# Explanation/Guide

### File Description and General Tips

This file contains a disadvantage that can be read against both the Surveillance State Repeal Act affirmative and the Secure Data Act affirmative. It contains materials for both the negative and the affirmative.

When reading this disadvantage, the negative should introduce it as an off-case position in the 1NC. The 1NC shell is included in this file. To extend the disadvantage in the negative block, the negative should prepare blocks to each affirmative response. When doing so, the negative can make use of the backline evidence contained in the file. Students should carefully choose which extension evidence to read; it is very unlikely that students will be able to read *all* extension cards in any 2NC or 1NR.

When answering this disadvantage, the affirmative should use the 2AC frontline. It includes seven arguments. For each 2AC argument, the affirmative is provided with two extension cards that could be useful for the 1AR. Due to the intense time constraints of that speech, students should carefully choose which (if any) extension evidence to read.

If debating the Secure Data Act affirmative, both teams are provided with additional case-specific evidence. The affirmative should add the “no specific link” argument to the 2AC frontline. In response, the negative can read the appropriate encryption-specific links.

### Explanation of the Negative

The Terrorism DA argues that reducing surveillance limits the governments’ ability to track and detect terrorist plots before they occur. The negative argues that NSA and other intelligence agencies need all of the information they can possibly have to thwart terror attacks. Absent surveillance, they argue that there will be an increase in terrorism—including nuclear terrorism. In the 2NC or 1NR, the negative can also argue that the disadvantage turns the case — a terrorist attack would lead to increased surveillance in the future because people would be scared and feel like they need to do anything possible to stop another attack.

### Explanation of the Affirmative

The affirmative argues that NSA mass surveillance is useless in finding terrorists. Instead, they argue that mass surveillance leads to data overload — intelligence agencies can’t separate the good data from the bad because there’s just too much of it. Reducing surveillance would allow the NSA to focus on targeted surveillance, which the affirmative contends is more effective. The affirmative also argues that the risk of terrorism is low and exaggerated and that the USA Freedom Act should have caused the impact because it curtailed domestic surveillance.

# Negative

## 1NC

### 1NC — Terrorism DA

#### The first/next off-case position is the Terrorism DA.

#### First, the risk of terrorism is the highest since 9/11, but the U.S. is preventing immanent attacks with domestic surveillance.

Carafano et al. 15 — James Jay Carafano, Ph. D., Vice President for the Institute for National Security and Foreign Policy at the Heritage Foundation, former senior fellow at the Center for Strategic and Budgetary Assessments, a Washington policy institute dedicated to defense issues, Charles “Cully” Stimson, Senior Legal Fellow at the Institute for National Security and Foreign Policy at The Heritage Foundation, former Deputy Assistant Secretary of Defense for Detainee Affairs, Steven P. Bucci, Ph.D., Director of the Center for Foreign and National Security Policies at the Heritage Foundation, former Army Special Forces officer and top Pentagon official, former lead consultant to IBM on cyber security policy, John Malcolm, Director, Center for Legal and Judicial Studies at The Heritage Foundation, former deputy assistant attorney general in the Department of Justice’s Criminal Division, and Paul Rosenzweig, policy expert at The Heritage Foundation, 2015 ("Section 215 of the PATRIOT Act and Metadata Collection: Responsible Options for the Way Forward," Heritage Foundation, May 21st, Available Online at http://www.heritage.org/research/reports/2015/05/section-215-of-the-patriot-act-and-metadata-collection-responsible-options-for-the-way-forward, Accessed 08-08-2015)

Any debate about America’s counterterrorism capabilities must be conducted in the context of the actual terrorist threat the U.S. faces. Since 9/11, The Heritage Foundation has tracked Islamist terrorist plots and attacks, which now, after the recent shooting in Garland, Texas, total 68.[1] This figure, however, does not consider foiled plots of which the public is unaware.

Recently, there has been a dramatic uptick in terrorism: The shooting in Garland is the sixth Islamist terrorist plot or attack in the past five months. Add to that number the surge of Americans seeking to support or join ISIS and al-Qaeda affiliates, and one fact becomes clear: The U.S. is facing the most concentrated period of terrorist activity in the homeland since 9/11.

Of course, it is no coincidence that this spike in terrorism parallels the spread of the Islamic State and other radical groups across Syria, Iraq, and other parts of the Middle East. More than 150 American passport holders have traveled to Syria, or attempted to travel there, to join the fighting, along with more than 20,000 fighters from more than 90 countries.[2] Many of these individuals with American passports are believed to have joined ISIS or the Nusra Front, an affiliate of al-Qaeda in Syria.

Both the Nusra Front and ISIS espouse an anti-Western Islamist ideology that calls for terrorist attacks against the United States. For example, in July 2012, the leader of ISIS, self-proclaimed caliph Abu Bakr Baghdadi, threatened to launch attacks against the U.S. homeland. Baghdadi warned Americans, “You will soon witness how attacks will resound in the heart of your land, because our war with you has now started.”[3] Toward this end, al-Qaeda formed a unit of veteran terrorists to recruit some of the Western foreign fighters in Syria and train them to conduct terrorist attacks in their home countries. This unit, dubbed the Khorasan group by U.S. officials, is embedded in the Nusra Front and is particularly interested in recruiting fighters who hold American passports.[4]

These terrorist organizations have undertaken a significant effort to reach out to individuals across the world in order to radicalize and recruit them. In recent testimony before the Senate Appropriations Committee, FBI Director James Comey stated that:

The threats posed by foreign fighters, including those recruited from the U.S., traveling to join the Islamic State of Iraq and the Levant (ISIL) and from homegrown violent extremists are extremely dynamic. These threats remain the biggest priorities and challenges for the FBI, the U.S. Intelligence Community, and our foreign, state, and local partners. ISIL is relentless and ruthless in its pursuits to terrorize individuals in Syria and Iraq, including Westerners. We are concerned about the possibility of individuals in the U.S. being radicalized and recruited via the Internet and social media to join ISIL in Syria and Iraq and then return to the U.S. to commit terrorist acts. ISIL’s widespread reach through the Internet and social media is most concerning as the group has proven dangerously competent at employing such tools for its nefarious strategy.[5]

In the past several weeks, Director Comey has increased the intensity of his warnings, stating that “hundreds, maybe thousands” of individuals across the U.S. are being contacted by ISIS to attack the U.S. homeland.[6]

Secretary of Homeland Security Jeh Johnson has echoed these warnings, saying that lone-wolf terrorists inspired by ISIS could strike at any moment.”[7] The 2015 Worldwide Threat Assessment of the U.S. Intelligence Community states that:

Attacks by lone actors are among the most difficult to warn about because they offer few or no signatures. If ISIL were to substantially increase the priority it places on attacking the West rather than fighting to maintain and expand territorial control, then the group’s access to radicalized Westerners who have fought in Syria and Iraq would provide a pool of operatives who potentially have access to the United States and other Western countries.[8]

On the same note, the Director of the National Counterterrorism Center also stated in his testimony to the Senate Select Committee on Intelligence this February that there has been a recent “uptick in terror attacks in the West.” This increase in attacks “underscores the threat of emboldened Homegrown Violent Extremists and, how the rapid succession of these attacks may motivate some to attempt to replicate these tactics with little-to-no warning.”[9]

These statements and assessments, together with the explicit and public statements of intent by multiple terrorist groups and the recent surge in terrorist plots and attacks against the U.S. homeland, demonstrate that the threat of terrorism is on the rise. Fortunately, the U.S. has improved its ability to foil these attacks, largely due to intelligence capabilities that include but are not limited to the bulk telephone metadata program under Section 215 of the PATRIOT Act.

#### Second, reducing surveillance causes attacks — NSA is crucial.

McLaughlin 14 — John McLaughlin, Distinguished Practitioner-in-Residence at the Philip Merrill Center for Strategic Studies at Johns Hopkins University, serves on the Director of the Central Intelligence Agency’s External Advisory Board, formerly served as Deputy Director and Acting Director of the CIA, holds an M.A. in International Relations from the School of Advanced International Studies at Johns Hopkins University, 2014 (“NSA intelligence-gathering programs keep us safe,” *Washington Post*, January 2nd, Available Online at <http://www.washingtonpost.com/opinions/nsa-intelligence-gathering-programs-keep-us-safe/2014/01/02/0fd51b22-7173-11e3-8b3f-b1666705ca3b_story.html>, Accessed 04-20-2015)

It’s time we all came to our senses about the National Security Agency (NSA). If it is true, as many allege, that the United States went a little nuts in its all-out pursuit of al-Qaeda after the Sept. 11, 2001, attacks, it is equally true that we are going a little nuts again in our dogged pursuit of the post-Snowden NSA.

Those who advocate sharply limiting the agency’s activities ought to consider that its work is the very foundation of U.S. intelligence.

I don’t mean to diminish the role of other intelligence agencies, and I say this as a 30-year veteran of the Central Intelligence Agency who is “CIA” through and through. But in most cases, the NSA is the starting point for determining what holes need to be filled through other means of intelligence-collection. That’s because its information on foreign developments is so comprehensive and generally so reliable. It is the core of intelligence support to U.S. troops in battle. Any efforts to “rein in” the agency must allow for the possibility that change risks serious damage to U.S. security and the country’s ability to navigate in an increasingly uncertain world.

The presumption that the NSA “spies” on Americans should also be challenged. In my experience, NSA analysts err on the side of caution before touching any data having to do with U.S. citizens. In 2010, at the request of then-Director of National Intelligence Dennis Blair, I chaired a panel investigating the intelligence community’s failure to be aware of Umar Farouk Abdulmutallab, the “underwear bomber” who tried to blow up a commercial plane over Detroit on Dec. 25, 2009.

The overall report remains classified, but I can say that the government lost vital time because of the extraordinary care the NSA and others took in handling any data involving a “U.S. person.” (Abdulmutallab, a Nigerian, was recruited and trained by the late Anwar al-Awlaki, a U.S. citizen based in Yemen.)

Regarding outrage over the NSA’s collection of telephone calling records, or metadata, I don’t know why anyone would have greater confidence in this information being held by private companies. And given the perceived threat to privacy, it’s astonishing how little attention has been paid to the Senate commerce committee’s recent report on companies that gather personal information on hundreds of millions of Americans and sell it to marketers, often highlighting people with financial vulnerability. Some companies group the data into categories including “rural and barely making it,” “retiring on empty” and “credit crunched: city families.” The aim is often to sell financially risky products to transient consumers with low incomes, the report found.

That’s a real scandal — and a universe away from the NSA’s ethical standards and congressional oversight.

The NSA, of course, is not perfect. But it is less a victim of its actions — the independent commission appointed by President Obama found no illegality or abuses — than of the broad distrust of government that has taken root in the United States in recent decades. Studies by Pew and others show distrust of government around 80 percent, an all-time high.

This distrust is the only logical explanation I see for fear of data being held by “the government” — and it’s not a circumstance the NSA created.

Although our society lauds, in almost “Stepford Wives”-like fashion, the merits of “transparency,” it lacks a collective, mature understanding of how intelligence works, how it integrates with foreign policy and how it contributes to the national welfare. Meanwhile, prurient interest in the details of leaked intelligence skyrockets, and people devour material that is not evidence of abuse but merely fascinating — and even more fascinating to U.S. adversaries.

So what makes sense going forward? Clearly, the widespread perception that there is at least the “potential for abuse” when the government holds information even as limited as telephone call metadata must be addressed. The recent presidential commission recommended adding a public privacy advocate to the deliberation process of courts that approve warrants — one proposal that would do no harm. But as the administration contemplates reform, it must reject any ideas that add time and process between the moment the NSA picks up a lead overseas and the time it can cross-check records to determine whether there is a domestic dimension to overseas plotting.

As our debate continues, the terrorist threat is not receding but transforming. The core leadership of al-Qaeda has been degraded and remains under pressure, but robust al-Qaeda affiliates have multiplied. With the decline of central government authority in the Middle East and North Africa in the wake of the Arab Spring and the war in Syria, terrorists have the largest havens and areas for operational planning in a decade.

If anything, the atomization of the movement has made the job of intelligence more labor-intensive, more detail-oriented and more demanding. Now is not the time to give up any tool in the counterterrorism arsenal.

#### Third, strong NSA intelligence is critical to prevent WMD terror attacks including the use of nuclear weapons.

Pittenger 14 — US Representative Robert Pittenger, R-NC, chair of the Congressional Task Force on Terrorism, 2014 (“Bipartisan bill on NSA data collection protects both privacy and national security," Washington Examiner, June 9th, Available Online via the Wayback Machine at https://web.archive.org/web/20140709222125/http://washingtonexaminer.com/rep.-robert-pittenger-bipartisan-bill-on-nsa-data-collection-protects-both-privacy-and-national-security/article/2549456, Accessed 08-10-2015)

In that light, is there a need for continued NSA access to phone records, albeit only on a case-by-case basis?

This February, I took that question to a meeting of European Ambassadors at the Organization for Security and Cooperation in Europe. During the conference, I asked three questions:

1. What is the current worldwide terrorist threat?

2. What is America’s role in addressing and mitigating this threat?

3. What role does intelligence data collection play in this process, given the multiple platforms for attack including physical assets, cyber, chemical, biological, nuclear and the electric grid?

Each ambassador acknowledged the threat was greater today than before 9/11, with al Qaeda and other extreme Islamist terrorists stronger, more sophisticated, and having a dozen or more training camps throughout the Middle East and Africa.

As to the role of the United States, they felt our efforts were primary and essential for peace and security around the world.

Regarding the intelligence-gathering, their consensus was, “We want privacy, but we must have your intelligence.” As a European foreign minister stated to me, “Without U.S. intelligence, we are blind.”

We cannot yield to those loud but misguided voices who view the world as void of the deadly and destructive intentions of unrelenting terrorists. The number of terrorism-related deaths worldwide doubled between 2012 and 2013, jumping from 10,000 to 20,000 in just one year. Now is not the time to stand down.

Those who embrace an altruistic worldview should remember that vigilance and strength have deterred our enemies in the past. That same commitment is required today to defeat those who seek to destroy us and our way of life. We must make careful, prudent use of all available technology to counter their sophisticated operations if we are to maintain our freedom and liberties.

#### Finally, nuclear terrorism causes accidental U.S.-Russian nuclear war — each side will believe they’ve been attacked by the other.

Barrett et al. 13 — Anthony M. Barrett, Director of Research and Co-Founder of the Global Catastrophic Risk Institute, Ph.D. in Engineering and Public Policy from Carnegie Mellon University, former postdoctoral research associate at the National Center for Risk and Economic Analysis of Terrorism Events at the University of Southern California and former Fellow in the RAND Stanton Nuclear Security Fellows Program, Seth Baum, Ph.D., Co-Founder and Executive Director, Global Catastrophic Risk Institute, Affiliate Scholar, Institute for Ethics and Emerging Technologies, Research Scientist, Blue Marble Space Institute of Science, and Kelly R. Hostetler, BS in Political Science from Columbia, Research Associate at the Global Catastrophic Risk Institute, 2013 (“Analyzing and Reducing the Risks of Inadvertent Nuclear War Between the United States and Russia,” Science and Global Security, Vol. 21, No. 2, pages 106-133, Available Online at <http://sethbaum.com/ac/2013_NuclearWar.pdf>, Accessed 08-10-2015)

War involving significant fractions of the U.S. and Russian nuclear arsenals, which are by far the largest of any nations, could have globally catastrophic effects such as severely reducing food production for years,1 potentially leading to collapse of modern civilization worldwide and even the extinction of humanity.2 Nuclear war between the United States and Russia could occur by various routes, including accidental or unauthorized launch; deliberate first attack by one nation; and inadvertent attack. In an accidental or unauthorized launch or detonation, system safeguards or procedures to maintain control over nuclear weapons fail in such a way that a nuclear weapon or missile launches or explodes without direction from leaders. In a deliberate first attack, the attacking nation decides to attack based on accurate information about the state of affairs. In an inadvertent attack, the attacking nation mistakenly concludes that it is under attack and launches nuclear weapons in what it believes is a counterattack.3 (Brinkmanship strategies incorporate elements of all of the above, in that they involve intentional manipulation of risks from otherwise accidental or inadvertent launches.4 )

Over the years, nuclear strategy was aimed primarily at minimizing risks of intentional attack through development of deterrence capabilities, though numerous measures were also taken to reduce probabilities of accidents, unauthorized attack, and inadvertent war. For purposes of deterrence, both U.S. and Soviet/Russian forces have maintained significant capabilities to have some forces survive a first attack by the other side and to launch a subsequent counterattack. However, concerns about the extreme disruptions that a first attack would cause in the other side’s forces and command-and-control capabilities led to both sides’ development of capabilities to detect a first attack and launch a counter-attack before suffering damage from the first attack.5

Many people believe that with the end of the Cold War and with improved relations between the United States and Russia, the risk of East-West nuclear war was significantly reduced.6 However, it has also been argued that inadvertent nuclear war between the United States and Russia has continued to present a substantial risk.7 While the United States and Russia are not actively threatening each other with war, they have remained ready to launch nuclear missiles in response to indications of attack.8

False indicators of nuclear attack could be caused in several ways. First, a wide range of events have already been mistakenly interpreted as indicators of attack, including weather phenomena, a faulty computer chip, wild animal activity, and control-room training tapes loaded at the wrong time.9 Second, terrorist groups or other actors might cause attacks on either the United States or Russia that resemble some kind of nuclear attack by the other nation by actions such as exploding a stolen or improvised nuclear bomb,10 especially if such an event occurs during a crisis between the United States and Russia.11 A variety of nuclear terrorism scenarios are possible.12 Al Qaeda has sought to obtain or construct nuclear weapons and to use them against the United States.13 Other methods could involve attempts to circumvent nuclear weapon launch control safeguards or exploit holes in their security.14

It has long been argued that the probability of inadvertent nuclear war is significantly higher during U.S.-Russian crisis conditions,15 with the Cuban Missile Crisis being a prime historical example. It is possible that U.S.-Russian relations will significantly deteriorate in the future, increasing nuclear tensions. There are a variety of ways for a third party to raise tensions between the United States and Russia, making one or both nations more likely to misinterpret events as attacks.16

## 2NC/1NR

### DA Outweighs Case

#### Electronic surveillance prevents terrorism. On balance, it does more to stop terrorism than it inhibits privacy.

Posner 8 — Richard A Posner, Judge for the United States Court of Appeals Seventh Circuit, Senior Lecturer at the University of Chicago School of Law, former Solicitor General of the US, former general council on the Presidential Task force on Communications Policy, written more than 2500 published judicial opinions, recipient of the Thomas C. Schelling Award for scholarly contributions that have had an impact on public policy from the John F. Kennedy School of Government at Harvard University, and the Henry J. Friendly Medal from the American Law Institute, 2008 (“Privacy, Surveillance, and Law,” *University of Chicago Law Review*, Volume 75, Available Online at <http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2808&context=journal_articles>, Accessed 08-08-2015, p. 254)

These things are true of government as well as of private individuals and firms. Civil libertarians want government to be transparent but private individuals opaque; national security hawks want the reverse. People hide from government, and government hides from the people, and people and government have both good and bad reasons for hiding from the other. Complete transparency paralyzes planning and action; complete opacity endangers both liberty and security. Terrorists know this best. Eavesdropping imposes costs on innocent people because their privacy is compromised; but the costs it imposes on terrorists are even steeper because it thwarts their plans utterly and places them at risk of capture or death. Of course, from our standpoint as a people endangered by terrorism, the higher those costs the better.

