; a law firm that represented a telecomm provider against a FISA order (Jacob, “FISA Authority and Blanket Surveillance: A Gatekeeper Without Opposition” Litigation, Spring, Vol. 40 No. 3

<http://www.americanbar.org/publications/litigation_journal/2013-14/spring/fisa_authority_and_blanket_surveillance_gatekeeper_without_opposition.html>

The window left open in Keith seems to be closed. Similarly, the FISC has approved of the NSA’s “collect now, restrict searching later” approach to minimization. See In re Application of the F.B.I. for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, LEXIS 134786 (FISA Ct. Sept. 13, 2013). In other words, the FISC has found no constitutional or statutory impediment to the government “over collecting” data—so long as it does not intentionally collect wholly domestic communications and it has minimization procedures to restrict access. There is no indication that the government has used its surveillance powers improperly (except in a limited number of circumstances attributable to NSA employee misconduct), but the FISC has not taken a robust view of the Fourth Amendment.

### No modeling

#### Modeling is empirically false

**Edgar, 4/13/15** - visiting fellow at the Institute and adjunct professor of law at the Georgetown University Law Center (Timothy, “The Good News About Spying”

<https://www.foreignaffairs.com/articles/united-states/2015-04-13/good-news-about-spying>

Despite high hopes for a fresh start on civil liberties, during his first term in office, Obama ratified and even expanded the surveillance programs that began under former President George W. Bush. After NSA contractor Edward Snowden began revealing the agency’s spying programs to The Guardian in 2013, however, Obama responded with a clear change of direction. Without great fanfare, his administration has made changes that open up the practices of the United States intelligence community and protect privacy in the United States and beyond. The last year and a half has been the most significant period of reform for national security surveillance since Senator Frank Church led the charge against domestic spying in the late 1970s. In 2013, at Obama’s direction, the Office of the Director of National Intelligence (ODNI) established a website for the intelligence community, IC on the Record, where previously secret documents are posted for all to see. These are not decades-old files about Cold War spying, but recent slides used at recent NSA training sessions, accounts of illegal wiretapping after the 9/11 attacks, and what had been highly classified opinions issued by the Foreign Intelligence Surveillance Court about ongoing surveillance programs. Although many assume that all public knowledge of NSA spying programs came from Snowden’s leaks, many of the revelations in fact came from IC on the Record, including mistakes that led to the unconstitutional collection of U.S. citizens’ emails. Documents released though this portal total more than 4,500 pages—surpassing even the 3,710 pages collected and leaked by Snowden. The Obama administration has instituted other mechanisms, such as an annual surveillance transparency report, that will continue to provide fodder for journalists, privacy activists, and researchers. The transparency reforms may seem trivial to some. From the perspective of an intelligence community steeped in the need to protect sources and methods, however, they are deeply unsettling. At a Brown University forum, ODNI Civil Liberties Protection Officer Alexander Joel said, “The intelligence community is not designed and built for transparency. Our culture is around finding our adversaries’ secrets and keeping our own secrets secret.” Accordingly, until only a few years ago, the intelligence community resisted making even the most basic information public. The number of FISA court opinions released to the public between 1978 and 2013 can be counted on one hand. Beyond more transparency, Obama has also changed the rules for surveillance of foreigners. Until last year, privacy rules applied only to “U.S. persons.” But in January 2014, Obama issued Presidential Policy Directive 28 (PPD-28), ordering intelligence agencies to write detailed rules assuring that privacy protections would apply regardless of nationality. These rules, which came out in January 2015, mark the first set of guidelines for intelligence agencies ordered by a U.S. president—or any world leader—that explicitly protect foreign citizens’ personal information in the course of intelligence operations. Under the directive, the NSA can keep personal information in its databases for no more than five years. It must delete personal information from the intelligence reports it provides its customers unless that person’s identity is necessary to understand foreign intelligence—a basic rule once reserved only for Americans. The new rules also include restrictions on bulk collection of signals intelligence worldwide—the practice critics call “mass surveillance.” The NSA’s bulk collection programs may no longer be used for uncovering all types of diplomatic secrets, but will now be limited to six specific categories of serious national security threats. Finally, agencies are no longer allowed simply to “collect it all.” Under PPD-28, the NSA and other agencies may collect signals intelligence only after weighing the benefits against the risks to privacy or civil liberties, and they must now consider the privacy of everyone, not just U.S. citizens. This is the first time any U.S. government official will be able to cite a written presidential directive to object to an intelligence program on the basis that the intelligence it produces is not worth the costs to privacy of innocent foreign citizens. THOSE IN GLASS HOUSES Obama’s reforms make great strides toward transparency and protecting civil liberties, but they have been neither celebrated nor matched abroad. When Chancellor Angela Merkel of Germany found out she had been the target of American eavesdropping, her reaction was swift. “This is not done,” she said, as if scolding a naughty child. Many Germans cheered. They and other Europeans believe that their laws protect privacy better than U.S. laws. But that is only partly true: Although Europe has stronger regulations limiting what private companies (such as Google and Facebook) can do with personal data, citizens are granted comparatively little protection against surveillance by government agencies. European human rights law requires no court approval for intelligence surveillance of domestic targets, as U.S. law has since 1978. Similarly, European governments do not observe limits on electronic surveillance of non-citizens outside of their own territories, as the United States now does under Obama’s presidential policy directive. By blaming only the NSA for mass surveillance, the public and foreign leaders let other intelligence services off the hook. No wonder that some human rights organizations, including Privacy International and Big Brother Watch UK, have filed legal challenges against mass surveillance by the NSA’s British counterpart, the Government Communications Headquarters (GCHQ). But foreign leaders have taken few steps to limit government surveillance, and none have done anything remotely comparable to what Obama did in last year’s directive.