Many people are frightened of the eavesdropping potential of modern computer technology. Suppose that the listening devices of the National Security Agency (NSA) gathered the entire world's electronic communications traffic, digitized it, and stored it in databases; that the digitized data were machine-searched for clues to terrorist activity; but that the search programs were designed to hide from intelligence officers all data that furnished no clues to terrorist plans or activity. (For all one knows, the NSA is doing all these things.) The data vacuumed by the NSA in the first, the gathering, stage of the intelligence project would, after screening by the search programs, present intelligence officers with two types of communication to study: communications that contained innocent references to terrorism and communications among the terrorists themselves. Engaging in either type of communication would be discouraged once people realized the scope of the agency's program, but the consequences for the nation would be quite different for the two types. Discouraging innocent people from mentioning anything that might lead a computer search to earmark the communication for examination by an intelligence officer would inhibit the free exchange of ideas on matters of public as well as private importance. But discouraging terrorists from communicating by electronic means would discourage terrorism. Foreign terrorists would find it difficult to communicate with colleagues or sympathizers in the United States if they had to do so face to face or through messengers because they would know the government was eavesdropping on all their electronic communications. This is simply my earlier point writ large: protected communications are valuable to the persons communicating, whether they are good people or bad people, and this duality is the source of both the costs and the benefits of intercepting communications for intelligence purposes.

### DA Turns Case — Rollback

#### DA turns case — another 9/11 would crush civil liberties and roll back the plan.

Friedman 13 — Thomas L. Friedman, Pulitzer Prize-winning Columnist for the *New York Times*, holds an M.Phil. in Middle Eastern Studies from St Antony's College at the University of Oxford, 2013 (“Blowing a Whistle,” *New York Times*, June 11th, Available Online at <http://www.nytimes.com/2013/06/12/opinion/friedman-blowing-a-whistle.html?hp>, Accessed 08-05-2015)

I’m glad I live in a country with people who are vigilant in defending civil liberties. But as I listen to the debate about the disclosure of two government programs designed to track suspected phone and e-mail contacts of terrorists, I do wonder if some of those who unequivocally defend this disclosure are behaving as if 9/11 never happened — that the only thing we have to fear is government intrusion in our lives, not the intrusion of those who gather in secret cells in Yemen, Afghanistan and Pakistan and plot how to topple our tallest buildings or bring down U.S. airliners with bombs planted inside underwear, tennis shoes or computer printers.

Yes, I worry about potential government abuse of privacy from a program designed to prevent another 9/11 — abuse that, so far, does not appear to have happened. But I worry even more about another 9/11. That is, I worry about something that’s already happened once — that was staggeringly costly — and that terrorists aspire to repeat.

I worry about that even more, not because I don’t care about civil liberties, but because what I cherish most about America is our open society, and I believe that if there is one more 9/11 — or worse, an attack involving nuclear material — it could lead to the end of the open society as we know it. If there were another 9/11, I fear that 99 percent of Americans would tell their members of Congress: “Do whatever you need to do to, privacy be damned, just make sure this does not happen again.” That is what I fear most.

That is why I’ll reluctantly, very reluctantly, trade off the government using data mining to look for suspicious patterns in phone numbers called and e-mail addresses — and then have to go to a judge to get a warrant to actually look at the content under guidelines set by Congress — to prevent a day where, out of fear, we give government a license to look at anyone, any e-mail, any phone call, anywhere, anytime.

So I don’t believe that Edward Snowden, the leaker of all this secret material, is some heroic whistle-blower. No, I believe Snowden is someone who needed a whistle-blower. He needed someone to challenge him with the argument that we don’t live in a world any longer where our government can protect its citizens from real, not imagined, threats without using big data — where we still have an edge — under constant judicial review. It’s not ideal. But if one more 9/11-scale attack gets through, the cost to civil liberties will be so much greater.

#### A new terrorist attack will massively increase surveillance — 9/11 proves.

Clarke et al. 13 — Richard A. Clarke, teaches as Harvard’s Kennedy School of Government, former Senior White House Advisor, former US National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, former Assistant Secretary of State for Political-Military Affairs, Michael J. Morell, former acting director and deputy director of the CIA, Geoffrey R. Stone, Distinguished Service Professor of Law at the University of Chicago Law School, Cass R. Sunstein, Administrator of the White House Office of Information and Regulatory Affairs in the Obama administration, Professor of Law at Harvard Law School, and Peter Swire, professor of law and ethics at the Georgia Institute of Technology, senior counsel with Alston & Bird LLP, and a cyber-fellow with New America, 2013 (“Liberty and Security in a Changing World: The Final Report of the President’s Review Group on Intelligence and Communications Technologies,” Presidential Commission Report, December 12th, Available Online at <https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>, Accessed 08-09-2015)

The September 11 attacks were a vivid demonstration of the need for detailed information about the activities of potential terrorists. This was so for several reasons.

First, some information, which could have been useful, was not collected and other information, which could have helped to prevent the attacks, was not shared among departments.

Second, the scale of damage that 21st-century terrorists can inflict is far greater than anything that their predecessors could have imagined. We are no longer dealing with threats from firearms and conventional explosives, but with the possibility of weapons of mass destruction, including nuclear devices and biological and chemical agents. The damage that such attacks could inflict on the nation, measured in terms of loss of life, economic and social disruption, and the consequent sacrifice of civil liberties, is extraordinary. The events of September 11 brought this home with crystal clarity.

Third, 21st-century terrorists operate within a global communications network that enables them both to hide their existence from outsiders and to communicate with one another across continents at the speed of light. Effective safeguards against terrorist attacks require the technological capacity to ferret out such communications in an international communications grid.

Fourth, many of the international terrorists that the United States and other nations confront today cannot realistically be deterred by the fear of punishment. The conventional means of preventing criminal conduct—the fear of capture and subsequent punishment—has relatively little role to play in combating some contemporary terrorists. Unlike the situation during the Cold War, in which the Soviet Union was deterred from launching a nuclear strike against the United States in part by its fear of a retaliatory counterattack, the terrorist enemy in the 21st-century is not a nation state against which the United States and its allies can retaliate with the same effectiveness. In such circumstances, detection in advance is essential in any effort to “provide for the common defence.”

Fifth, the threat of massive terrorist attacks involving nuclear, chemical, or biological weapons can generate a chilling and destructive environment of fear and anxiety among our nation’s citizens. If Americans came to believe that we are infiltrated by enemies we cannot identify and who have the power to bring death, destruction, and chaos to our lives on a massive scale, and that preventing such attacks is beyond the capacity of our government, the quality of national life would be greatly imperiled. Indeed, if a similar or even more devastating attack were to occur in the future, there would almost surely be an impulse to increase the use of surveillance technology to prevent further strikes, despite the potentially corrosive effects on individual freedom and self-governance.

#### If a terrorist attack occurs, the government will overreact and eliminate privacy and civil liberties.

Clarke et al. 13 — Richard A. Clarke, teaches as Harvard’s Kennedy School of Government, former Senior White House Advisor, former US National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, former Assistant Secretary of State for Political-Military Affairs, Michael J. Morell, former acting director and deputy director of the CIA, Geoffrey R. Stone, Distinguished Service Professor of Law at the University of Chicago Law School, Cass R. Sunstein, Administrator of the White House Office of Information and Regulatory Affairs in the Obama administration, Professor of Law at Harvard Law School, and Peter Swire, professor of law and ethics at the Georgia Institute of Technology, senior counsel with Alston & Bird LLP, and a cyber-fellow with New America, 2013 (“Liberty and Security in a Changing World: The Final Report of the President’s Review Group on Intelligence and Communications Technologies,” Presidential Commission Report, December 12th, Available Online at <https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>, Accessed 08-09-2015)

For reasons that we have outlined, it is always challenging to strike the right balance between the often competing values of national security and individual liberty, but as history teaches, it is particularly difficult to reconcile these values in times of real or perceived national crisis. Human nature being what it is, there is inevitably a risk of overreaction when we act out of fear. At such moments, those charged with the responsibility for keeping our nation safe, supported by an anxious public, have too often gone beyond programs and policies that were in fact necessary and appropriate to protect the nation and taken steps that unnecessarily and sometimes dangerously jeopardized individual freedom.

This phenomenon is evident throughout American history. Too often, we have overreacted in periods of national crisis and then later, with the benefit of hindsight, recognized our failures, reevaluated our judgments, and attempted to correct our policies going forward. We must learn the lessons of history.

As early as 1798, Congress enacted the Sedition Act, now widely regarded as a violation of the most fundamental principles of freedom of expression. Nor is the historical verdict kind to a wide range of liberty restricting measures undertaken in other periods of great national anxiety, including the repeated suspensions of the writ of habeas corpus during the Civil War, the suppression of dissent during World War I, the internment of Japanese-Americans during World War II, the campaign to expose and harass persons suspected of “disloyalty” during the McCarthy era, and the widespread and unlawful spying on critics of the government’s policies during the Vietnam War. 3

It is true that when the nation is at risk, or engaged in some kind of military conflict, the argument for new restrictions may seem, and even be, plausible. Serious threats may tip preexisting balances. But it is also true that in such periods, there is a temptation to ignore the fact that risks are on all sides of the equation, and to compromise liberty at the expense of security. One of our central goals in this Report is to provide secure foundations for future decisions, when public fears may heighten those dangers.

With respect to surveillance in particular, the nation’s history is lengthy and elaborate, but the issues in the modern era can be traced back directly to the Vietnam War. Presidents Lyndon Johnson and Richard Nixon encouraged government intelligence agencies to investigate alleged “subversives” in the antiwar movement. The Federal Bureau of Investigation (FBI) engaged in extensive infiltration and electronic surveillance of individuals and organizations opposed to the war; the Central Intelligence Agency (CIA) monitored a broad array of antiwar organizations and activities, accumulating information on more than 300,000 people; and Army intelligence initiated its own domestic spying operation, gathering information on more than 100,000 opponents of the Vietnam War, including Members of Congress, civil rights leaders, and journalists. The government sought not only to investigate its critics on a massive scale, but also to expose, disrupt, and neutralize their efforts to affect public opinion.4

### They Say: “No Immanent Terror Threat”

#### The FBI thwarted several attacks, but ISIS is expanding its influence — the homeland is under threat.

Racine 15 — Hope Racine, DC-based Freelance Writer and Associate Editor of *Literally, Darling*—an online magazine by and for twenty-something women, 2015 (“Several ISIS July 4 Attacks Were Prevented, The FBI Says, & The Few Details We Know Are Pretty Scary,” *Bustle*, July 9th, Available Online at <http://www.bustle.com/articles/96240-several-isis-july-4-attacks-were-prevented-the-fbi-says-the-few-details-we-know>, Accessed 07-12-2015)

On Thursday, FBI director James Comey released a statement revealing that the FBI stopped several ISIS related Fourth of July attacks. Though Comey didn’t state how many plots there were, or the details of any cases, he did say that the attempted plots ranged from coast to coast, and were intended to take American lives. Leading up to the holiday weekend, local law enforcement agencies were encouraged to take extra precautions, and be aware of possible terror attacks. Within the past four weeks, there have been 10 ISIS-related arrests.

It’s important to note that, as far as Comey told the public, none of the thwarted plots were formally sanctioned ISIS attacks. Instead, these plots were “unsophisticated” and were ISIS-inspired rather than ISIS-endorsed. Leading up to the holiday, the terror organization made calls encouraging ISIS sympathizers to attack in any way possible, and as such many of the foiled plans involved guns, knives, and other close range weapons.

News that the attacks were foiled is reassuring, as it gives proof that the FBI is combatting domestic terrorism, but it’s also terrifying when you look at these potential plots in context of what might have happened. ISIS’s influence is reaching beyond the Middle East, and their fighters are growing more sophisticated in the way that they communicate with American residents.

#### The threat of terrorism has dramatically increased in the last year — NSA surveillance is key to stop attacks.

Bolton 15 — John R. Bolton, former U.S. Under Secretary of State for Arms Control and International Security, fellow at the American Enterprise Institute, former U.S. Representative to the United Nations, 2015 ("NSA activities key to terrorism fight," American Enterprise Institute, April 28th, Available Online at https://www.aei.org/publication/nsa-activities-key-to-terrorism-fight/, Accessed 08-08-2015)

In fact, just in the year since Congress last considered the NSA programs, the global terrorist threat has dramatically increased. ISIS is carving out an entirely new state from what used to be Syria and Iraq, which no longer exist within the borders created from the former Ottoman Empire after World War I. In already-chaotic Libya, ISIS has grown rapidly, eclipsing al-Qaeda there and across the region as the largest terrorist threat. Boko Haram is expanding beyond Nigeria, declaring its own caliphate, even while pledging allegiance to ISIS. Yemen has descended into chaos, following Libya’s pattern, and Iran has expanded support for the terrorist Houthi coalition. Afghanistan is likely to fall back under Taliban control if, as Obama continually reaffirms, he withdraws all American troops before the end of 2016.

This is not the time to cripple our intelligence-gathering capabilities against the rising terrorist threat. Congress should unquestionably reauthorize the NSA programs, but only for three years. That would take us into a new presidency, hopefully one that inspires more confidence, where a calmer, more sensible debate can take place.

#### The risk of terror is high and increasing — only surveillance has prevented another 9/11.

Lewis 14 — James Andrew Lewis, Ph.D. from U.Chicago, Senior Fellow and Director of the Strategic Technologies Program at the Center for Strategic and International Studies, former member of the U.S. Foreign Service and Senior Executive Service, where he worked on regional security, military intervention and insurgency, conventional arms negotiations, technology transfer, encryption, internet security, space remote sensing, high-tech trade with China, sanctions and Internet policy, led the U.S. delegation to the Wassenaar Arrangement Experts Group for advanced civil and military technologies, assigned to the U.S. Southern Command for Just Cause, the U.S. Central Command for Desert Shield, and to the National Security Council and the U.S. Central American Task Force for programs in Nicaragua, 2015 (“Underestimating Risk in the Surveillance Debate,” CSIS Strategic Technologies Program, December, Available Online at <https://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf>, Accessed 08-08-2015)

There is general agreement that as terrorists splinter into regional groups, the risk of attack increases. Certainly, the threat to Europe from militants returning from Syria points to increased risk for U.S. allies. The messy U.S. withdrawal from Iraq and (soon) Afghanistan contributes to an increase in risk.24 European authorities have increased surveillance and arrests of suspected militants as the Syrian conflict lures hundreds of Europeans. Spanish counterterrorism police say they have broken up more terrorist cells than in any other European country in the last three years.25 The chairman of the House Select Committee on Intelligence, who is better placed than most members of Congress to assess risk, said in June 2014 that the level of terrorist activity was higher than he had ever seen it.26 If the United States overreacted in response to September 11, it now risks overreacting to the leaks with potentially fatal consequences.

A simple assessment of the risk of attack by jihadis would take into account a resurgent Taliban, the power of lslamist groups in North Africa, the continued existence of Shabaab in Somalia, and the appearance of a powerful new force, the Islamic State in Iraq and Syria (ISIS). Al Qaeda, previously the leading threat, has splintered into independent groups that make it a less coordinated force but more difficult target. On the positive side, the United States, working with allies and friends, appears to have contained or eliminated jihadi groups in Southeast Asia.

Many of these groups seek to use adherents in Europe and the United States for manpower and funding. A Florida teenager was a suicide bomber in Syria and Al Shabaab has in the past drawn upon the Somali population in the United States. Hamas and Hezbollah have achieved quasi-statehood status, and Hamas has supporters in the United States. Iran, which supports the two groups, has advanced capabilities to launch attacks and routinely attacked U.S. forces in Iraq. The United Kingdom faces problems from several hundred potential terrorists within its large Pakistani population, and there are potential attackers in other Western European nations, including Germany, Spain, and the Scandinavian countries. France, with its large Muslim population faces the most serious challenge and is experiencing a wave of troubling anti-Semitic attacks that suggest both popular support for extremism and a decline in control by security forces.

The chief difference between now and the situation before 9/11 is that all of these countries have put in place much more robust surveillance systems, nationally and in cooperation with others, including the United States, to detect and prevent potential attacks. Another difference is that the failure of U.S. efforts in Iraq and Afghanistan and the opportunities created by the Arab Spring have opened a new “front” for jihadi groups that makes their primary focus regional. Western targets still remain of interest, but are more likely to face attacks from domestic sympathizers. This could change if the well-resourced ISIS is frustrated in its efforts to establish a new Caliphate and turns its focus to the West. In addition, the al Qaeda affiliate in Yemen (al Qaeda in the Arabian Peninsula) continues to regularly plan attacks against U.S. targets. 27

The incidence of attacks in the United States or Europe is very low, but we do not have good data on the number of planned attacks that did not come to fruition. This includes not just attacks that were detected and stopped, but also attacks where the jihadis were discouraged and did not initiate an operation or press an attack to its conclusion because of operational difficulties. These attacks are the threat that mass surveillance was created to prevent. The needed reduction in public anti-terror measures without increasing the chances of successful attack is contingent upon maintaining the capability provided by communications surveillance to detect, predict, and prevent attacks. Our opponents have not given up; neither should we.

### They Say: “USA Freedom Act Curtailed Surveillance”

#### The status quo solves the case and avoids the DA — the USA Freedom Act sufficiently protects privacy while ensuring enough surveillance to prevent terrorism.

Carafano et al. 15 — James Jay Carafano, Ph. D., Vice President for the Institute for National Security and Foreign Policy at the Heritage Foundation, former senior fellow at the Center for Strategic and Budgetary Assessments, a Washington policy institute dedicated to defense issues, Charles “Cully” Stimson, Senior Legal Fellow at the Institute for National Security and Foreign Policy at The Heritage Foundation, former Deputy Assistant Secretary of Defense for Detainee Affairs, Steven P. Bucci, Ph.D., Director of the Center for Foreign and National Security Policies at the Heritage Foundation, former Army Special Forces officer and top Pentagon official, former lead consultant to IBM on cyber security policy, John Malcolm, Director, Center for Legal and Judicial Studies at The Heritage Foundation, former deputy assistant attorney general in the Department of Justice’s Criminal Division, and Paul Rosenzweig, policy expert at The Heritage Foundation, 2015 ("Section 215 of the PATRIOT Act and Metadata Collection: Responsible Options for the Way Forward," Heritage Foundation, May 21st, Available Online at http://www.heritage.org/research/reports/2015/05/section-215-of-the-patriot-act-and-metadata-collection-responsible-options-for-the-way-forward, Accessed 08-08-2015)

Policy Option No. 3. The third policy option is the House-passed USA FREEDOM Act—legislation that reauthorizes Section 215 and reforms it to end government bulk collection of telephone metadata by the NSA. Instead, the metadata resides with the telephone carriers, where the government will have access to it subject to a court order by the FISC.

The USA FREEDOM Act replaces bulk collection with a program called a “Call Detail Record.” Under this new program, whenever the NSA feels it has reasonable, articulable suspicion that a phone number is associated with international terrorism, it can seek an order to access information about that number from the FISC.

If the FISC gives the order, the NSA will submit one or several queries to the telecom companies for historical and real-time data on the number in question. At that time, both historical and real-time data related to the suspicious number will flow into the NSA, as well as data on the two generations of numbers surrounding it (referred to as “hops”). This information will flow on a 24/7 basis for 180 days, double the amount of time that a FISC order currently authorizes. At the end of 180 days, the NSA can seek renewal for another 180-day time period.

Ending the bulk collection of telephone metadata by the government, or even housing it in a private third-party entity, may encumber the ability of the intelligence community to analyze all the data in real time across a known pool of data. Such a change will inevitably slow down investigators, but as the technology changes, this should be rectified. That said, numerous intelligence community leaders have said that while it is far from ideal, they could live with such a system, understanding that America is accepting some risk by doing so.

Section 102 provides for emergency authority for the Attorney General to require emergency production of tangible things absent a court order as long as he or she informs a FISC judge and subsequently makes an application to the court within seven days after taking this action. The USA FREEDOM Act also establishes several civil liberties protections for the existing program as it relates to the telephone metadata program.

Section 401 of the Act requires the presiding judges of the FISC to designate not fewer than five individuals to be eligible to serve as amicus curiae—friends of the court. Those designated shall be experts in privacy and civil liberties, intelligence collection, and communications technology and be eligible for a security clearance. The amicus curiae serve to assist the court in the consideration of any novel or significant interpretation of the law.

Section 402 of the Act also mandates the Director of National Intelligence, in consultation with the Attorney General, to conduct a declassification review of each decision, order, or opinion by the FISC and, to the extent practicable, make those decisions, orders, or opinions publicly available.

The USA FREEDOM Act also contains other reforms, including prohibiting bulk collection utilizing FISA pen register and the “trap and trace” procedures in Section 201.

The Act is the only legislative vehicle that has passed a chamber of Congress. It is not perfect and could be improved. For example, there should be a uniform period of time for carriers to maintain the telephone metadata. Another could be designating a specific format in which the carriers must maintain the data to allow more expeditious analysis once the data is appropriately obtained. The USA FREEDOM Act strikes a balance between maintaining our national security capabilities and protecting privacy and civil liberties, and this should always be the goal.

#### Section 215 was the least useful surveillance tool.

Lewis 14 — James Andrew Lewis, Ph.D. from U.Chicago, Senior Fellow and Director of the Strategic Technologies Program at the Center for Strategic and International Studies, former member of the U.S. Foreign Service and Senior Executive Service, where he worked on regional security, military intervention and insurgency, conventional arms negotiations, technology transfer, encryption, internet security, space remote sensing, high-tech trade with China, sanctions and Internet policy, led the U.S. delegation to the Wassenaar Arrangement Experts Group for advanced civil and military technologies, assigned to the U.S. Southern Command for Just Cause, the U.S. Central Command for Desert Shield, and to the National Security Council and the U.S. Central American Task Force for programs in Nicaragua, 2015 (“Executive Summary: Underestimating Risk in the Surveillance Debate,” CSIS Strategic Technologies Program, December, Available Online at <https://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf>, Accessed 08-08-2015)

In practice, analysts must simultaneously explore many possible scenarios. A collection program contributes by not only what it reveals, but also what it lets us reject as false. The Patriot Act Section 215 domestic bulk telephony metadata program provided information that allowed analysts to rule out some scenarios and suspects. The consensus view from interviews with current and former intelligence officials is that while metadata collection is useful, it is the least useful of the collection programs available to the intelligence community. If there was one surveillance program they had to give up, it would be 215, but this would not come without an increase in risk. Restricting metadata collection will make it harder to identify attacks and increase the time it takes to do this.

#### The New Freedom Act didn’t meaningfully limit NSA surveillance.

Kaplan 15 — Fred Kaplan, Ph.D. in Political Science from MIT, Edward R. Murrow press fellow at the Council on Foreign Relations, “War Stories” columnist at Slate, former defense-policy adviser for Rep. Les Aspin in the House of Representatives, and author of The Insurgents: David Petraeus and the Plot to Change the American Way of War, 2015 ("The NSA Debate We Should Be Having," Slate Magazine, June 8th, Available Online at http://www.slate.com/articles/news\_and\_politics/war\_stories/2015/06/the\_national\_security\_agency\_s\_surveillance\_and\_the\_usa\_freedom\_act\_the.html, Accessed 08-09-2015)

The whole point—really, the only point—of the USA Freedom Act, and the overhaul of Section 215 telephone metadata, was to strengthen that oversight, to erect yet another fence that the intelligence agencies have to hurdle to get access to private information.

But no one should infer from this that we’ve entered into a new era or that government surveillance and cyberespionage have been—for better or worse—dealt a serious setback. The NSA is not in retreat, nor are its counterparts in Russia, China, Israel, France, Iran, North Korea, and other countries. That’s not an excuse for complacency or alarm; it’s cause for vigilance, oversight—and an understanding of what these programs are about.

### They Say: “Data Overload Turn”

#### False negatives outweigh false positives — absent casting a wide net, terrorism is inevitable.

Posner 8 — Richard A Posner, Judge for the United States Court of Appeals Seventh Circuit, Senior Lecturer at the University of Chicago School of Law, former Solicitor General of the US, former general council on the Presidential Task force on Communications Policy, written more than 2500 published judicial opinions, recipient of the Thomas C. Schelling Award for scholarly contributions that have had an impact on public policy from the John F. Kennedy School of Government at Harvard University, and the Henry J. Friendly Medal from the American Law Institute, 2008 (“Privacy, Surveillance, and Law,” University of Chicago Law Review, Volume 75, Available Online at <http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2808&context=journal_articles>, Accessed 08-08-2015, p. 254)

It is true that surveillance not cabined by a conventional probable cause requirement produces many false positives-interceptions that prove upon investigation to have no intelligence value. But that is not a valid criticism. The cost of false positives must be balanced against that of false negatives. The failure to detect the 9/11 plot was an exceptionally costly false negative. The intelligence services have no alternative to casting a wide net with a fine mesh if they are to have reasonable prospects of obtaining the clues that will enable future terrorist attacks on the United States to be prevented.

The NSA's Terrorist Surveillance Program-the controversial program, secret until revealed by the New York Times in December 2005,2 for conducting electronic surveillance without warrants and therefore outside the boundaries of FISA'"-involves an initial sifting, performed by computer search programs, of electronic communications for clues to terrorist activity. The sifting uses both "content filtering" and "traffic analysis" to pick out a tiny percentage of communications to be read. Content filtering is searching for particular words or patterns of words inside the communication. Traffic analysis is examining message length, frequency, and time of communication and other noncontent information that may reveal suspicious patterns; thus traffic analysis cannot be foiled by encryption because the information is not content based." The NSA has obtained call records from telephone companies to aid in its traffic analysis. If the agency has the phone number of a known or suspected terrorist, it can use call records to determine the most frequent numbers called to or from that number, and it can then determine the most frequent numbers called to or from those numbers and in this way piece together a possible terrorist network-all without listening to any conversation. That comes later.

#### Schneier is wrong about mass surveillance — it’s a vital counter-terror tool.

Knee 15 — Jonathan A. Knee, Professor of Professional Practice at Columbia Business School, Senior Adviser at Evercore Partners—a U.S. investment bank, holds a J.D. from Yale Law School and an M.B.A. from the Stanford Business School, 2015 (“Looking at the Promise and Perils of the Emerging Big Data Sector: Book Review of ‘Data and Goliath’ by Bruce Schneier,” *Deal Book*—a *New York Times* blog, March 16th, Available Online at <http://www.nytimes.com/2015/03/17/business/dealbook/book-review-of-data-and-goliath-by-bruce-schneier.html>, Accessed 07-12-2015)

When it comes to his specific policy recommendations, however, Mr. Schneier becomes significantly less compelling. And the underlying philosophy that emerges — once he has dispensed with all pretense of an evenhanded presentation of the issues — seems actually subversive of the very democratic principles that he claims animates his mission.

The author is at his most vehement in his opposition of all forms of government mass surveillance. He claims that data mining of undifferentiated bulk communications sucked up by our national security apparatus is “an inappropriate tool for finding terrorists.” “Whenever we learn about an N.S.A. success,” Mr. Schneier informs us, “it invariably comes from targeted surveillance rather than from mass surveillance.”

Like the claim that waterboarding failed to yield actionable intelligence that thwarted terrorist plots, it is impossible for a citizen without access to classified information to assess its validity.

Even if Mr. Schneier is correct that “traditional investigative police work” is ultimately responsible for successfully identifying the truly dangerous, there are still reasons that the public would want our spies to have access to a ready cache of metadata. As soon as the bad guy is found using old-fashioned methods, data-mining of previous communications would still presumably allow the speedy identification of known associates with a potentially lifesaving efficiency.

#### The risk is linear — eliminating any surveillance authority increases the likelihood of a successful attack.

Lewis 14 — James Andrew Lewis, Ph.D. from U.Chicago, Senior Fellow and Director of the Strategic Technologies Program at the Center for Strategic and International Studies, former member of the U.S. Foreign Service and Senior Executive Service, where he worked on regional security, military intervention and insurgency, conventional arms negotiations, technology transfer, encryption, internet security, space remote sensing, high-tech trade with China, sanctions and Internet policy, led the U.S. delegation to the Wassenaar Arrangement Experts Group for advanced civil and military technologies, assigned to the U.S. Southern Command for Just Cause, the U.S. Central Command for Desert Shield, and to the National Security Council and the U.S. Central American Task Force for programs in Nicaragua, 2015 (“Underestimating Risk in the Surveillance Debate,” CSIS Strategic Technologies Program, December, Available Online at <https://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf>, Accessed 08-08-2015)

This effort takes place over months and involves multiple intelligence, law enforcement, and military agencies, with more than a dozen individuals from these agencies collaborating to build up a picture of the bomb-maker and his planned attack. When the bomb-maker leaves the Middle East to carry out his attack, he is prevented from entering the United States. An analogy for how this works would be to take a 1,000-piece jigsaw puzzle, randomly select 200 pieces, and provide them to a team of analysts who, using incomplete data, must guess what the entire picture looks like. The likelihood of their success is determined by how much information they receive, how much time they have, and by experience and luck. Their guess can be tested by using a range of collection programs, including communications surveillance programs like the 215 metadata program.

What is left out of this picture (and from most fictional portrayals of intelligence analysis) is the number of false leads the analysts must pursue, the number of dead ends they must walk down, and the tools they use to decide that something is a false lead or dead end. Police officers are familiar with how many leads in an investigation must be eliminated through legwork and query before an accurate picture emerges. Most leads are wrong, and much of the work is a process of elimination that eventually focuses in on the most probable threat. If real intelligence work were a film, it would be mostly boring. Where the metadata program contributes is in eliminating possible leads and suspects.

This makes the critique of the 215 program like a critique of airbags in a car—you own a car for years, the airbags never deploy, so therefore they are useless and can be removed. The weakness in this argument is that discarding airbags would increase risk. How much risk would increase and whether other considerations outweigh this increased risk are fundamental problems for assessing surveillance programs. With the Section 215 program, Americans gave up a portion of their privacy in exchange for decreased risk. Eliminating 215 collection is like subtracting a few of the random pieces of the jigsaw puzzle. It decreases the chances that the analysts will be able to deduce what is actually going on and may increase the time it takes to do this. That means there is an increase in the risk of a successful attack. How much of an increase in risk is difficult to determine, but this is crucial for assessing the value of domestic surveillance programs.

### They Say: “Government Doesn’t Need More Data”

#### Americans consistently underestimate the threat of terrorism — communications surveillance is the only tool to prevent attacks.

Lewis 14 — James Andrew Lewis, Ph.D. from U.Chicago, Senior Fellow and Director of the Strategic Technologies Program at the Center for Strategic and International Studies, former member of the U.S. Foreign Service and Senior Executive Service, where he worked on regional security, military intervention and insurgency, conventional arms negotiations, technology transfer, encryption, internet security, space remote sensing, high-tech trade with China, sanctions and Internet policy, led the U.S. delegation to the Wassenaar Arrangement Experts Group for advanced civil and military technologies, assigned to the U.S. Southern Command for Just Cause, the U.S. Central Command for Desert Shield, and to the National Security Council and the U.S. Central American Task Force for programs in Nicaragua, 2015 (“Underestimating Risk in the Surveillance Debate,” CSIS Strategic Technologies Program, December, Available Online at <https://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf>, Accessed 08-08-2015)

The echoes of September 11 have faded and the fear of attack has diminished. We are reluctant to accept terrorism as a facet of our daily lives, but major attacks—roughly one a year in the last five years—are regularly planned against U.S. targets, particularly passenger aircraft and cities. America’s failures in the Middle East have spawned new, aggressive terrorist groups. These groups include radicalized recruits from the West—one estimate puts the number at over 3,000—who will return home embittered and hardened by combat. Particularly in Europe, the next few years will see an influx of jihadis joining the existing population of homegrown radicals, but the United States itself remains a target.

America’s size and population make it is easy to disappear into the seams of this sprawling society. Government surveillance is, with one exception and contrary to cinematic fantasy, limited and disconnected. That exception is communications surveillance, which provides the best and perhaps the only national-level solution to find and prevent attacks against Americans and their allies. Some of the suggestions for alternative approaches to surveillance, such as the recommendation that NSA only track “known or suspected terrorists,” reflect both deep ignorance and wishful thinking. It is the unknown terrorist who will inflict the greatest harm.

This administration could reasonably argue that everything it has done is legal and meets existing requirements for oversight, but this defense is universally perceived as legalistic hairsplitting. If the government can be faulted, it is for obsessive secrecy. The public debate over NSA’s surveillance programs routinely exaggerates risks and errors, 1 but in the absence of a compelling official narrative, the space was filled with conjecture and distortion. This has not helped a crucial debate where a wrong answer could mean more bombings.

#### Robust surveillance is critical to preventing terrorist attacks — experts believe it would have prevented 9/11.

Carafano et al. 15 — James Jay Carafano, Ph. D., Vice President for the Institute for National Security and Foreign Policy at the Heritage Foundation, former senior fellow at the Center for Strategic and Budgetary Assessments, a Washington policy institute dedicated to defense issues, Charles “Cully” Stimson, Senior Legal Fellow at the Institute for National Security and Foreign Policy at The Heritage Foundation, former Deputy Assistant Secretary of Defense for Detainee Affairs, Steven P. Bucci, Ph.D., Director of the Center for Foreign and National Security Policies at the Heritage Foundation, former Army Special Forces officer and top Pentagon official, former lead consultant to IBM on cyber security policy, John Malcolm, Director, Center for Legal and Judicial Studies at The Heritage Foundation, former deputy assistant attorney general in the Department of Justice’s Criminal Division, and Paul Rosenzweig, policy expert at The Heritage Foundation, 2015 ("Section 215 of the PATRIOT Act and Metadata Collection: Responsible Options for the Way Forward," Heritage Foundation, May 21st, Available Online at http://www.heritage.org/research/reports/2015/05/section-215-of-the-patriot-act-and-metadata-collection-responsible-options-for-the-way-forward, Accessed 08-08-2015)

The United States is in a state of armed conflict against al-Qaeda, the Afghan Taliban, ISIS, and associated forces. It must therefore rely on all lawful tools of national security, including but not limited to robust signals intelligence.

As the 9/11 Commission Report made crystal clear, one of the key failures of the United States before the 9/11 attacks was the government’s inability to “connect the dots” between known or suspected terrorists. The artificial “wall” between domestic law enforcement and U.S. intelligence agencies, enacted during the 1990s, proved to be America’s Achilles’ heel.

Some analysts believe that had America had a Section 215–type program in place before 9/11, U.S. intelligence, along with domestic law enforcement, would have been able to connect the dots and prevent at least some of the hijackers from launching their devastating attack.[14]

In fact, according to a report by the House Permanent Select Committee on Intelligence, using the authorities under Section 215 of the PATRIOT Act and Section 702 of the FISA has contributed to thwarting 54 total international terrorist plots in 20 countries.[15] Thirteen of those plots were directed inside the United States.

#### Intelligence agencies require a complete database of activities to prevent terrorism — every little bit helps.

Yoo 15 — John Yoo, law professor at UC Berkeley and a scholar at the American Enterprise Institute, former Deputy Assistant Attorney General in the Office of Legal Council for the Justice Department under President George W. Bush, 2015 (“Will Congress reject the dangerous NSA ruling by reauthorizing the Patriot Act?,” American Enterprise Institute, May 8th, Available Online at <https://www.aei.org/publication/will-congress-reject-todays-dangerous-nsa-ruling-by-reauthorizing-the-patriot-act/>, Accessed 08-08-2015)

Finally, the Court displays a deep misunderstanding of the challenges of counterterrorism policy, which Congress understands far better. As Judge Richard Posner has recognized, an intelligence search “is a search for the needle in a haystack.” Rather than pursue suspects who have already committed a crime and whose identity is already known, intelligence agencies must search for clues among millions of potentially innocent connections, communications, and links. “The intelligence services,” Posner writes, “must cast a wide net with a fine mesh to catch the clues that may enable the next attack to be prevented.” Our government can detect terrorists by examining phone and e-mail communications, as well as evidence of joint travel, shared assets, common histories or families, meetings, and so on. If our intelligence agents locate a lead, they must quickly follow its many possible links to identify cells and the broader network of terrorists. A database of call data would allow a fast search for possible links in the most important place — the United States, where terrorists can inflict the most damage. Most of the calling records may well be innocent (just as most of the financial records of a suspected white-collar criminal may also be innocent), but the more complete the database, the better our intelligence agencies can pursue a lead into the U.S.

### They Say: “Surveillance Has Never Stopped an Attack”

#### At least 60 terrorist plots since 9/11 — US intelligence was critical to stopping them.

Zuckerman et al. 13 — Jessica Zuckerman, Research Associate in Foreign Policy Studies at The Heritage Foundation, Steven P. Bucci, Ph.D., Director of the Center for Foreign and National Security Policies at the Heritage Foundation, former Army Special Forces officer and top Pentagon official, former lead consultant to IBM on cyber security policy, and James Jay Carafano, Ph. D., Vice President for the Institute for National Security and Foreign Policy at the Heritage Foundation, former senior fellow at the Center for Strategic and Budgetary Assessments, a Washington policy institute dedicated to defense issues, 2013 (“Abstract: 60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism," Heritage Foundation, July 22nd, Available Online at http://www.heritage.org/research/reports/2013/07/60-terrorist-plots-since-911-continued-lessons-in-domestic-counterterrorism, Accessed 08-08-2015)

At 2:50 p.m. on April 15, 2013, two explosions went off at the finish line of the Boston Marathon. The brazen terrorist attack killed three people, injured and maimed hundreds more, and shocked the nation. Despite being long recognized as a potential threat by law enforcement and intelligence, few Americans had considered the use of an improvised explosive device (IED) on American soil. And, due to only a few, and relatively small, attacks since 9/11, the public was not in a state of awareness.

Yet, the fact remains that there have been at least 60 Islamist-inspired terrorist plots against the homeland since 9/11, illustrating the continued threat of terrorism against the United States. Fifty-three of these plots were thwarted long before the public was ever in danger, due in large part to the concerted efforts of U.S. law enforcement and intelligence.

The Heritage Foundation has tracked the foiled terrorist plots against the United States since 9/11 in an effort to study the evolving nature of the threat and garner lessons learned. The best way to protect the United States from the continued threat of terrorism is to ensure a strong and capable domestic counterterrorism enterprise—and to understand the continuing nature of the terror threat.

The bombings in Boston are not likely to be the last such attempt to attack the U.S. as a whole. Now is not the time for the U.S. to stand still. Congress and the Administration should:

* Ensure a proactive approach to halting terrorism,
* Maintain essential counterterrorism tools,
* Break down silos of information,
* Streamline the domestic counterterrorism system, and
* Fully implement a strategy to counter violent extremism

#### Critics are ill-informed about surveillance — domestic programs are critical to rule out unlikely to scenarios to focus on the greatest threats.

Lewis 14 — James Andrew Lewis, Ph.D. from U.Chicago, Senior Fellow and Director of the Strategic Technologies Program at the Center for Strategic and International Studies, former member of the U.S. Foreign Service and Senior Executive Service, where he worked on regional security, military intervention and insurgency, conventional arms negotiations, technology transfer, encryption, internet security, space remote sensing, high-tech trade with China, sanctions and Internet policy, led the U.S. delegation to the Wassenaar Arrangement Experts Group for advanced civil and military technologies, assigned to the U.S. Southern Command for Just Cause, the U.S. Central Command for Desert Shield, and to the National Security Council and the U.S. Central American Task Force for programs in Nicaragua, 2015 (“Underestimating Risk in the Surveillance Debate,” CSIS Strategic Technologies Program, December, Available Online at <https://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf>, Accessed 08-08-2015)

Assertions that a collection program contributes nothing because it has not singlehandedly prevented an attack reflect an ill-informed understanding of how the United States conducts collection and analysis to prevent harmful acts against itself and its allies. Intelligence does not work as it is portrayed in films—solitary agents do not make startling discoveries that lead to dramatic, last-minute success (nor is technology consistently infallible). Intelligence is a team sport. Perfect knowledge does not exist and success is the product of the efforts of teams of dedicated individuals from many agencies, using many tools and techniques, working together to assemble fragments of data from many sources into a coherent picture. Analysts assemble this mosaic from many different sources and based on experience and intuition. Luck is still more important than anyone would like and the alternative to luck is acquiring more information. This ability to blend different sources of intelligence has improved U.S. intelligence capabilities and gives us an advantage over some opponents.

Portrayals of spying in popular culture focus on a central narrative, essential for storytelling but deeply misleading. In practice, there can be many possible narratives that analysts must explore simultaneously. An analyst might decide, for example, to see if there is additional confirming information that points to which explanation deserves further investigation. Often, the contribution from collection programs comes not from what they tell us, but what they let us reject as false. In the case of the 215 program, its utility was in being able to provide information that allowed analysts to rule out some theories and suspects. This allows analysts to focus on other, more likely, scenarios.