### Circumvention

#### Redundant capabilities from other agencies circumvent

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

The NSA might get the headlines, but the US intelligence community is actually composed of 17 different agencies. There’s the CIA, of course. You might have heard of the NRO—the National Reconnaissance Office—it’s in charge of the country’s spy satellites. Then there are the intelligence agencies associated with all four branches of the military. The Departments of Justice (both FBI and DEA), State, Energy, the Treasury, and Homeland Security all conduct surveillance, as do a few other agencies. And there may be a still-secret 18th agency. (It’s unlikely, but possible. The details of the NSA’s mission remained largely secret until the 1970s, over 20 years after its formation.) After the NSA, the FBI appears to be the most prolific government surveillance agency. It is tightly connected with the NSA, and the two share data, technologies, and legislative authorities. It’s easy to forget that the first Snowden document published by the Guardian—the order requiring Verizon to turn over the calling metadata for all of its customers—was an order by the FBI to turn the data over to the NSA. We know there is considerable sharing amongst the NSA, CIA, DEA, DIA, and DHS. An NSA program code-named ICREACH provides surveillance information to over 23 government agencies, including information about Americans.

#### Domestic constraints cause a foreign shift – turns the case

**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)

First, the United States, like many countries, concentrates much of its surveillance efforts abroad. Indeed, the Foreign Intelligence Surveillance Act is focused on gathering information overseas, limiting data gathering largely only when it implicates U.S. persons. n174 The recent NSA surveillance disclosures have revealed extensive foreign operations. n175 Indeed, constraints on domestic operations may well have spurred the NSA to expand operations abroad. As the Washington Post reports, "Intercepting communications overseas has clear advantages for the NSA, with looser restrictions and less oversight." n176 Deterred by a 2011 ruling by the Foreign Intelligence Surveillance Court barring certain broad domestic surveillance of Internet and telephone traffic, n177 the NSA may have increasingly turned its attention overseas.

#### Allied cooperation circumvents domestic restrictions

**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>

7. The NSA coordinates its spying closely with Intelligence agencies of the four other English-speaking countries that participate in "Five Finger" alliance: the UK, Canada, Australia and New Zealand. Their data sharing does not stop at that acquired by legal means. They do each other favors by relying on a partner to circumvent domestic restrictions in any one of them. There are credible reports that NSA has assisted Britain's GCHQ in this respect. Both have assisted the German NBD in spying on German targets- as has been revealed within the past few weeks. Therefore, the significance of last week legislation is undercut by this close collaboration.

#### Creative lawyering guarantees circumvention

**Redmond, 14** – J.D. Candidate, 2015, Fordham University School of Law (Valerie, “I Spy with My Not So Little Eye: A Comparison of Surveillance Law in the United States and New Zealand” FORDHAM INTERNATIONAL LAW JOURNAL [Vol. 37:733

In the United States, the current state of surveillance law is a product of FISA, its amendments, and its strictures. An evaluation of US surveillance law proves that inherent loopholes undercut FISA’s protections, which allows the US Government to circumvent privacy protections.182 The main problems are the insufficient definition of surveillance, the ability to spy on agents of foreign powers, the lack of protection against third party surveillance, and the ability to collect incidental information.183

First, a significant loophole arises in the interpretation of the term “surveillance.”184 In order for information collection to be regulated by FISA, it must fall under FISA’s definition of surveillance.185 This definition does not apply to certain National Security Letters, which are secret authorizations for the Federal Bureau of Investigation (“FBI”) to obtain records from telephone companies, credit agencies, and other organizations if they merely certify that the information is relevant to an international terrorism investigation.186 National Security Letters are regularly used to circumvent FISA’s warrant procedures.187 Additionally, FISA’s definition of surveillance is antiquated because it distinguishes between data acquired inside of the United States and outside of the United States.188 This distinction allows the NSA to process surveillance that is received from other countries irrespective of whether the target is a US citizen.189 Therefore, the NSA is unrestrained when a communication is not physically intercepted within the United States.190 Second, an issue arises when US citizens are construed to be agents of foreign powers under FISA because a warrant can be issued to engage in surveillance against them.191 According to FISA’s procedures, the only way to spy on a US citizen is when they can be considered to be an agent of a foreign power, or engaged in information gathering, aiding, or abetting a foreign power.192 However, this limitation does not result in total privacy protection because it only requires probable cause that a person is an agent of a foreign power, not that a crime is being committed.193 The effect of this ability is that the US Government can conduct surveillance on a US citizen with no ties to terrorism such as a suburban mother telling her friend that her son “bombed” a school play.194