#### Claims that surveillance is useless misunderstand the cumulative nature of intelligence — every tool is critical to both rule *in* and rule *out* suspects.

Lewis 14 — James Andrew Lewis, Ph.D. from U.Chicago, Senior Fellow and Director of the Strategic Technologies Program at the Center for Strategic and International Studies, former member of the U.S. Foreign Service and Senior Executive Service, where he worked on regional security, military intervention and insurgency, conventional arms negotiations, technology transfer, encryption, internet security, space remote sensing, high-tech trade with China, sanctions and Internet policy, led the U.S. delegation to the Wassenaar Arrangement Experts Group for advanced civil and military technologies, assigned to the U.S. Southern Command for Just Cause, the U.S. Central Command for Desert Shield, and to the National Security Council and the U.S. Central American Task Force for programs in Nicaragua, 2015 (“Executive Summary: Underestimating Risk in the Surveillance Debate,” CSIS Strategic Technologies Program, December, Available Online at <https://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf>, Accessed 08-08-2015)

NSA carried out two kinds of signals intelligence programs: bulk surveillance to support counterterrorism and collection to support U.S. national security interests. The debate over surveillance unhelpfully conflated the two programs. Domestic bulk collection for counterterrorism is politically problematic, but assertions that a collection program is useless because it has not by itself prevented an attack reflect unfamiliarity with intelligence. Intelligence does not work as it is portrayed in films—solitary agents do not make startling discoveries that lead to dramatic, last-minute success. Success is the product of the efforts of teams of dedicated individuals from many agencies, using many tools and techniques, working together to assemble fragments of data from many sources into a coherent picture.

In practice, analysts must simultaneously explore many possible scenarios. A collection program contributes by not only what it reveals, but also what it lets us reject as false. The Patriot Act Section 215 domestic bulk telephony metadata program provided information that allowed analysts to rule out some scenarios and suspects. The consensus view from interviews with current and former intelligence officials is that while metadata collection is useful, it is the least useful of the collection programs available to the intelligence community. If there was one surveillance program they had to give up, it would be 215, but this would not come without an increase in risk. Restricting metadata collection will make it harder to identify attacks and increase the time it takes to do this.

### They Say: “Terror Threat Exaggerated”

#### Discontinuous risk of terrorism means people consistently underestimate the threat — lack of major attacks since 9/11 is due to success of surveillance, not lack of terrorists. Surveillance is the only way to locate unknown terrorists.

Lewis 14 — James Andrew Lewis, Ph.D. from U.Chicago, Senior Fellow and Director of the Strategic Technologies Program at the Center for Strategic and International Studies, former member of the U.S. Foreign Service and Senior Executive Service, where he worked on regional security, military intervention and insurgency, conventional arms negotiations, technology transfer, encryption, internet security, space remote sensing, high-tech trade with China, sanctions and Internet policy, led the U.S. delegation to the Wassenaar Arrangement Experts Group for advanced civil and military technologies, assigned to the U.S. Southern Command for Just Cause, the U.S. Central Command for Desert Shield, and to the National Security Council and the U.S. Central American Task Force for programs in Nicaragua, 2015 (“Executive Summary: Underestimating Risk in the Surveillance Debate,” CSIS Strategic Technologies Program, December, Available Online at <https://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf>, Accessed 08-08-2015)

Americans are reluctant to accept terrorism is part of their daily lives, but attacks have been planned or attempted against American targets (usually airliners or urban areas) almost every year since 9/11. Europe faces even greater risk, given the thousands of European Union citizens who will return hardened and radicalized from fighting in Syria and Iraq.

The threat of attack is easy to exaggerate, but that does not mean it is nonexistent. Australia’s then-attorney general said in August 2013 that communications surveillance had stopped four “mass casualty events” since 2008. The constant planning and preparation for attack by terrorist groups is not apparent to the public. The dilemma in assessing risk is that it is discontinuous. There can be long periods with no noticeable activity, only to have the apparent calm explode.

The debate over how to reform communications surveillance has discounted this risk. Communications surveillance is an essential law enforcement and intelligence tool. There is no replacement for it. Some suggestions for alternative approaches to surveillance, such as the idea that the National Security Agency (NSA) only track known or suspected terrorists, reflect wishful thinking, as it is the unknown terrorist who will inflict the greatest harm.

#### Err negative on the terrorism and privacy debate — the NSA can’t reveal all of its successes.

Bolton 15 — John R. Bolton, former U.S. Under Secretary of State for Arms Control and International Security, fellow at the American Enterprise Institute, former U.S. Representative to the United Nations, 2015 ("NSA activities key to terrorism fight," American Enterprise Institute, April 28th, Available Online at https://www.aei.org/publication/nsa-activities-key-to-terrorism-fight/, Accessed 08-08-2015)

Congress is poised to decide whether to re-authorize programs run by the National Security Agency that assess patterns of domestic and international telephone calls and emails to uncover linkages with known terrorists. These NSA activities, initiated after al-Qaeda’s deadly 9/11 attacks, have played a vital role in protecting America and our citizens around the world from the still-metastasizing terrorist threat.

The NSA programs do not involve listening to or reading conversations, but rather seek to detect communications networks. If patterns are found, and more detailed investigation seems warranted, then NSA or other federal authorities, consistent with the Fourth Amendment’s prohibition against unreasonable searches and seizures, must obtain judicial approval for more specific investigations. Indeed, even the collection of the so-called metadata is surrounded by procedural protections to prevent spying on U.S. citizens.

Nonetheless, critics from the right and left have attacked the NSA for infringing on the legitimate expectations of privacy Americans enjoy under our Constitution. Unfortunately, many of these critics have absolutely no idea what they are talking about; they are engaging in classic McCarthyite tactics, hoping to score political points with a public justifiably worried about the abuses of power characteristic of the Obama administration. Other critics, following Vietnam-era antipathies to America’s intelligence community, have never reconciled themselves to the need for robust clandestine capabilities. Still others yearn for simpler times, embodying Secretary of State Henry Stimson’s famous comment that “gentlemen don’t read each others’ mail.”

The ill-informed nature of the debate has facilitated scare-mongering, with one wild accusation about NSA’s activities after another being launched before the mundane reality catches up. And there is an important asymmetry at work here as well. The critics can say whatever their imaginations conjure up, but NSA and its defenders are significantly limited in how they can respond. By definition, the programs’ success rests on the secrecy fundamental to all intelligence activities. Frequently, therefore, explaining what is not happening could well reveal information about NSA’s methods and capabilities that terrorists and others, in turn, could use to stymie future detection efforts.

#### Even if the aff is right that terrorism is exaggerated, that doesn’t mean there is *no* threat — planning and preparation is critical.

Lewis 14 — James Andrew Lewis, Ph.D. from U.Chicago, Senior Fellow and Director of the Strategic Technologies Program at the Center for Strategic and International Studies, former member of the U.S. Foreign Service and Senior Executive Service, where he worked on regional security, military intervention and insurgency, conventional arms negotiations, technology transfer, encryption, internet security, space remote sensing, high-tech trade with China, sanctions and Internet policy, led the U.S. delegation to the Wassenaar Arrangement Experts Group for advanced civil and military technologies, assigned to the U.S. Southern Command for Just Cause, the U.S. Central Command for Desert Shield, and to the National Security Council and the U.S. Central American Task Force for programs in Nicaragua, 2015 (“Underestimating Risk in the Surveillance Debate,” CSIS Strategic Technologies Program, December, Available Online at <https://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf>, Accessed 08-08-2015)

The phrase “terrorism” is overused, and the threat of terrorist attack is easily exaggerated, but that does not mean this threat it is nonexistent. Groups and individuals still plan to attack American citizens and the citizens of allied countries. The dilemma in assessing risk is that it is discontinuous. There can be long periods where no activity is apparent, only to have the apparent calm explode in an attack. The constant, low-level activity in planning and preparation in Western countries is not apparent to the public, nor is it easy to identify the moment that discontent turns into action.

### They Say: “No Nuclear Terrorism”

#### Nuclear terrorism is both possible and likely — the effects would be catastrophic.

Bunn et al. 13 — Matthew Bunn, Professor of the Practice of Public Policy at Harvard Kennedy School and Co-Principal Investigator of Project on Managing the Atom at Harvard University’s Belfer Center for Science and International Affairs, Vice Admiral Valentin Kuznetsov (retired Russian Navy), Senior research fellow at the Institute for U.S. and Canadian Studies of the Russian Academy of Sciences, Senior Military Representative of the Russian Ministry of Defense to NATO from 2002 to 2008, Martin Malin, Executive Director of the Project on Managing the Atom at the Belfer Center for Science and International Affairs, Colonel Yuri Morozov (retired Russian Armed Forces), Professor of the Russian Academy of Military Sciences and senior research fellow at the Institute for U.S. and Canadian Studies of the Russian Academy of Sciences, chief of department at the Center for Military-Strategic Studies at the General Staff of the Russian Armed Forces from 1995 to 2000, Simon Saradzhyan, Fellow at Harvard University’s Belfer Center for Science and International Affairs, Moscow-based defense and security expert and writer from 1993 to 2008, William Tobey, Senior fellow at Harvard University’s Belfer Center for Science and International Affairs and director of the U.S.-Russia Initiative to Prevent Nuclear Terrorism, deputy administrator for Defense Nuclear Nonproliferation at the U.S. National Nuclear Security Administration from 2006 to 2009, Colonel General Viktor Yesin (retired Russian Armed Forces, Leading research fellow at the Institute for U.S. and Canadian Studies of the Russian Academy of Sciences and advisor to commander of the Strategic Missile Forces of Russia, chief of staff of the Strategic Missile Forces from 1994 to 1996, Major General Pavel Zolotarev (retired Russian Armed Forces), Deputy director of the Institute for U.S. and Canadian Studies of the Russian Academy of Sciences, head of the Information and Analysis Center of the Russian Ministry of Defense from1993 to 1997, deputy chief of staff of the Defense Council of Russia from 1997 to 1998, 2013 (“Steps to Prevent Nuclear Terrorism: Recommendations Based on the U.S.-Russia Joint Threat Assessment,” Belfer Center for Science and International Affair at Harvard and the Institute for U.S. and Canadian Studies at the Russian Academy of Sciences, September, Available Online at <http://belfercenter.ksg.harvard.edu/files/JTA%20eng%20web2.pdf>, Accessed 08-10-2015)

In 2011, Harvard’s Belfer Center for Science and International Affairs and the Russian Academy of Sciences’ Institute for U.S. and Canadian Studies published “The U.S. – Russia Joint Threat Assessment on Nuclear Terrorism.” The assessment analyzed the means, motives, and access of would-be nuclear terrorists, and concluded that the threat of nuclear terrorism is urgent and real.

The Washington and Seoul Nuclear Security Summits in 2010 and 2012 established and demonstrated a consensus among political leaders from around the world that nuclear terrorism poses a serious threat to the peace, security, and prosperity of our planet. For any country, a terrorist attack with a nuclear device would be an immediate and catastrophic disaster, and the negative effects would reverberate around the world far beyond the location and moment of the detonation.

Preventing a nuclear terrorist attack requires international cooperation to secure nuclear materials, especially among those states producing nuclear materials and weapons. As the world’s two greatest nuclear powers, the United States and Russia have the greatest experience and capabilities in securing nuclear materials and plants and, therefore, share a special responsibility to lead international efforts to prevent terrorists from seizing such materials and plants.

The depth of convergence between U.S. and Russian vital national interests on the issue of nuclear security is best illustrated by the fact that bilateral cooperation on this issue has continued uninterrupted for more than two decades, even when relations between the two countries occasionally became frosty, as in the aftermath of the August 2008 war in Georgia.

Russia and the United States have strong incentives to forge a close and trusting partnership to prevent nuclear terrorism and have made enormous progress in securing fissile material both at home and in partnership with other countries. However, to meet the evolving threat posed by those individuals intent upon using nuclear weapons for terrorist purposes, the United States and Russia need to deepen and broaden their cooperation.

The 2011 “U.S. - Russia Joint Threat Assessment” offered both specific conclusions about the nature of the threat and general observations about how it might be addressed. This report builds on that foundation and analyzes the existing framework for action, cites gaps and deficiencies, and makes specific recommendations for improvement.

“The U.S. – Russia Joint Threat Assessment on Nuclear Terrorism” (The 2011 report executive summary):

• Nuclear terrorism is a real and urgent threat. Urgent actions are required to reduce the risk. The risk is driven by the rise of terrorists who seek to inflict unlimited damage, many of whom have sought justification for their plans in radical interpretations of Islam; by the spread of information about the decades-old technology of nuclear weapons; by the increased availability of weapons-usable nuclear materials; and by globalization, which makes it easier to move people, technologies, and materials across the world.

• Making a crude nuclear bomb would not be easy, but is potentially within the capabilities of a technically sophisticated terrorist group, as numerous government studies have confirmed. Detonating a stolen nuclear weapon would likely be difficult for terrorists to accomplish, if the weapon was equipped with modern technical safeguards (such as the electronic locks known as Permissive Action Links, or PALs). Terrorists could, however, cut open a stolen nuclear weapon and make use of its nuclear material for a bomb of their own.

• The nuclear material for a bomb is small and difficult to detect, making it a major challenge to stop nuclear smuggling or to recover nuclear material after it has been stolen. Hence, a primary focus in reducing the risk must be to keep nuclear material and nuclear weapons from being stolen by continually improving their security, as agreed at the Nuclear Security Summit in Washington in April 2010.

• Al-Qaeda has sought nuclear weapons for almost two decades. The group has repeatedly attempted to purchase stolen nuclear material or nuclear weapons, and has repeatedly attempted to recruit nuclear expertise. Al-Qaeda reportedly conducted tests of conventional explosives for its nuclear program in the desert in Afghanistan. The group’s nuclear ambitions continued after its dispersal following the fall of the Taliban regime in Afghanistan. Recent writings from top al-Qaeda leadership are focused on justifying the mass slaughter of civilians, including the use of weapons of mass destruction, and are in all likelihood intended to provide a formal religious justification for nuclear use.

• While there are significant gaps in coverage of the group’s activities, al-Qaeda appears to have been frustrated thus far in acquiring a nuclear capability; it is unclear whether the the group has acquired weapons-usable nuclear material or the expertise needed to make such material into a bomb. Furthermore, pressure from a broad range of counter-terrorist actions probably has reduced the group’s ability to manage large, complex projects, but has not eliminated the danger. However, there is no sign the group has abandoned its nuclear ambitions. On the contrary, leadership statements as recently as 2008 indicate that the intention to acquire and use nuclear weapons is as strong as ever.

#### Nuclear terrorism is possible even without theft — terrorists can build dirty bombs and gun-style devices easily. Attacks escalate and turn the case.

Dvorkin 12 — Vladimir Z. Dvorkin, Retired Major-General, Head of Research at the Center for Strategic Nuclear Forces at the Russian Academy of Military Sciences, co-authored all of the guideline and policy papers on the development of the Soviet/Russian Strategic Nuclear Forces and Strategic Rocket Forces, took part in the preparation of SALT II, INF, START I and START II, member of the Russian Council on Foreign and Defense Policy, former director of the Research Institute of the Strategic Rocket Forces (RISRF), and actively served in the Russian armed forces for more than twenty years, 2012 (“What Can Destroy Strategic Stability: Nuclear Terrorism Is a Real Threat,” Excerpt Published in English by the Belfer Center at Harvard’s Kennedy School of Government, Original Published in Russian by Nezavisimoye Voyennoye Obozrenie (magazine), September 21st, Available Online at <http://belfercenter.ksg.harvard.edu/publication/22333/what_can_destroy_strategic_stability.html>, Accessed 08-10-2015)

There is growing concern in the world about the threat of nuclear terrorism. There are sufficient grounds for such concerns even though there has been so far no direct evidence of international terrorist organizations conducting work to build improvised nuclear devices. We can assume from statements by certain terrorist organizations affiliated with al-Qaeda that they seek to acquire such devices for propaganda effect only.

Hundreds of scientific papers and reports have been published on nuclear terrorism. International conferences have been held on this threat with participation of Russian organizations, including IMEMO and the Institute of U.S. and Canadian Studies. Recommendations on how to combat the threat have been issued by the International Luxembourg Forum on Preventing Nuclear Catastrophe, Pugwash Conferences on Science and World Affairs, Russian-American Elbe Group, and other organizations. The UN General Assembly adopted the International Convention for the Suppression of Acts of Nuclear Terrorism in 2005 and cooperation among intelligence services of leading states in this sphere is developing.

At the same time, these efforts fall short for a number of reasons, partly because various acts of nuclear terrorism are possible. Dispersal of radioactive material by detonation of conventional explosives (“dirty bombs”) is a method that is most accessible for terrorists. With the wide spread of radioactive sources, raw materials for such attacks have become much more accessible than weapons-useable nuclear material or nuclear weapons. The use of “dirty bombs” will not cause many immediate casualties, but it will result into long-term radioactive contamination, contributing to the spread of panic and socio-economic destabilization.

Severe consequences can be caused by sabotaging nuclear power plants, research reactors, and radioactive materials storage facilities. Large cities are especially vulnerable to such attacks. A large city may host dozens of research reactors with a nuclear power plant or a couple of spent nuclear fuel storage facilities and dozens of large radioactive materials storage facilities located nearby. The past few years have seen significant efforts made to enhance organizational and physical aspects of security at facilities, especially at nuclear power plants. Efforts have also been made to improve security culture. But these efforts do not preclude the possibility that well-trained terrorists may be able to penetrate nuclear facilities.

Some estimates show that sabotage of a research reactor in a metropolis may expose hundreds of thousands to high doses of radiation. A formidable part of the city would become uninhabitable for a long time.

Of all the scenarios, it is building an improvised nuclear device by terrorists that poses the maximum risk. There are no engineering problems that cannot be solved if terrorists decide to build a simple “gun-type” nuclear device. Information on the design of such devices, as well as implosion-type devices, is available in the public domain. It is the acquisition of weapons-grade uranium that presents the sole serious obstacle. Despite numerous preventive measures taken, we cannot rule out the possibility that such materials can be bought on the black market. Theft of weapons-grade uranium is also possible. Research reactor fuel is considered to be particularly vulnerable to theft, as it is scattered at sites in dozens of countries. There are about 100 research reactors in the world that run on weapons-grade uranium fuel, according to the International Atomic Energy Agency (IAEA).

A terrorist “gun-type” uranium bomb can have a yield of least 10-15 kt, which is comparable to the yield of the bomb dropped on Hiroshima. The explosion of such a bomb in a modern metropolis can kill and wound hundreds of thousands and cause serious economic damage. There will also be long-term sociopsychological and political consequences.

The vast majority of states have introduced unprecedented security and surveillance measures at transportation and other large-scale public facilities after the terrorist attacks in the United States, Great Britain, Italy, and other countries. These measures have proved burdensome for the countries’ populations, but the public has accepted them as necessary. A nuclear terrorist attack will make the public accept further measures meant to enhance control even if these measures significantly restrict the democratic liberties they are accustomed to. Authoritarian states could be expected to adopt even more restrictive measures.

If a nuclear terrorist act occurs, nations will delegate tens of thousands of their secret services’ best personnel to investigate and attribute the attack. Radical Islamist groups are among those capable of such an act. We can imagine what would happen if they do so, given the anti-Muslim sentiments and resentment that conventional terrorist attacks by Islamists have generated in developed democratic countries. Mass deportation of the non-indigenous population and severe sanctions would follow such an attack in what will cause violent protests in the Muslim world. Series of armed clashing terrorist attacks may follow. The prediction that Samuel Huntington has made in his book “The Clash of Civilizations and the Remaking of World Order” may come true. Huntington’s book clearly demonstrates that it is not Islamic extremists that are the cause of the Western world’s problems. Rather there is a deep, intractable conflict that is rooted in the fault lines that run between Islam and Christianity. This is especially dangerous for Russia because these fault lines run across its territory.

#### We have entered a new age of mega-terror — terrorists have the means and motive to acquire nuclear weapons.

Allison 12 — Graham Allison, Former US Assistant Secretary of Defense, received the Defense Department's highest civilian award, the Defense Medal for Distinguished Public Service, for "reshaping relations with Russia, Ukraine, Belarus, and Kazakhstan to reduce the former Soviet nuclear arsenal,” Director, Belfer Center for Science and International Affairs at Harvard, Professor of Government, Harvard Kennedy School and currently serves on the Advisory boards of the Secretary of State, Secretary of Defense, and the Director of the CIA, 2012 ("Living in the Era of Megaterror,” International Herald Tribune, republished by the Belfer Center for Science and International Affairs at Harvard’s Kennedy School of Government, September 7th, Available Online at <http://belfercenter.ksg.harvard.edu/publication/22302/living_in_the_era_of_megaterror.html>, Accessed 08-10-2015)

Forty years ago this week at the Munich Olympics of 1972, Palestinian terrorists conducted one of the most dramatic terrorist attacks of the 20th century. The kidnapping and massacre of 11 Israeli athletes attracted days of around-the-clock global news coverage of Black September’s anti-Israel message. Three decades later, on 9/11, Al Qaeda killed nearly 3,000 individuals at the World Trade Center and the Pentagon, announcing a new era of megaterror. In an act that killed more people than Japan’s attack on Pearl Harbor, a band of terrorists headquartered in ungoverned Afghanistan demonstrated that individuals and small groups can kill on a scale previously the exclusive preserve of states.

Today, how many people can a small group of terrorists kill in a single blow? Had Bruce Ivins, the U.S. government microbiologist responsible for the 2001 anthrax attacks, distributed his deadly agent with sprayers he could have purchased off the shelf, tens of thousands of Americans would have died. Had the 2001 “Dragonfire” report that Al Qaeda had a small nuclear weapon (from the former Soviet arsenal) in New York City proved correct, and not a false alarm, detonation of that bomb in Times Square could have incinerated a half million Americans.

In this electoral season, President Obama is claiming credit, rightly, for actions he and U.S. Special Forces took in killing Osama bin Laden. Similarly, at last week’s Republican convention in Tampa, Jeb Bush praised his brother for making the United States safer after 9/11. There can be no doubt that the thousands of actions taken at federal, state and local levels have made people safer from terrorist attacks.

Many are therefore attracted to the chorus of officials and experts claiming that the “strategic defeat” of Al Qaeda means the end of this chapter of history. But we should remember a deeper and more profound truth. While applauding actions that have made us safer from future terrorist attacks, we must recognize that they have not reversed an inescapable reality: The relentless advance of science and technology is making it possible for smaller and smaller groups to kill larger and larger numbers of people.

If a Qaeda affiliate, or some terrorist group in Pakistan whose name readers have never heard, acquires highly enriched uranium or plutonium made by a state, they can construct an elementary nuclear bomb capable of killing hundreds of thousands of people. At biotech labs across the United States and around the world, research scientists making medicines that advance human well-being are also capable of making pathogens, like anthrax, that can produce massive casualties.

What to do? Sherlock Holmes examined crime scenes using a method he called M.M.O.: motive, means and opportunity. In a society where citizens gather in unprotected movie theaters, churches, shopping centers and stadiums, opportunities for attack abound. Free societies are inherently “target rich.”

Motive to commit such atrocities poses a more difficult challenge. In all societies, a percentage of the population will be homicidal. No one can examine the mounting number of cases of mass murder in schools, movie theaters and elsewhere without worrying about a society’s mental health. Additionally, actions we take abroad unquestionably impact others’ motivation to attack us.

As Faisal Shahzad, the 2010 would-be “Times Square bomber,” testified at his trial: “Until the hour the U.S. ... stops the occupation of Muslim lands, and stops killing the Muslims ... we will be attacking U.S., and I plead guilty to that.”

Fortunately, it is more difficult for a terrorist to acquire the “means” to cause mass casualties. Producing highly enriched uranium or plutonium requires expensive industrial-scale investments that only states will make. If all fissile material can be secured to a gold standard beyond the reach of thieves or terrorists, aspirations to become the world’s first nuclear terrorist can be thwarted.

Capabilities for producing bioterrorist agents are not so easily secured or policed. While more has been done, and much more could be done to further raise the technological barrier, as knowledge advances and technological capabilities to make pathogens become more accessible, the means for bioterrorism will come within the reach of terrorists.

One of the hardest truths about modern life is that the same advances in science and technology that enrich our lives also empower potential killers to achieve their deadliest ambitions. To imagine that we can escape this reality and return to a world in which we are invulnerable to future 9/11s or worse is an illusion. For as far as the eye can see, we will live in an era of megaterror.

### They Say: “No Encryption Link”

#### The plan risks catastrophic terrorism.

Weissmann 14 — Andrew Weissmann, Senior Fellow at the Center for Law and Security and the Center on the Administration of Criminal Law at New York University, former General Counsel for the Federal Bureau of Investigation, holds a J.D. from Columbia Law School, 2014 (“Apple, Boyd, and Going Dark,” *Just Security*, October 20th, Available Online at <http://justsecurity.org/16592/apple-boyd-dark/>, Accessed 07-05-2015)

To my mind – although, as in many areas of the law, there is no perfect solution — the cost of a system where we may be more at risk to illegal hacking is outweighed by the vital role lawful electronic interception plays in thwarting crime – including devastating terrorist attacks. Law enforcement and intelligence officials, including most recently FBI Director James Comey, have noted that we all – including criminals — increasingly use non-telephonic means to communicate. The ability to monitor electronic communications is decreasing with every new encryption tool on such communication systems. Law enforcement authorities in the US and overseas rightfully note how such data is critical to solving everyday crimes, such as kidnapping, fraud, child pornography and exploitation, among many others. And at least as important, preventing terrorist attacks requires such ability, as intelligence agencies note (although due to the Snowden leaks, resulting in the public perception that the intelligence community has too much, not too little, access to information, the ramifications from encryption on traditional law enforcement is likely to be relied on by the government in the public debate on this issue).

This is a judgment Congress needs to make, and soon. In weighing the interests, however, it is no answer to say that the government should revert to means other than lawful intercepts obtained through court orders based on probable cause to prevent crimes. The reality of electronic communications is here to stay and plays a vital role in how crimes are perpetrated by allowing people to communicate with conspirators and to carry out their nefarious plans. In this regard, the government and privacy advocates both need to be consistent in their arguments: it is the latter who usually remind us that the advent of smartphones and “big data” makes traditional Fourth Amendment line-drawing obsolete. And they have a point, as the Supreme Court is starting to recognize. But by the same token, it is increasingly important to have an ability to monitor such communications, after meeting the necessary Fourth Amendment standard upon a showing to an independent Article III court.

#### Encryption *exponentially* increases the risk of catastrophic terrorism.

Hosko 14 — Ronald T. Hosko, President of the Law Enforcement Legal Defense Fund, Former Assistant Director of the Criminal Investigative Division at the Federal Bureau of Investigation, 2014 (“Apple and Google’s new encryption rules will make law enforcement’s job much harder,” *Washington Post*, September 23rd, Available Online at http://www.washingtonpost.com/posteverything/wp/2014/09/23/i-helped-save-a-kidnapped-man-from-murder-with-apples-new-encryption-rules-we-never-wouldve-found-him/, Accessed 07-05-2015)

Last week, Apple and Google announced that their new operating systems will be encrypted by default. Encrypting a phone doesn’t make it any harder to tap, or “lawfully intercept” calls. But it does limit law enforcement’s access to a data, contacts, photos and email stored on the phone itself.

That kind information can help law enforcement officials solve big cases quickly. For example, criminals sometimes avoid phone interception by communicating plans via Snapchat or video. Their phones contain contacts, texts, and geo-tagged data that can help police track down accomplices. These new rules will make it impossible for us to access that information. They will create needless delays that could cost victims their lives.\*

Law enforcement officials rely on all kinds of tools to solve crimes and bring criminals to justice. Most investigations don’t rely solely on information from one source, even a smartphone. But without each and every important piece of the investigative puzzle, criminals and those who plan acts destructive to our national security may walk free.

In my last FBI assignments, I was privy to information that regularly demonstrated how criminal actors adapted to law enforcement investigative techniques – how drug conspirators routinely “dropped” their cellphones every 30 days or so, estimating the time it takes agents to identify and develop probable cause on a new device before seeking interception authority; how child predators migrated to technologies like the Onion Router to obfuscate who’s posting and viewing online posting and viewing online images and videos of horrific acts of child abuse.

We shouldn’t give them one more tool.

But the long-used cellular service selling points of clarity and coverage have been overtaken by a new one – concealment. Capitalizing on post-Snowden disclosures fears, Apple and Android have pitched this as a move to protect consumers’ privacy. Don’t misunderstand me — I, too, place a great value on personal privacy. I have little interest in the government collecting and storing all of my texts and e-mails or logging all of my calls.

But Apple’s and Android’s new protections will protect many thousands of criminals who seek to do us great harm, physically or financially. They will protect those who desperately need to be stopped from lawful, authorized, and entirely necessary safety and security efforts. And they will make it impossible for police to access crucial information, even with a warrant.

As Apple and Android trumpet their victories over law enforcement efforts, our citizenry, our Congress, and our media ought to start managing expectations about future law enforcement and national security success. We’ve lived in an era where the term “connecting the dots” is commonly used. If our cutting edge technologies are designed to keep important dots out of the hands of our government, we all might start thinking about how safe and secure we will be when the most tech-savvy, dedicated criminals exponentially increase their own success rates​.

\* Editors note: This story incorrectly stated that Apple and Google’s new encryption rules would have hindered law enforcement’s ability to rescue the kidnap victim in Wake Forest, N.C. This is not the case. The piece has been corrected.

#### The plan substantially increases the risk of catastrophic terrorism.

Rubin 14 — Jennifer Rubin, Columnist and Blogger for the *Washington Post*, holds a J.D. from the University of California-Berkeley, 2014 (“Silicon Valley enables terrorists and criminals,” *Right Turn*—a *Washington Post* blog, October 19th, Available Online at <http://www.washingtonpost.com/blogs/right-turn/wp/2014/10/19/silicon-valley-enables-terrorists-and-criminals/>, Accessed 07-05-2015)

Google chairman Eric Schmidt likes to brag that his company is “on the right side of history.” He pats himself on the back for pulling out of China because of that country’s censoring practices. His company even has a slogan, “Don’t be evil,” meant to remind Google employees that they aspire to the highest ethical standards. But, to be blunt, Google is violating its own “don’t be evil” rule by insisting on encryption technology which locks out anti-terrorist and law enforcement agencies. That gives terrorists and common criminals alike huge protection and puts their fellow Americans at risk.

Benjamin Wittes of the Brookings Institution explains this is not about “encryption,” as some reports characterize it. No one is talking about eliminating encryption, he explains, “Without it, you couldn’t have electronic commerce. Nobody wants to get rid of encryption.” He explains, “The only question is whether there should be government access with lawful process — or not.”

In a scantly covered speech this week, FBI Director James Comey explained:

The issue is whether companies not currently subject to the Communications Assistance for Law Enforcement Act should be required to build lawful intercept capabilities for law enforcement. We aren’t seeking to expand our authority to intercept communications. We are struggling to keep up with changing technology and to maintain our ability to actually collect the communications we are authorized to intercept.

And if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place.

Encryption is nothing new. But the challenge to law enforcement and national security officials is markedly worse, with recent default encryption settings and encrypted devices and networks—all designed to increase security and privacy.

With Apple’s new operating system, the information stored on many iPhones and other Apple devices will be encrypted by default. Shortly after Apple’s announcement, Google announced plans to follow suit with its Android operating system. This means the companies themselves won’t be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mail, and recordings stored within.

That is a problem that is not solved, as Apple claims, by providing access to the cloud. “But uploading to the cloud doesn’t include all of the stored data on a bad guy’s phone, which has the potential to create a black hole for law enforcement,” Comey said. “And if the bad guys don’t back up their phones routinely, or if they opt out of uploading to the cloud, the data will only be found on the encrypted devices themselves. And it is people most worried about what’s on the phone who will be most likely to avoid the cloud and to make sure that law enforcement cannot access incriminating data.”

In fact, the blocked phones are simply part of a marketing pitch to cater to young people who are misinformed and paranoid about what information the government has access to. Comey observed that “it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It’s the equivalent of a closet that can’t be opened. A safe that can’t be cracked. And my question is, at what cost?”

Well, some terrorists will use it to plan and execute murderous schemes, organized crime will use it to hide from law enforcement and the American people will be less safe and less secure.

Maybe the president (whose party benefits from liberal high-tech donors) should call these people in for a chat and explain why they should stop this. Alternatively, Congress should hold open hearings and have these execs explain why they want to give terrorists an e-hideout. Then again, maybe concerned Americans who want to combat terrorists should simply not use these products. (Hang onto your old phone until they drop the “locked safe,” for example.) What President Obama, Congress and the American people should not do is sit idly by while they put us at risk for pecuniary gain.

Comey went out of his way to be nice to these companies: “Both companies are run by good people, responding to what they perceive is a market demand.” Too nice, in my mind. Instead he should have just told them flat out, “Don’t be evil.”

# Affirmative

## 2AC

### 2AC — Terrorism DA

#### 1. No immanent terror threat — *every* dire warning has proven wrong. The government is *oh-for-forty*.

Timm 15 — Trevor Timm, Co-Founder and Executive Director of the Freedom of the Press Foundation, Columnist for the *Guardian* on privacy, free speech, and national security, former Activist and Writer with the Electronic Frontier Foundation, holds a J.D. from New York Law School and a B.A. in Political Science from Northeastern University, 2015 (“Here’s how not to report on the US government’s terror warnings,” *Columbia Journalism Review*, July 10th, Available Online at <http://www.cjr.org/analysis/heres_how_not_to_report_on_the_us_governments_terror_warnings.php>, Accessed 07-12-2015)

If you turned on the television or checked your phone in the lead up to July 4th, it was almost impossible to miss the wall-to-wall coverage blaring ominous warnings from the US government: ISIS terrorists could strike Americans at any minute over the holiday weekend.

As it often is in such instances, the media’s reporting was breathless, hyperbolic, and barely contained a hint of skepticism. When nothing happened—as has been the case literally every time the government has issued these warnings in the past—there was no apparent self-reflection by these media outlets about how they could have tempered their coverage.

Instead, many doubled down by re-writing government press releases, claiming that arrests that happened well before July 4th, and in which the alleged criminals never mentioned the American holiday, are proof of “just how close” the US came to a terror attack over the holiday weekend.

During the Bush administration, terror alerts were issued with such frequency that they were widely derided and criticized—even by seasoned counter-terrorism experts. Now that ISIS has emerged, the Bush administration’s derided “color code system” is gone, but the willingness of the media to immediately buy into the idea that the public should be freaking out is still alive and well. The last two years have seen the media become much more skeptical of government surveillance powers. Yet when the terror alert flashes, they revert right back to their old ways.

Last weekend’s coverage was a case study in rash judgment. All the caveats issued with the warning’s release were hardly noticeable, downplayed and buried in the middle of the articles, sandwiched in-between urgent calls for caution from various government agencies.

There will soon be a next time; the government will issue a warning, and the media will inevitably jump. When it does, the first rule of reporting should be to determine whether the alerts are based on anything at all and to put that information in the lede. Authorities flatly acknowledged two weeks ago that they have no “credible” or “specific” information that any attacks will occur, but that barely registered in the media’s coverage.

CBS News waited until the sixth paragraph in one of their main articles on the subject to tell its readers of the mitigating information. USA Today also stuck the phrase in the middle of its sixth paragraph and never returned to it. CNN, with a finely honed talent for siren headlines, didn’t disclose this information until their 10th paragraph.

NBC News, though, was the most brazen. They told readers that authorities “are unaware of any specific or credible threat inside the country” in the 7th paragraph, quickly followed by a qualifier that could not contain more hyperbole if they tried: “But the dangers are more complex and unpredictable than ever.” Really? Apparently the dangers are more complex and unpredictable than ever if you ignore the fact that terrorism attacks in the US are close to all-time lows, and that Americans have generally never been safer.

[Graphic Omitted]

None of these major news stories mentioned that the US government had issued similar terrorism warnings that generated alarming headlines at least forty times since 9/11. As FAIR’s Adam Johnson detailed, all forty times nothing happened. If news organizations are going to list all the reasons readers should be scared, they should at least attempt to note the reasons that they probably shouldn’t be.

#### 2. Link Not Unique — the USA Freedom Act curtailed surveillance in June. If the link were true, that should have triggered terrorist attacks.

#### 3. Turn: Data Overload — mass surveillance *causes* terrorism. Data mining overloads systems and trades off with effective strategies.

Schneier 15 — Bruce Schneier, Chief Technology Officer for Counterpane Internet Security, Fellow at the Berkman Center for Internet and Society at Harvard Law School, Program Fellow at the New America Foundation's Open Technology Institute, Board Member of the Electronic Frontier Foundation, Advisory Board Member of the Electronic Privacy Information Center, 2015 (“Why Mass Surveillance Can't, Won't, And Never Has Stopped A Terrorist,” *Digg* — excerpt from *Data and Goliath*, March 24th, Available Online at https://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist, Accessed 07-12-2015)

The NSA repeatedly uses a connect-the-dots metaphor to justify its surveillance activities. Again and again — after 9/11, after the Underwear Bomber, after the Boston Marathon bombings — government is criticized for not connecting the dots.

However, this is a terribly misleading metaphor. Connecting the dots in a coloring book is easy, because they’re all numbered and visible. In real life, the dots can only be recognized after the fact.

That doesn’t stop us from demanding to know why the authorities couldn’t connect the dots. The warning signs left by the Fort Hood shooter, the Boston Marathon bombers, and the Isla Vista shooter look obvious in hindsight. Nassim Taleb, an expert on risk engineering, calls this tendency the “narrative fallacy.” Humans are natural storytellers, and the world of stories is much more tidy, predictable, and coherent than reality. Millions of people behave strangely enough to attract the FBI’s notice, and almost all of them are harmless. The TSA’s no-fly list has over 20,000 people on it. The Terrorist Identities Datamart Environment, also known as the watch list, has 680,000, 40% of whom have “no recognized terrorist group affiliation.”

Data mining is offered as the technique that will enable us to connect those dots. But while corporations are successfully mining our personal data in order to target advertising, detect financial fraud, and perform other tasks, three critical issues make data mining an inappropriate tool for finding terrorists.

The first, and most important, issue is error rates. For advertising, data mining can be successful even with a large error rate, but finding terrorists requires a much higher degree of accuracy than data-mining systems can possibly provide.

Data mining works best when you’re searching for a well-defined profile, when there are a reasonable number of events per year, and when the cost of false alarms is low. Detecting credit card fraud is one of data mining’s security success stories: all credit card companies mine their transaction databases for spending patterns that indicate a stolen card. There are over a billion active credit cards in circulation in the United States, and nearly 8% of those are fraudulently used each year. Many credit card thefts share a pattern — purchases in locations not normally frequented by the cardholder, and purchases of travel, luxury goods, and easily fenced items — and in many cases data-mining systems can minimize the losses by preventing fraudulent transactions. The only cost of a false alarm is a phone call to the cardholder asking her to verify a couple of her purchases.

Similarly, the IRS uses data mining to identify tax evaders, the police use it to predict crime hot spots, and banks use it to predict loan defaults. These applications have had mixed success, based on the data and the application, but they’re all within the scope of what data mining can accomplish.

Terrorist plots are different, mostly because whereas fraud is common, terrorist attacks are very rare. This means that even highly accurate terrorism prediction systems will be so flooded with false alarms that they will be useless.

The reason lies in the mathematics of detection. All detection systems have errors, and system designers can tune them to minimize either false positives or false negatives. In a terrorist-detection system, a false positive occurs when the system mistakenly identifies something harmless as a threat. A false negative occurs when the system misses an actual attack. Depending on how you “tune” your detection system, you can increase the number of false positives to assure you are less likely to miss an attack, or you can reduce the number of false positives at the expense of missing attacks.