#### Section 702 fails to limit domestic surveillance—legal loopholes and circumventions

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

For years, FISA and especially its s. 702 have been criticized for providing legal loopholes for warrantless political and economic surveillance on U.S. lawyers, NGOs, journalists and corporations communicating internationally through U.S. Internet companies [33]; the media reports in December 2005, around warrant-less wiretapping in bulk from the Internet backbone at an AT&T switch [28],have highlighted some of this tension. Nonetheless, U.S. Congress passed FAA after the AT&T revelations and extended the validity of the FAA for another five years on 31 December 2012, one day before the sunset deadline. Two months later, on 26 February 2013 in the case `Clapper v. Amnesty International', the U.S. Supreme Court denied several U.S. organizations a right to claim that the privacy of their international communications was violated by s. 702 on procedural grounds. In what appeared to be the final ruling on the constitutionality of s. 702 for the foreseeable future, a 5-4 majority argued that these organizations were merely `speculating', and could not prove that their communications had actually been intercepted [6]. Justice Breyer, on behalf of the minority, noted in his dissent that s. 702 prohibits the same applicants to actually gain knowledge of the surveillance itself because of national security secrecy, and that the broad authorities probably existed for a reason. The political debate and the issue of legal standing have shifted considerably since June 2013, when it became clear that s. 702 indeed serves as the legal basis for many operations, among them ‘UPSTREAM’ and ‘PRISM’ [13]. Moreover, several of the classified targeting and minimization procedures under s. 702 have been leaked or declassified [2, 3]. Both revelations have spurred the N.S.A. to confirm that a principle use of s. 702 is compelling assistance from U.S. Internet companies for warrantless surveillance [5, p. 4]. This new dynamic enables a unique insight into classified and generous interpretations of the legal provisions in FISA made by the intelligence community and the FISA Court [13]. Before we dive into the details of FISA, we mention that FISA also contains s. 703 and s. 704, that regulate surveillance intentionally targeting U.S. persons located abroad. These sections are outside the scope of this paper, since our focus is on surveillance operations on Americans located in the U.S., with surveillance conducted on foreign soil. As an aside, Donohue has observed that the warrant requirements in these sections have been circumvented by applying s. 702 criteria to the collection phase, and then seeing whether collected data is of use for further processing after the fact [13, p.26]. 2.2.2 Scope of the Second Regulatory Regime under FISA: The 1978 ‘Electronic Surveillance’ Definition All communications surveillance operations that constitute ‘electronic surveillance’, as defined s. 1801(f) of FISA, fall within the scope of FISA (cf. 18 U.S.C. s.2511(2)(f); 50 U.S.C. s.1812(a)). The definition has largely remained intact since 1978. To acquire the content of ‘wired communications’, surveillance only falls within the FISA definition when authorities ‘intentionally target a U.S. person’ (s. 1801(f)(1)), or when the acquisition is conducted on U.S. soil (s. 1801(f)(2)). Importantly, when authorities conduct targeted surveillance from abroad, even if they know that both ‘sender and all intended recipients are located in the U.S.’, then only ‘radio’ (i.e., wireless) communications fall within the FISA definition of ‘electronic surveillance’ (s. 1801(f)(3)). The FISA defi- nition only mentions communications ‘content’, but not ‘metadata’ (location, time, duration, identity of communicants, etc.), which in itself gives rise to privacy concerns that we will not further discuss here. Relevant for our purposes, is the observation that operations on ‘wired communications’, when conducted abroad, only fall within the scope of FISA if they ‘intentionally target a U.S. person’. Intentionally Targeting U.S. Persons. ‘Intentionally targeting a U.S. person’ constitutes ‘electronic surveillance’ under FISA (s. 1801(f)(1)). However, ‘intention’ and ‘targeting’ are not defined in FISA, leaving the concepts open to generous interpretation by authorities in classified ‘targeting’ and ‘minimization’ procedures. Apart from providing clarity that bulk surveillance is not regarded as intentional targeting (we discuss this further when we look at legal protections from U.S. persons under FISA), the disclosure of these procedures has revealed two important new facts related to surveillance operations conducted abroad. Firstly, conducting the surveillance abroad creates the presumption that the surveillance targets a non-U.S. person [2, p. 3-4]. Secondly, the ‘targeting procedures’ do not provide any due diligence requirement or duty of care to establish the identity of parties on either side of a communication [2, p.3-4] [3]. This implies that unless a communicant is known to be a U.S. person, the procedures consider the communicant to be a non-U.S. person. In other words, authorities have a strong incentive to conduct surveillance abroad: legal protections offered to U.S. persons under FISA can be circumvented, and a more generous legal regime applies to the data collection itself.