Because terrorist attacks are so rare, false positives completely overwhelm the system, no matter how well you tune. And I mean completely: millions of people will be falsely accused for every real terrorist plot the system finds, if it ever finds any.

We might be able to deal with all of the innocents being flagged by the system if the cost of false positives were minor. Think about the full-body scanners at airports. Those alert all the time when scanning people. But a TSA officer can easily check for a false alarm with a simple pat-down. This doesn’t work for a more general data-based terrorism-detection system. Each alert requires a lengthy investigation to determine whether it’s real or not. That takes time and money, and prevents intelligence officers from doing other productive work. Or, more pithily, when you’re watching everything, you’re not seeing anything.

The US intelligence community also likens finding a terrorist plot to looking for a needle in a haystack. And, as former NSA director General Keith Alexander said, “you need the haystack to find the needle.” That statement perfectly illustrates the problem with mass surveillance and bulk collection. When you’re looking for the needle, the last thing you want to do is pile lots more hay on it. More specifically, there is no scientific rationale for believing that adding irrelevant data about innocent people makes it easier to find a terrorist attack, and lots of evidence that it does not. You might be adding slightly more signal, but you’re also adding much more noise. And despite the NSA’s “collect it all” mentality, its own documents bear this out. The military intelligence community even talks about the problem of “drinking from a fire hose”: having so much irrelevant data that it’s impossible to find the important bits.

We saw this problem with the NSA’s eavesdropping program: the false positives overwhelmed the system. In the years after 9/11, the NSA passed to the FBI thousands of tips per month; every one of them turned out to be a false alarm. The cost was enormous, and ended up frustrating the FBI agents who were obligated to investigate all the tips. We also saw this with the Suspicious Activity Reports —or SAR — database: tens of thousands of reports, and no actual results. And all the telephone metadata the NSA collected led to just one success: the conviction of a taxi driver who sent $8,500 to a Somali group that posed no direct threat to the US — and that was probably trumped up so the NSA would have better talking points in front of Congress.

The second problem with using data-mining techniques to try to uncover terrorist plots is that each attack is unique. Who would have guessed that two pressure-cooker bombs would be delivered to the Boston Marathon finish line in backpacks by a Boston college kid and his older brother? Each rare individual who carries out a terrorist attack will have a disproportionate impact on the criteria used to decide who’s a likely terrorist, leading to ineffective detection strategies.

The third problem is that the people the NSA is trying to find are wily, and they’re trying to avoid detection. In the world of personalized marketing, the typical surveillance subject isn’t trying to hide his activities. That is not true in a police or national security context. An adversarial relationship makes the problem much harder, and means that most commercial big data analysis tools just don’t work. A commercial tool can simply ignore people trying to hide and assume benign behavior on the part of everyone else. Government data-mining techniques can’t do that, because those are the very people they’re looking for.

Adversaries vary in the sophistication of their ability to avoid surveillance. Most criminals and terrorists — and political dissidents, sad to say — are pretty unsavvy and make lots of mistakes. But that’s no justification for data mining; targeted surveillance could potentially identify them just as well. The question is whether mass surveillance performs sufficiently better than targeted surveillance to justify its extremely high costs. Several analyses of all the NSA’s efforts indicate that it does not.

The three problems listed above cannot be fixed. Data mining is simply the wrong tool for this job, which means that all the mass surveillance required to feed it cannot be justified. When he was NSA director, General Keith Alexander argued that ubiquitous surveillance would have enabled the NSA to prevent 9/11. That seems unlikely. He wasn’t able to prevent the Boston Marathon bombings in 2013, even though one of the bombers was on the terrorist watch list and both had sloppy social media trails — and this was after a dozen post-9/11 years of honing techniques. The NSA collected data on the Tsarnaevs before the bombing, but hadn’t realized that it was more important than the data they collected on millions of other people.

This point was made in the 9/11 Commission Report. That report described a failure to “connect the dots,” which proponents of mass surveillance claim requires collection of more data. But what the report actually said was that the intelligence community had all the information about the plot without mass surveillance, and that the failures were the result of inadequate analysis.

Mass surveillance didn’t catch underwear bomber Umar Farouk Abdulmutallab in 2006, even though his father had repeatedly warned the U.S. government that he was dangerous. And the liquid bombers (they’re the reason governments prohibit passengers from bringing large bottles of liquids, creams, and gels on airplanes in their carry-on luggage) were captured in 2006 in their London apartment not due to mass surveillance but through traditional investigative police work. Whenever we learn about an NSA success, it invariably comes from targeted surveillance rather than from mass surveillance. One analysis showed that the FBI identifies potential terrorist plots from reports of suspicious activity, reports of plots, and investigations of other, unrelated, crimes.

This is a critical point. Ubiquitous surveillance and data mining are not suitable tools for finding dedicated criminals or terrorists. We taxpayers are wasting billions on mass-surveillance programs, and not getting the security we’ve been promised. More importantly, the money we’re wasting on these ineffective surveillance programs is not being spent on investigation, intelligence, and emergency response: tactics that have been proven to work. The NSA's surveillance efforts have actually made us less secure.

#### 4. No Internal Link — NSA surveillance has never stopped a single attack.

Schneier 15 — Bruce Schneier, Chief Technology Officer for Counterpane Internet Security, Fellow at the Berkman Center for Internet and Society at Harvard Law School, Program Fellow at the New America Foundation's Open Technology Institute, Board Member of the Electronic Frontier Foundation, Advisory Board Member of the Electronic Privacy Information Center, interviewed by Felix Macherez, 2015 (“This Security Expert Reckons Mass Surveillance Doesn't Stop Terror Attacks,” *Vice*, June 26th, Available Online at https://www.vice.com/en\_uk/read/bruce-schneier-mass-surveillance-wont-stop-terror-876, Accessed 07-12-2015)

*Is there any proof that the omnipresent surveillance that exists in the US – on the internet, with phone conversations – has actually helped to stop terrorist attacks in the past?*

No. It's now a clear fact that the mass surveillance performed in the US has never stopped a single attack. On several occasions, the government was asked to justify its surveillance methods, and they have failed to ever do so. Sometimes, they provide scenarios and vague plans, but the data never withstands any test.

*Are there better ways of stopping terrorist attacks then in your opinion?*

What works and has proven efficient several times in the US, is to use "conventional" detective techniques – just following the clues. However there's an important caveat here: no method of surveillance or inquiry will ever stop a lone gunman.

There are simply never enough hints to stop the aggressor before he acts in such cases. Individuals such as the Fort Hood shooter, or Anders Behring Breivik , or the Charlie Hebdo attackers in France, will always be a problem. Early intervention aimed at identifying and helping troubled individuals before they become murderers is the only real solution here.

#### 5. Data Not Key — the government doesn’t need more data — it doesn’t understand or share the data it already has.

Bergen et al. 14 — Peter Bergen, Director of the National Security Program at the New America Foundation, Professor of Practice at the School of Politics and Global Studies and Co-Director of the Center on the Future of War at Arizona State University, Research Fellow at the Center on National Security at Fordham University, National Security Analyst for CNN, has taught at the John F. Kennedy School of Government at Harvard University and the School of Advanced International Studies at Johns Hopkins University, holds an M.A. in Modern History from New College (Oxford), et al., with David Sterman, Research Assistant at the New America Foundation, holds an M.A. in Security Studies from Georgetown University and a B.A. in Political Science and Government from Dartmouth College, Emily Schneider, Research Assistant at the New America Foundation, holds a J.D. in National Security and Counterterrorism Law from Syracuse University College of Law, an M.A. in English from the University of Rochester, and a B.A. in English from Penn State University, and Bailey Cahall, Research Associate at the New America Foundation, holds an M.A. in Global Security and Foreign Policy from the Maxwell School of Citizenship and Public Affairs at Syracuse University and a B.A. in History from West Virginia University, 2014 (“Do NSA's Bulk Surveillance Programs Stop Terrorists?,” New America Foundation, January 13th, Available Online at <http://www.newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists>, Accessed 08-09-2015)

Additionally, a careful review of three of the key terrorism cases the government has cited to defend NSA bulk surveillance programs reveals that government officials have exaggerated the role of the NSA in the cases against David Coleman Headley and Najibullah Zazi, and the significance of the threat posed by a notional plot to bomb the New York Stock Exchange.

In 28 percent of the cases we reviewed, court records and public reporting do not identify which specific methods initiated the investigation. These cases, involving 62 individuals, may have been initiated by an undercover informant, an undercover officer, a family member tip, other traditional law enforcement methods, CIA- or FBI-generated intelligence, NSA surveillance of some kind, or any number of other methods. In 23 of these 62 cases (37 percent), an informant was used. However, we were unable to determine whether the informant initiated the investigation or was used after the investigation was initiated as a result of the use of some other investigative means. Some of these cases may also be too recent to have developed a public record large enough to identify which investigative tools were used.

We have also identified three additional plots that the government has not publicly claimed as NSA successes, but in which court records and public reporting suggest the NSA had a role. However, it is not clear whether any of those three cases involved bulk surveillance programs.

Finally, the overall problem for U.S. counterterrorism officials is not that they need vaster amounts of information from the bulk surveillance programs, but that they don’t sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement and intelligence techniques. This was true for two of the 9/11 hijackers who were known to be in the United States before the attacks on New York and Washington, as well as with the case of Chicago resident David Coleman Headley, who helped plan the 2008 terrorist attacks in Mumbai, and it is the unfortunate pattern we have also seen in several other significant terrorism cases.

#### 6. Terror Threat Exaggerated — there have been zero major attacks since 9/11.

#### 7. No Nuclear Terrorism Impact — problems with acquisition, theft, construction and delivery.

Mearsheimer 14 — John J. Mearsheimer, Ph.D. in Government from Cornell, Distinguished Service Professor of Political Science and chair of the Political Science Department at the University of Chicago, co-director of the Program on International Security Policy, faculty member in the Committee on International Relations graduate program, member of the Advisory Council of The National Interest, former Fellow at the Council on Foreign Relations in New York, 2014 (“America Unhinged,” The National Interest, No. 129, Jan/Feb, Available Online at <http://mearsheimer.uchicago.edu/pdfs/America%20Unhinged.pdf>, Accessed 08-10-2015)

Am I overlooking the obvious threat that strikes fear into the hearts of so many Americans, which is terrorism? Not at all. Sure, the United States has a terrorism problem. But it is a minor threat. There is no question we fell victim to a spectacular attack on September 11, but it did not cripple the United States in any meaningful way and another attack of that magnitude is highly unlikely in the foreseeable future. Indeed, there has not been a single instance over the past twelve years of a terrorist organization exploding a primitive bomb on American soil, much less striking a major blow. Terrorism—most of it arising from domestic groups—was a much bigger problem in the United States during the 1970s than it has been since the Twin Towers were toppled.

What about the possibility that a terrorist group might obtain a nuclear weapon? Such an occurrence would be a game changer, but the chances of that happening are virtually nil. No nuclear-armed state is going to supply terrorists with a nuclear weapon because it would have no control over how the recipients might use that weapon.1 Political turmoil in a nuclear armed state could in theory allow terrorists to grab a loose nuclear weapon, but the United States already has detailed plans to deal with that highly unlikely contingency.

Terrorists might also try to acquire fissile material and build their own bomb. But that scenario is extremely unlikely as well: there are significant obstacles to getting enough material and even bigger obstacles to building a bomb and then delivering it. More generally, virtually every country has a profound interest in making sure no terrorist group acquires a nuclear weapon, because they cannot be sure they will not be the target of a nuclear attack, either by the terrorists or another country the terrorists strike. Nuclear terrorism, in short, is not a serious threat. And to the extent that we should worry about it, the main remedy is to encourage and help other states to place nuclear materials in highly secure custody.

### 2AC — No Encryption Link

#### No Encryption Link — strong encryption *doesn’t* foster terrorism.

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

BI: Won't the proliferation of encryption help terrorists?

BS: No. It's the exact opposite: encryption is one of the things that protects us from terrorists, criminals, foreign intelligence, and every other threat on the Internet, and against our data and communications. Encryption protects our trade secrets, our financial transactions, our medical records, and our conversations. In a world where cyberattacks are becoming more common and more catastrophic, encryption is one of our most important defenses.

In 2010, the US Deputy Secretary of Defense William Lynn wrote: "Although the threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyberthreat that the United States will face over the long term." Encryption protects against intellectual property theft, and it also protects critical national infrastructure.

What you're asking is much more narrow: won't terrorists be able to use encryption to protect their secrets? Of course they will. Like so many other aspects of our society, the benefits of encryption are general and can be enjoyed by both the good guys and the bad guys. Automobiles benefit both long-distance travelers and bank robbers. Telephones benefit both distant relatives and kidnappers. Late-night all-you-can-eat buffets benefit both hungry students and terrorists plotting their next moves.

This is simply reality. And there are two reasons it's okay. One, good people far outnumber bad people in society, so we manage to thrive nonetheless. And two, the bad guys trip themselves up in so many other ways that allowing them access to automobiles, telephones, late-night restaurants, and encryption isn't enough to make them successful.

Most of the time we recognize that harming the overwhelming number of honest people in society to try to harm the few bad people is a dumb trade-off. Consider an analogy: Cameron is unlikely to demand that cars redesign their engines so as to limit their speeds to 60 kph so bank robbers can't get away so fast. But he doesn't understand the comparable trade-offs in his proposed legislation.

## 1AR

### They Say: “DA Turns Case – Rollback”

#### DA doesn’t “turn case” — NSA programs aren’t effective. Ending surveillance *now* is key to civil liberties.

Dawson 13 — Tyler Dawson, Reporter at the *Low Down to Hull and Back News*—a regional newspaper in Quebec, former Reporter at the *Edmonton Journal* and *Ottawa Citizen*, holds an M.A. in Journalism from Carleton University and a B.A. in History and Political Science from the University of Alberta, 2013 (“A Response to Tom Friedman on Spying,” Tyler Dawson’s blog, June 12th, Available Online at <https://tylerdawson.wordpress.com/2013/06/12/a-response-to-tom-friedman-on-spying/>, Accessed 08-10-2015)

The latest defence of spying comes from the vastly overpraised New York Times columnist Tom L. Friedman.

In his latest, entitled “Blowing a Whistle,” Friedman frets in a roundabout fashion: if the NSA did not mine data, then there would be another terrorist attack, and then Congress would crush our civil liberties as we know them.

In his own words:

I believe that if there is one more 9/11 — or worse, an attack involving nuclear material — it could lead to the end of the open society as we know it. If there were another 9/11, I fear that 99 percent of Americans would tell their members of Congress: “Do whatever you need to do to, privacy be damned, just make sure this does not happen again.” That is what I fear most.

Undoubtedly, if there was another 9/11, there would be a further rollback on American civil liberties. However, does that justify a preemptive invasion of those very liberties?

I don’t think so.

Without reverting to the old quotes from the Founding Fathers about the tradeoff between liberty and security, it seems obvious to me that this sort of justification is a sorry one, and unbecoming to someone as accomplished as Friedman. If there is to be a national debate in the United States on the limits of privacy, it doesn’t really do that much good to hypothesize about future infringements on liberties.

Here, now, on June 12, 2013, there is a clear infringement on civil liberties.

We know that this information has been used in many of the President’s briefings.

What we don’t know is exactly what this information — gathered by mining metadata and monitoring phone conversations — has actually prevented. Were there imminent attacks thwarted? Terrorists scooped up? Terrorist organizations dismantled? Nuclear weapons intercepted?

Anyone with even a passing knowledge of foreign affairs knows that al-Qaeda is on the run institutionally. It is fractured in many parts of the world, and without clear leadership. Affiliates in Somalia, for example, are also on the verge of elimination.

There has been no evidence that these programs have done anything to increase the security of the United States.

There is no way of knowing if the NSA program has prevented attacks — though, in defending it, you’d think the White House could march out at least one example, if it has been even remotely useful.

I haven’t heard of one, and frankly, even if one does exist, is there any reason to think that slightly more old-fashioned methods wouldn’t have yielded the same result?

Each time there is a thwarted attempt, this is used as a justification for further invasions of privacy, more stringent screening and surrender of liberty. That’s a convenient argument, but here, the logical fallacy in Friedman’s argument is that this program is worth preserving, because it will prevent more terrorist attacks, when there is no indication the program has done anything.

It is, in my view, better to shore up the bulwark of liberty today, and fight for the rollback of a potentially illegal and certainly unethical program.

Imagine how many real restrictions to our beautiful open society we would tolerate if there were another attack on the scale of 9/11. Pardon me if I blow that whistle.

Absolutely … but does granting a free pass to such an invasive system of spying today guarantee Americans’ safety (and, incidentally, Canadians’ as well)? And, if another attack were to happen, acquiescence in a time of relative security (ie. now) does little to offset any further attempts to curtail freedoms.

Best to fight against infringements, both now, and later, unless the government can damn well prove it’s actually doing anything useful.

At the moment, I can’t see any evidence of this.

#### No rollback — Boston bombing proves that terrorism doesn’t increase surveillance.

Hayes 13 — Danny Hayes, associate professor of political science at George Washington University, focusing on political communication and political behavior; co-author of *Influence from Abroad*, a book about Americans' views toward U.S. foreign policy, 2013 (“Why the Boston Marathon bombing won’t erode civil liberties,” Wonkblog, The Washington Post, April 28th, Available Online at <http://www.washingtonpost.com/blogs/wonkblog/wp/2013/04/28/why-the-boston-maraton-bombing-wont-erode-civil-liberties/>, Accessed 06-21-2013)

From the moment that Boston bombing suspect Dzhokhar Tsarnaev was pulled out of a boat in Watertown, Mass., the debate over civil liberties and domestic anti-terrorism policies, largely dormant in recent years, was reignited.

Noting that “the homeland is the battlefield,” Sen. Lindsey Graham (R-S.C.) urged the Obama administration to designate Tsarnaev, an American citizen, as an enemy combatant. Civil liberties groups then objected when authorities decided not to read Miranda rights to the Boston Marathon bombing suspect, invoking a public safety exception. Speculation also arose that police might now find it easier to persuade the public to support the use of surveillance technology and domestic drones. “After Boston,” Ryan Gallagher wrote this week in Slate, “the balance in the struggle between privacy and security may swing back in their favor.”

But research conducted shortly after 9/11, combined with some recent polling data, suggests that Americans may be unlikely to trade civil liberties for a greater sense of security as a result of the bombing. That’s because the attack hasn’t made the public significantly more fearful of future domestic terrorism, and because trust in government is low.

After 9/11, concern over terrorism skyrocketed. In a Gallup survey fielded in the days before the attack, less than one-half of one percent of Americans said terrorism was the country’s most important problem. But in October 2001, 46 percent did. These worries boosted support for legislation, such as the USA PATRIOT Act, that expanded law enforcement’s power to investigate suspected terrorism, even as those measures were criticized for eroding civil liberties protections.

In a survey conducted between November 2001 and January 2002, political scientists Darren Davis and Brian Silver designed a series of questions to explore the tradeoffs between security and civil liberties. They began by asking people whether they agreed more with the statement that “in order to curb terrorism in this country, it will be necessary to give up some civil liberties” or that “we should preserve our freedoms above all, even if there remains some risk of terrorism.” Forty-five percent of Americans chose the first option, indicating a willingness to give up some freedoms in exchange for greater security.

When respondents were asked about the tradeoffs involving specific measures, there was wide variation. Davis and Silver found that very few Americans – eight percent – believed that the government should have the power to investigate people who participate in nonviolent protests. And just 18 percent said they supported racial profiling. But when asked, for instance, whether they agreed that “high school teachers have the right to criticize America’s policies toward terrorism” or that “high school teachers should defend America’s policies in order to promote loyalty to our country,” 60 percent said teachers should back the government.

Perhaps not surprisingly, the biggest influence on whether people were willing to offer pro-security over pro-civil liberties responses was their fear of a second attack. Respondents who believed another terrorist act was imminent were more likely to support tradeoffs in favor of security. Importantly, Davis and Silver found that the relationship was strongest among people who expressed high levels of political trust: People who believe the government typically does the right thing and who were fearful of another terrorist attack were the most willing to relinquish civil liberties protections.

Those findings are consistent with a series of studies by Stanley Feldman, Leonie Huddy and their colleagues at Stony Brook University. In one survey conducted between October 2001 and March 2002, the researchers found that 86 percent of Americans said they were “very” or “somewhat” concerned about another domestic terrorist act. The greater the concern, the more likely respondents were to support the use of government-issued ID cards and allowing authorities to monitor phone calls and e-mail.

But in contrast to 9/11, polling since the Boston Marathon suggests that the bombing has made Americans only slightly more fearful of future terrorist attacks than they were beforehand. Fifty-eight percent of respondents in a Pew poll conducted April 18-21 said they were “very” or “somewhat” worried about another attack on the United States. That was no higher, however, than when the same question was asked in November 2010. And it was significantly lower than the 71 percent who said they were worried in October 2001.

A slightly different question in a Washington Post poll taken April 17-18 found that 69 percent of Americans said that the possibility of a major terrorist attack worried them either “a great deal” or “somewhat.” That figure was only a few percentage points higher than when the same question was asked in 2007 and 2008.

In addition, political trust is lower today than it was in 2001, when public confidence in government rose sharply after the terrorist attacks. If Davis and Silver’s findings are correct, then greater skepticism of government – produced in part by the struggling economy – should limit the public’s willingness to give law enforcement more latitude.

Ultimately, the scope of the Boston tragedy was smaller than 9/11, which could help explain its limited effect on the public. It may also be that because Americans believe terrorist attacks are now a fundamental part of life in the United States, any single event will have a more muted effect on public opinion. And because the Tsarnaev brothers have not been connected to any known terrorist organizations, Americans may feel less under siege than they did when al-Qaeda and Osama bin Laden were identified as the perpetrators of the 2001 attacks.

Regardless of the reason, all of this suggests that policymakers are likely to face a more difficult task than they did after 9/11 in persuading the public to support additional security measures that infringe on Americans’ freedoms.

#### “Turns case” is not unique — Friedman is wrong.

Rothschild 13 — Matthew Rothschild, Senior Editor of *The Progressive* magazine, holds a B.A. in Social Studies and Political Philosophy from Harvard University, 2013 (“See Tom Friedman Go Along with the NSA,” *The Progressive*, June 12th, Available Online at <http://www.progressive.org/news/2013/06/182670/see-tom-friedman-go-along-nsa>, Accessed 08-05-2015)

New York Times columnist Thomas Friedman hit a new low with his piece today on the NSA spying scandal.

Basically, he says he's willing to give away some of his freedom today for fear that the government will take more of it away tomorrow if we're attacked again.

He says he wants "to prevent a day where, out of fear, we give government a license to look at anyone, any e-mail, any phone call, anywhere, anytime."

Problem is, we're just about there already.

Where's he been the last week?

Friedman does express a worry that I've been writing about for years now: that if there is another 9/11, "it could lead to the end of the open society as we know it."

See "Is Martial Law Coming?" and "The FBI Deputizes Business."

But the rational response to that worry is not to agree to start amputating our rights, but to demand public hearings on what our government has in store for us if we are attacked again, and to insist that we are able to remain free, as have citizens of other countries that have faced terrorist attacks.

And how much of our freedom is Friedman willing to sacrifice in his acquiescence, for fear that there is worse to come?

Then Friedman uses the second half of his column to lifting massive quotes from David Simon of "The Wire," who says, "We don't know of any actual abuse."

Of course, we don't: The NSA holds all the evidence!

Friedman writes that "what I cherish most about America is our open society."

It sure doesn't seem like it from this column.

### Extend: “No Immanent Terror Threat”

#### Now isn’t key — threat alerts are *always* wrong.

Johnson 15 — Adam Johnson, Associate Editor at *AlterNet*, Frequent Contributor to *FAIR: Fairness & Accuracy in Reporting*—a national media watchdog group, 2015 (“Zero for 40 at Predicting Attacks: Why Do Media Still Take FBI Terror Warnings Seriously?,” *FAIR: Fairness & Accuracy in Reporting*, July 1st, Available Online at <http://fair.org/home/zero-for-40-at-predicting-attacks-why-do-media-still-take-fbi-terror-warnings-seriously/>, Accessed 07-12-2015)

On Monday, several mainstream media outlets repeated the latest press release by the FBI that country was under a new “heightened terror alert” from “ISIL-inspired attacks” “leading up to the July 4th weekend.” One of the more sensational outlets, CNN, led with the breathless warning on several of its cable programs, complete with a special report by The Lead’s Jim Sciutto in primetime:

[Image Omitted]

The threat was given extra credence when former CIA director—and consultant at DC PR firm Beacon Global Strategies—Michael Morell went on CBS This Morning (6/29/15) and scared the ever-living bejesus out of everyone by saying he “wouldn’t be surprised if we were sitting [in the studio] next week discussing an attack on the US.” The first piece of evidence Morell used to justify his apocalyptic posture, the “50 ISIS arrests,” was accompanied by a scary map on the CBS jumbotron showing “ISIS arrests” all throughout the US:

[Image Omitted]

But one key detail is missing from this graphic: None of these “ISIS arrests” involved any actual members of ISIS, only members of the FBI—and their network of informants—posing as such. (The one exception being the man arrested in Arizona, who, while having no contact with ISIS, was also not prompted by the FBI.) So even if one thinks the threat of “lone wolf” attacks is a serious one, it cannot be said these are really “ISIS arrests.” Perhaps on some meta-level, it shows an increase of “radicalization,” but it’s impossible to distinguish between this and simply more aggressive sting operations by the FBI.

In any event, this nuance gets left out entirely. As I’ve previously shown, in the media’s rush to hype the threat, the fact of FBI-manufactured—or at least “assisted”—terror plots is left out as a complicating factor altogether, and the viewer is left thinking the FBI arrested 50 actual ISIS sleeper cells.

Nevertheless, the ominous FBI (or Department of Homeland Security) “terror warning” has become such a staple of the on-going, seemingly endless “war on terror” (d/b/a war on ISIS), we hardly even notice it anymore. Marked by a feedback loop of extremist propaganda, unverifiable claims about “online chatter” and fuzzy pronouncements issued by a neverending string of faceless Muslim bad guys, and given PR cover by FBI-contrived “terror plots,” the specter of the impending “attack” is part of a broader white noise of fear that never went away after 9/11. Indeed, the verbiage employed by the FBI in this latest warning —“we’re asking people to remain vigilant”—implies no actual change of the status quo, just an hysterical nudge to not let down our collective guard.

There’s only one problem: These warnings never actually come to fruition. Not rarely, or almost never, but—by all accounts—never. No attacks, no arrests, no suspects at large.

Here’s a selection of previous FBI and DHS “terror warnings” over the past 14 years, not a single one of which actually predicted or foiled a terror attack:

October 2001: “Potential use of chemical/biological and/or radiological/nuclear weapons“

November 2001: California bridges

February 2002: “Hollywood studios”

May 2002: Statue of Liberty

June 2002: “Around the Fourth of July holiday”

July 2002: Stadiums

August 2002: “Landmarks”

October 2002: “AQ to attack Amtrak”

November 2002: “Spectacular Al Qaeda attacks”

February 2003: “Apartments, hotels, sports arenas and amusement parks“

May 2003: “Possibility of multiple attacks”

May 2004: “Attempt to affect the outcome” of presidential election

July 2004: “Military facilities and large gatherings” on July 4th

August 2004: VA hospitals

January 2005: Dirty bomb

March 2005: US/Mexican border

October 2005: NYC & Baltimore subways

March 2006: “Sporting events”

June 2007: Colleges

December 2007: “Shopping malls in Chicago and LA”

November 2008: “Al Qaeda to attack transit during Thanksgiving”

November 2010: Mass transit in New York City

October 2011: “Americans in Europe” facing “commando-style AQ attack”

February 2011: “Financial institutions”

May 2011: “Threats of retaliation”

June 2011: Al Qaeda “hit list”

July 2011: “Private jets of executives” involved in drone manufacturing

September 2011: “Small planes”

September 2011: “New York City or Washington around…10th anniversary of 9/11”

September 2011: Airports

March 2012: “Terrorist hacking”

August 2012: Anarchists blowing up bridge during Tampa RNC

September 2012: “Islamic violence over movie”

August 2013: “San Fransisco on high alert”

November 2013: “cyber attacks”

April 2014: “College students abroad”

December 2014: ISIS targeting Mississippi River bridge

December 2014: ISIS “sabotaging US military personnel” over social media

April 2015: ISIS targeting “parts of California”

May 2015: ISIS targeting “military bases”

A casual search reveals the FBI and DHS are a pitiful 0 for 40 warning of terror attacks—some of which were specifically about 4th of July threats, none of which materialized in any way. This should not be considered a comprehensive list of all threat warnings transmitted by media; I tried to narrow the scope to warnings that were at least in some way specific.

The actual terror attacks carried out on US soil—the Times Square bomber, “Underwear bomber,” Boston bombing and Garland attacks—were accompanied by no such warnings. (Nor were the often deadlier terrorist attacks by right-wing white terrorists–but terrorism in this category is rarely if ever the subject of FBI warnings.)

So why, a rational person may ask, does the media keeps repeating them if they’re wrong 100 percent of the time?

The problem is three fold:

1. The FBI has all the incentive in the world to issue warnings and no incentive whatsoever to not issue warnings. Issuing warnings has no downside, while not doing so is all downside.

2. The FBI, like all agencies of the government, does not operate in a political vacuum. Emphasizing the “ISIS threat” at home necessarily helps prop up the broader war effort the FBI’s boss, the president of the United States, must sell to a war-weary public. The incentive is to therefore highlight the smallest threats. This was a feature that did not go unnoticed during the Bush years, but has since fallen out of fashion.

3. It has no actual utility. What does it mean to be “more vigilant”? It’s a vague call to alertness that officials, aside from “beefing up security” by local police, never quite explain what it means. If the FBI wanted to tell local police departments to up their security of the 4th of July weekend, surely they could do so quietly, without the chair of the House Committee on Homeland Security having to go on all major networks talking over b-roll of ISIS in apocalyptic terms.

#### There were no “July 4th” attacks — reports are fabricated to avoid embarrassment over the terror alert hype.

Gosztola 15 — Kevin Gosztola, journalist, author, and documentary filmmaker known for work on whistleblowers, Wikileaks, national security, secrecy, civil liberties, and digital freedom, has written for The *Nation*, *Salon*, and *OpEdNews*, 2015 (“Podcast: The Threat of Unspecified Terrorism Attacks by People Who Shall Not Be Named is Very Real,” *Firedoglake*—a progressive news site, July 12th, Available Online at http://firedoglake.com/2015/07/12/podcast-the-threat-of-unspecified-terrorism-attacks-by-people-who-shall-not-be-named-is-very-real/, Accessed 07-12-2015)

There were no Islamic State-inspired terrorism attacks on or around the Fourth of July in the United States, but CNN and other major US media organizations expended much energy spreading fear far and wide so Americans would be on edge throughout the holiday weekend. And, when nothing happened, FBI Director James Comey fabricated claims that terrorism suspects arrested in June were at one point prepared to attack on July 4.

At least ten individuals were said to have been arrested with Islamic State ties. These were the people, who the FBI allegedly stopped from attacking Americans on Independence Day, and that justified all the hysteria in the media around potential terrorism. However, the government’s own complaints against them contain no allegations that any of their planned acts were being timed to coincide with the holiday.

Officially, the FBI would not back up its claims with specifics. “We are not providing any information beyond what you’re seeing in media reports. There was no information provided on specific individual[s] or what they hoped to do,” an FBI spokesperson replied to a request for evidence.

### Extend: “USA Freedom Act Curtailed Surveillance”

#### The USA Freedom Act limited NSA authority — the link is non-unique.

Washington Post 15 — Washington Post, Byline Mike Debonis, Congressional reporter for the Washington Post, 2015 ("Congress turns away from post-9/11 law, retooling U.S. surveillance powers," Washington Post, June 2nd, Available Online at https://www.washingtonpost.com/politics/senate-moves-ahead-with-retooling-of-us-surveillance-powers/2015/06/02/28f5e1ce-092d-11e5-a7ad-b430fc1d3f5c\_story.html, Accessed 08-09-2015)

Congress on Tuesday rejected some of the sweeping intelligence-gathering powers it granted national security officials after the 9/11 terrorist attacks, with the Senate voting to end the government’s bulk collection of private telephone records and to reform other surveillance policies.

The bill, known as the USA Freedom Act, passed on a 67-to-32 vote, against the will of Senate Republican leaders who wished to preserve existing spy programs.

The opposition to the bill, led by Majority Leader Mitch McConnell (R-Ky.), prompted an intraparty standoff that exposed sharp splits along philosophical and generational lines, and between the two chambers on Capitol Hill. The standoff led to a two-day lapse in the legal authority for those programs.

The bill passed by a wide margin in the House last month but languished as those who sought to maintain the status quo, led by McConnell, tried to stare down Sen. Rand Paul (R-Ky.) and the other senators who supported either ending or reforming the most controversial provisions of the surveillance programs.

“It does not enhance the privacy protections of American citizens, and it surely compromises American security by taking one more tool from our war fighters, in my view, at exactly the wrong time,” McConnell said Tuesday, minutes before colleagues rejected a series of amendments he favored.

The USA Freedom Act represents the first legislative overhaul passed in response to the 2013 disclosures of former National Security Agency contractor Edward Snowden, who revealed the NSA’s bulk collection of telephone “metadata” and the legal rationale for it — the little-noticed Section 215 of the USA Patriot Act, passed in the months after the Sept. 11, 2001, attacks.

The new legislation places additional curbs on that authority, most significantly by mandating a six-month transition to a system in which the call data — which includes call numbers, times and durations — would remain in private company hands but could be searched on a case-by-case basis under a court order. One supporter, Sen. Patrick J. Leahy (D-Vt.), described the legislation as “the most significant surveillance reform in decades.”

#### USA Freedom Act just limited surveillance of phone metadata — that should have caused the impact.

ABC News 15 — ABC News, 2015 ("Freedom Act to limit domestic surveillance signed into US law by president Barack Obama," ABC News, June 3rd, Available Online at http://www.abc.net.au/news/2015-06-03/us-congress-passes-bill-to-limit-domestic-surveillance/6516826, Accessed 08-09-2015)

US president Barack Obama has signed into law legislation ending spy agencies' bulk collection of Americans' telephone records, reversing a national security policy that had been in place since shortly after the September 11 attacks in 2001.

The Senate passed the USA Freedom Act by a vote of 67-32, with support from both Democrats and Republicans, after passing the House of Representatives last month.

After the vote the bill was swiftly handed to Mr Obama, who tweeted his promise to "sign it as soon as I get it".

"My administration will work expeditiously to ensure our national security professionals again have the full set of vital tools they need to continue protecting the country," Mr Obama said.

Senator Patrick Leahy, the senior Democratic sponsor of the bill, said: "It's a historic moment."

He described the bill as "the first major overhaul of government surveillance laws in decades".

The measure replaces a program in which the National Security Agency swept up data about Americans' telephone calls — including telephone numbers and dates and times of calls, but not content — with a more targeted system.

It also shifts responsibility for storing the data to telephone companies, allowing authorities to access the information only with a warrant from a secret counter-terror court that identifies a specific person or group of people suspected of having ties to terrorism.

### Extend: “Data Overload Turn”

#### Mass surveillance causes attacks — data overload led to the failure to prevent every terrorist attack this century. Even government reports agree.

Eddington 15 — Patrick G. Eddington, policy analyst in homeland security and civil liberties at the Cato Institute, former senior policy advisor to Rep. Rush Holt (D-N.J.), former CIA military imagery analyst, 2015 ("No, Mass Surveillance Won't Stop Terrorist Attacks," Cato Institute, January 27th Available Online at http://www.cato.org/publications/commentary/no-mass-surveillance-wont-stop-terrorist-attacks, Accessed 08-09-2015)

But would more mass surveillance have prevented the assault on the Charlie Hebdo office? Events from 9/11 to the present help provide the answer:

2009: Umar Farouk Abdulmutallab—i.e., the “underwear bomber”—nearly succeeded in downing the airline he was on over Detroit because, according to then-National Counterterrorism Center (NCC) director Michael Leiter, the federal Intelligence Community (IC) failed “to connect, integrate, and fully understand the intelligence” it had collected.

2009: Army Major Nidal Hasan was able to conduct his deadly, Anwar al-Awlaki-inspired rampage at Ft. Hood, Texas, because the FBI bungled its Hasan investigation.

2013: The Boston Marathon bombing happened, at least in part, because the CIA, Department of Homeland Security (DHS), FBI, NCC, and National Security Agency (NSA) failed to properly coordinate and share information about Tamerlan Tsarnaev and his family, associations, and travel to and from Russia in 2012. Those failures were detailed in a 2014 report prepared by the Inspectors General of the IC, Department of Justice, CIA, and DHS.

2014: The Charlie Hebdo and French grocery store attackers were not only known to French and U.S. authorities but one had a prior terrorism conviction and another was monitored for years by French authorities until less than a year before the attack on the magazine.

No, mass surveillance does not prevent terrorist attacks.

It’s worth remembering that the mass surveillance programs initiated by the U.S. government after the 9/11 attacks—the legal ones and the constitutionally-dubious ones—were premised on the belief that bin Laden’s hijacker-terrorists were able to pull off the attacks because of a failure to collect enough data. Yet in their subsequent reports on the attacks, the Congressional Joint Inquiry (2002) and the 9/11 Commission found exactly the opposite. The data to detect (and thus foil) the plots was in the U.S. government’s hands prior to the attacks; the failures were ones of sharing, analysis, and dissemination. That malady perfectly describes every intelligence failure from Pearl Harbor to the present day.

The Office of the Director of National Intelligence (created by Congress in 2004) was supposed to be the answer to the “failure-to-connect-the-dots” problem. Ten years on, the problem remains, the IC bureaucracy is bigger than ever, and our government is continuing to rely on mass surveillance programs that have failed time and again to stop terrorists while simultaneously undermining the civil liberties and personal privacy of every American. The quest to “collect it all,” to borrow a phrase from NSA Director Keith Alexander, only leads to the accumulation of masses of useless information, making it harder to find real threats and costing billions to store.

A recent Guardian editorial noted that such mass-surveillance myopia is spreading among European political leaders as well, despite the fact that “terrorists, from 9/11 to the Woolwich jihadists and the neo-Nazi Anders Breivik, have almost always come to the authorities’ attention before murdering.”

Mass surveillance is not only destructive of our liberties, its continued use is a virtual guarantee of more lethal intelligence failures. And our continued will to disbelieve those facts is a mental dodge we engage in at our peril.

#### Mass surveillance hurts the ability to find terrorists — our data overload turn is mathematically proven.

Corrigan 15 — Ray Corrigan, Senior Lecturer in Mathematics, Computing and Technology at The Open University, author of 'Digital Decision Making: Back to the Future', 2015 ("Mass surveillance not effective for finding terrorists," New Scientist, January 15th, Available Online at https://www.newscientist.com/article/dn26801-mass-surveillance-not-effective-for-finding-terrorists/, Accessed 08-09-2015)

Police, intelligence and security systems are imperfect. They process vast amounts of imperfect intelligence data and do not have the resources to monitor all known suspects 24/7. The French authorities lost track of these extremists long enough for them to carry out their murderous acts. You cannot fix any of this by treating the entire population as suspects and then engaging in suspicionless, blanket collection and processing of personal data.

Mass data collectors can dig deeply into anyone’s digital persona but don’t have the resources to do so with everyone. Surveillance of the entire population, the vast majority of whom are innocent, leads to the diversion of limited intelligence resources in pursuit of huge numbers of false leads. Terrorists are comparatively rare, so finding one is a needle in a haystack problem. You don’t make it easier by throwing more needleless hay on the stack.

It is statistically impossible for total population surveillance to be an effective tool for catching terrorists.

Even if your magic terrorist-catching machine has a false positive rate of 1 in 1000 – and no security technology comes anywhere near this – every time you asked it for suspects in the UK it would flag 60,000 innocent people.

Law enforcement and security services need to be able to move with the times, use modern digital technologies intelligently and through targeted data preservation – not a mass surveillance regime – to engage in court-supervised technological surveillance of individuals whom they have reasonable cause to suspect. That is not, however, the same as building an infrastructure of mass surveillance.

Mass surveillance makes the job of the security services more difficult and the rest of us less secure.

### Extend: “Government Doesn’t Need More Data”

#### Mass surveillance *can’t* stop terrorism — too much data.

Schneier 15 — Bruce Schneier, Chief Technology Officer for Counterpane Internet Security, Fellow at the Berkman Center for Internet and Society at Harvard Law School, Program Fellow at the New America Foundation's Open Technology Institute, Board Member of the Electronic Frontier Foundation, Advisory Board Member of the Electronic Privacy Information Center, interviewed by Felix Macherez, 2015 (“This Security Expert Reckons Mass Surveillance Doesn't Stop Terror Attacks,” *Vice*, June 26th, Available Online at https://www.vice.com/en\_uk/read/bruce-schneier-mass-surveillance-wont-stop-terror-876, Accessed 07-12-2015)

*VICE: The NSA uses the metaphor "connecting the dots" to justify its surveillance activities. However the US government actually struggles to ever connect those dots. Why is that?*

Bruce Schneier: There is too much external noise when you do mass surveillance. The problem is that "connecting the dots" is neither the right method nor the right metaphor. When you look at a child's colouring book, connecting the dots is very easy because they are all visible – they are all on the same page and they have numbers written on them. All you have to do is move the lead of your pencil across your page, from one dot to the other, and there you go – the drawing is done.

In reality, those "dots" can only be seen and connected after things have occurred – so after each terrorist attack, if you want. When you look, it's easy to make the link between, say, an information request coming from Russia, a visit abroad, and other potential information gathered elsewhere. So with hindsight, we know who the terrorists are. That's why we're able to chase after them, but not stop them. Before an event occurs, there is an extremely huge number of potential "human dangers," and an even greater number of possible scenarios. There are so many variables to take into account that it's impossible to rely on a single potential course of events.

*You're saying that mass surveillance cannot really stop terrorist attacks in the US. Would you say the same for France?*

Mass surveillance is unreliable for statistical reasons, not for cultural or linguistic reasons. That analysis is valid for all countries, including France.

#### Efficiency of collection is a lie — the government doesn’t investigate quickly even when they have NSA data.

Bergen et al. 14 — Peter Bergen, Director of the National Security Program at the New America Foundation, Professor of Practice at the School of Politics and Global Studies and Co-Director of the Center on the Future of War at Arizona State University, Research Fellow at the Center on National Security at Fordham University, National Security Analyst for CNN, has taught at the John F. Kennedy School of Government at Harvard University and the School of Advanced International Studies at Johns Hopkins University, holds an M.A. in Modern History from New College (Oxford), et al., with David Sterman, Research Assistant at the New America Foundation, holds an M.A. in Security Studies from Georgetown University and a B.A. in Political Science and Government from Dartmouth College, Emily Schneider, Research Assistant at the New America Foundation, holds a J.D. in National Security and Counterterrorism Law from Syracuse University College of Law, an M.A. in English from the University of Rochester, and a B.A. in English from Penn State University, and Bailey Cahall, Research Associate at the New America Foundation, holds an M.A. in Global Security and Foreign Policy from the Maxwell School of Citizenship and Public Affairs at Syracuse University and a B.A. in History from West Virginia University, 2014 (“Do NSA's Bulk Surveillance Programs Stop Terrorists?,” New America Foundation, January 13th, Available Online at <http://www.newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists>, Accessed 08-09-2015)

Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group. Furthermore, our examination of the role of the database of U.S. citizens’ telephone metadata in the single plot the government uses to justify the importance of the program – that of Basaaly Moalin, a San Diego cabdriver who in 2007 and 2008 provided $8,500 to al-Shabaab, al-Qaeda’s affiliate in Somalia – calls into question the necessity of the Section 215 bulk collection program. According to the government, the database of American phone metadata allows intelligence authorities to quickly circumvent the traditional burden of proof associated with criminal warrants, thus allowing them to “connect the dots” faster and prevent future 9/11-scale attacks. Yet in the Moalin case, after using the NSA’s phone database to link a number in Somalia to Moalin, the FBI waited two months to begin an investigation and wiretap his phone. Although it’s unclear why there was a delay between the NSA tip and the FBI wiretapping, court documents show there was a two-month period in which the FBI was not monitoring Moalin’s calls, despite official statements that the bureau had Moalin’s phone number and had identified him. This undercuts the government’s theory that the database of Americans’ telephone metadata is necessary to expedite the investigative process, since it clearly didn’t expedite the process in the single case the government uses to extol its virtues.

### Extend: “Surveillance Has Never Stopped an Attack”

#### Disregard any evidence that refers to 50 terrorist attacks or the ability to prevent 9/11 — this is a thoroughly debunked lie.

Cohn and Kayyali 14 — Cindy Cohn, JD from Michigan, Executive Director of the Electronic Frontier Foundation, former EFF Legal Director and General Counsel, lead attorney in Bernstein v. Dept. of Justice, the successful First Amendment challenge to the U.S. export restrictions on cryptography, named by the National Law Journal as one of the 100 most influential lawyers in America (2013), one of the 50 most influential female lawyers in America (2007), winner of the State Bar of California’s Intellectual Property Vanguard Award, and Nadia Kayyali, JD from UC Hastings, member of EFF’s activism team in surveillance, national security policy and digital civil liberties, former Bill of Rights Defense Committee Legal Fellow, former Community Outreach Editor for the Hastings Race and Poverty Law Journal, 2014 ("The Top 5 Claims That Defenders of the NSA Have to Stop Making to Remain Credible," Electronic Frontier Foundation, June 2nd , Available Online at https://www.eff.org/deeplinks/2014/06/top-5-claims-defenders-nsa-have-stop-making-remain-credible, Accessed 08-09-2015)

Over the past year, as the Snowden revelations have rolled out, the government and its apologists have developed a set of talking points about mass spying that the public has now heard over and over again. From the President, to Hilary Clinton to Rep. Mike Rogers, Sen. Dianne Feinstein and many others, the arguments are often eerily similar.

But as we approach the one year anniversary, it’s time to call out the key claims that have been thoroughly debunked and insist that the NSA apologists retire them.

So if you hear any one of these in the future, you can tell yourself straight up: “this person isn’t credible,” and look elsewhere for current information about the NSA spying. And if these are still in your talking points (you know who you are) it’s time to retire them if you want to remain credible. And next time, the talking points should stand the test of time.

1. The NSA has Stopped 54 Terrorist Attacks with Mass Spying

The discredited claim

NSA defenders have thrown out many claims about how NSA surveillance has protected us from terrorists, including repeatedly declaring that it has thwarted 54 plots. Rep. Mike Rogers says it often. Only weeks after the first Snowden leak, US President Barack Obama claimed: “We know of at least 50 threats that have been averted” because of the NSA’s spy powers. Former NSA Director Gen. Keith Alexander also repeatedly claimed that those programs thwarted 54 different attacks.

Others, including former Vice President Dick Cheney have claimed that had the bulk spying programs in place, the government could have stopped the 9/11 bombings, specifically noting that the government needed the program to locate Khalid al Mihdhar, a hijacker who was living in San Diego.

Why it’s not credible:

These claims have been thoroughly debunked. First, the claim that the information stopped 54 terrorist plots fell completely apart. In dramatic Congressional testimony, Sen. Leahy forced a formal retraction from NSA Director Alexander in October, 2013:

"Would you agree that the 54 cases that keep getting cited by the administration were not all plots, and of the 54, only 13 had some nexus to the U.S.?" Leahy said at the hearing. "Would you agree with that, yes or no?"

"Yes," Alexander replied, without elaborating.

But that didn’t stop the apologists. We keep hearing the “54 plots” line to this day.

As for 9/11, sadly, the same is true. The government did not need additional mass collection capabilities, like the mass phone records programs, to find al Mihdhar in San Diego. As ProPublica noted, quoting Bob Graham, the former chair of the Senate Intelligence Committee:

U.S. intelligence agencies knew the identity of the hijacker in question, Saudi national Khalid al Mihdhar, long before 9/11 and had the ability find him, but they failed to do so.

"There were plenty of opportunities without having to rely on this metadata system for the FBI and intelligence agencies to have located Mihdhar," says former Senator Bob Graham, the Florida Democrat who extensively investigated 9/11 as chairman of the Senate’s intelligence committee.

Moreover, Peter Bergen and a team at the New America Foundation dug into the government’s claims about plots in America, including studying over 225 individuals recruited by al Qaeda and similar groups in the United States and charged with terrorism, and concluded:

Our review of the government’s claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading...

When backed into a corner, the government’s apologists cite the capture of Zazi, the so-called New York subway bomber. However, in that case, the Associated Press reported that the government could have easily stopped the plot without the NSA program, under authorities that comply with the Constitution. Sens. Ron Wyden and Mark Udall have been saying this for a long time.

Both of the President’s hand-picked advisors on mass surveillance concur about the telephone records collection. The President’s Review Board issued a report in which it stated “the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks,” The Privacy and Civil Liberties Oversight Board (PCLOB) also issued a report in which it stated, “we have not identified a single instance involving a threat to the United States in which [bulk collection under Section 215 of the Patriot Act] made a concrete difference in the outcome of a counterterrorism investigation.”

And in an amicus brief in EFF’s case First Unitarian Church of Los Angeles v. the NSA case, Sens. Ron Wyden, Mark Udall, and Martin Heinrich stated that, while the administration has claimed that bulk collection is necessary to prevent terrorism, they “have reviewed the bulk-collection program extensively, and none of the claims appears to hold up to scrutiny.”

Even former top NSA official John Inglis admitted that the phone records program has not stopped any terrorist attacks aimed at the US and at most, helped catch one guy who shipped about $8,000 to a Somalian group that the US has designated as a terrorist group but that has never even remotely been involved in any attacks aimed at the US.

#### The negative’s evidence about the effectiveness of surveillance is biased and misleading — it comes from government exaggerations, not detailed studies.

Bergen et al. 14 — Peter Bergen, Director of the National Security Program at the New America Foundation, Professor of Practice at the School of Politics and Global Studies and Co-Director of the Center on the Future of War at Arizona State University, Research Fellow at the Center on National Security at Fordham University, National Security Analyst for CNN, has taught at the John F. Kennedy School of Government at Harvard University and the School of Advanced International Studies at Johns Hopkins University, holds an M.A. in Modern History from New College (Oxford), et al., with David Sterman, Research Assistant at the New America Foundation, holds an M.A. in Security Studies from Georgetown University and a B.A. in Political Science and Government from Dartmouth College, Emily Schneider, Research Assistant at the New America Foundation, holds a J.D. in National Security and Counterterrorism Law from Syracuse University College of Law, an M.A. in English from the University of Rochester, and a B.A. in English from Penn State University, and Bailey Cahall, Research Associate at the New America Foundation, holds an M.A. in Global Security and Foreign Policy from the Maxwell School of Citizenship and Public Affairs at Syracuse University and a B.A. in History from West Virginia University, 2014 (“Do NSA's Bulk Surveillance Programs Stop Terrorists?,” New America Foundation, January 13th, Available Online at <http://www.newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists>, Accessed 08-09-2015)

On June 5, 2013, the Guardian broke the first story in what would become a flood of revelations regarding the extent and nature of the NSA’s surveillance programs. Facing an uproar over the threat such programs posed to privacy, the Obama administration scrambled to defend them as legal and essential to U.S. national security and counterterrorism. Two weeks after the first leaks by former NSA contractor Edward Snowden were published, President Obama defended the NSA surveillance programs during a visit to Berlin, saying: “We know of at least 50 threats that have been averted because of this information not just in the United States, but, in some cases, threats here in Germany. So lives have been saved.” Gen. Keith Alexander, the director of the NSA, testified before Congress that: “the information gathered from these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world.” Rep. Mike Rogers (R-Mich.), chairman of the House Permanent Select Committee on Intelligence, said on the House floor in July that “54 times [the NSA programs] stopped and thwarted terrorist attacks both here and in Europe – saving real lives.”

However, our review of the government’s claims about the role that NSA “bulk” surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading. An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda’s ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA’s bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, which includes the telephone numbers that originate and receive calls, as well as the time and date of those calls but not their content, under Section 215 of the USA PATRIOT Act, appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases. NSA programs involving the surveillance of non-U.S. persons outside of the United States under Section 702 of the FISA Amendments Act played a role in 4.4 percent of the terrorism cases we examined, and NSA surveillance under an unidentified authority played a role in 1.3 percent of the cases we examined.

### Extend: “Terror Threat Exaggerated”

#### The threat of domestic jihadi terrorism is massively overblown.

Greenwald and Begley 15 — Glenn Greenwald, journalist who received the 2014 Pulitzer Prize for Public Service for his work with Edward Snowden to report on NSA surveillance, Founding Editor of *The Intercept*, former Columnist for the *Guardian* and *Salon*, recipient of the Park Center I.F. Stone Award for Independent Journalism, the Online Journalism Award for investigative work on the abusive detention conditions of Chelsea Manning, the George Polk Award for National Security Reporting, the Gannett Foundation Award for investigative journalism, the Gannett Foundation Watchdog Journalism Award, the Esso Premio for Excellence in Investigative Reporting in Brazil, and the Electronic Frontier Foundation’s Pioneer Award, holds a J.D. from New York University School of Law, and Josh Begley, Research Editor specializing in artistic design at *The Intercept*, 2015 (“The Greatest Obstacle to Anti-Muslim Fear-Mongering and Bigotry: Reality,” *The Intercept*, June 24th, Available Online at <https://firstlook.org/theintercept/2015/06/24/greatest-obstacle-anti-muslim-fear-mongering-bigotry-reality/>, Accessed 06-24-2015)

The think tank New America issued a report today documenting “the lethal terrorist incidents in the United States since 9/11.” It found that a total of 26 Americans have been killed by “deadly jihadist attacks” in the last 14 years, while almost double that number – 48 – have been killed by “deadly right wing attacks.” The significance of that finding was well-captured by the New York Times‘ online home page caption today, promoting the paper’s article that included this quote from Terrorism Professor John Horgan: “There’s an acceptance now of the idea that the threat from jihadi terrorism in the United States has been overblown.”

[Graphic of the NYT headline omitted]

That the U.S. Government, media and various anti-Muslim polemicists relentlessly, aggressively exaggerate “the terror threat” generally and the menace of Muslims specifically requires no studies to see. It’s confirmed by people’s every day experiences. On the list of threats that Americans wake up and worry about every morning, is there anyone beyond hypnotic Sean Hannity viewers for whom “terrorism by radical Islam” is high on the list?

To believe the prevailing U.S. government/media narrative is to believe that radical Islam poses some sort of grave threat to the safety of American families. The fear-mongering works not because it resonates in people’s daily experiences and observations: it plainly does not. It works because it’s grounded in tribalistic appeals (our tribe is better than that one over there) and the Otherizing of the marginalized (those people over there are not just different but inferior): historically very potent tactics of manipulation and propaganda. Add to that all the pragmatic benefits from maintaining this Scary Muslim mythology – the power, profit and policy advancement it enables for numerous factions – and it’s not hard to see why it’s been so easily sustained despite being so patently false.

It’s literally hard to overstate how trivial the risk of “radical Islam” is to the average American. So consider this: [chart translated from image to text]

In The United States…

96 people killed in car accidents every day

62 people killed by bees, wasps, or hornets in 2013

48 people killed by right-wing extremists since 9/11

32 people killed by lightning every year

27 people crushed by their own furniture every year

26 people killed by Muslim extremists since 9/11

(Sources: deaths from traffic accidents; deaths from bees; deaths from lightning; deaths from furniture; deaths from right-wing extremists)

If anything, the chart severely understates how exaggerated the threat is, since it compares the total number of deaths caused by “Muslim extremists” over the past 14 years to the number of deaths caused daily or annually by threats widely regarded as insignificant. This is the “threat” in whose name the U.S. and its western allies have radically reduced basic legal protections; created all sorts of dangerous precedents for invasions, detentions, and targeted killings; and generally driven themselves to a state of collective hysteria and manipulation.

#### Don’t trust NSA’s numbers *even though* some info is classified.

Van Dongen 13 — Teun van Dongen, National Security Expert and a Ph.D. Candidate in Counterterrorism Studies at Leiden University, former Analyst at The Hague Centre for Strategic Studies where he worked for the Dutch National Coordinator for Security and Counterterrorism, 2013 (“The NSA Isn’t Foiling Terrorist Plots,” *Foreign Policy In Focus*, October 8th, Available Online at <http://fpif.org/nsa-isnt-foiling-terrorist-plots/>, Accessed 07-09-2015)

What about the NSA?

Admittedly we do not know how all terrorist plots have been detected. But going by what we do know, the conclusion is simple: terrorist plots have been foiled in all sorts of ways, few of which had anything to do with mass digital surveillance. True, in the case of the dismantlement of the Sauerland Cell in Germany in 2007, NSA information played a role. But whether the authorities got this information from “digital dragnet surveillance” or from more individualized and targeted monitoring is hard to tell.

It might be tempting to give the NSA the benefit of the doubt, given that the organization speaks on the basis of information that we do not have. But such dubious claims about the effectiveness of the digital surveillance programs fit seamlessly into a pattern of misinformation and deceit. The U.S. government acknowledged the existence of PRISM only after Edward Snowden had leaked details about it to The Guardian. Moreover, when the news broke, President Obama and Director of National Intelligence James Clapper tried to downplay the scale of the digital data gathering, even though we know now that the NSA is essentially making a back-up of pretty much all conceivable forms of online communication. President Obama further promised that “nobody is listening to your phone calls,” but it later became clear that the NSA can access the content of phone calls and e-mails if it so desires. Congressional oversight is poor, privacy rules are frequently broken, and the NSA liberally shares data with other intelligence agencies and foreign governments.

Against this background of disputed or outright false government claims, the public is wise to be skeptical of the NSA’s claims about the effectiveness of the digital surveillance programs. The recent revelations may be mind-boggling in their technological, legal, and procedural complexities, but the bottom line is quite simple: The first credible piece of evidence that these programs are doing any good in the fight against terrorism has yet to surface. Until such evidence is provided, the Obama administration is only eroding the trust of the citizens it is claiming to protect.

### Extend: “No Nuclear Terrorism”

#### No risk of nuclear terror — people consistently over-estimate the risk.

Walt 12 — Stephen Walt, professor of international relations and Academic Dean at Harvard University’s Kennedy School of Government, serves on the editorial boards of Foreign Policy, Security Studies, International Relations, and the Journal of Cold War Studies, and as Co-Editor of the Cornell Studies in Security Affairs, elected a Fellow in the American Academy of Arts and Sciences, former professor at Princeton University and the University of Chicago, where he served as Master of the Social Science Collegiate Division and Deputy Dean of Social Sciences, 2012 ("What terrorist threat?," Foreign Policy, August 13th, Available Online at http://foreignpolicy.com/2012/08/13/what-terrorist-threat/, Accessed 08-11-2015)

Remember how the London Olympics were supposedly left vulnerable to terrorists after the security firm hired for the games admitted that it couldn’t supply enough manpower? This "humiliating shambles" forced the British government to call in 3,500 security personnel of its own, and led GOP presidential candidate Mitt Romney to utter some tactless remarks about Britain’s alleged mismanagement during his official "Foot-in-Mouth" foreign tour last month.

Well, surprise, surprise. Not only was there no terrorist attack, the Games themselves came off rather well. There were the inevitable minor glitches, of course, but no disasters and some quite impressive organizational achievements. And of course, athletes from around the world delivered inspiring, impressive, heroic, and sometimes disappointing performances, which is what the Games are all about.

Two lessons might be drawn from this event. The first is that the head-long rush to privatize everything — including the provision of security — has some obvious downsides. When markets and private firms fail, it is the state that has to come to the rescue. It was true after the 2007-08 financial crisis, it’s true in the ongoing euro-mess, and it was true in the Olympics. Bear that in mind when Romney and new VP nominee Paul Ryan tout the virtues of shrinking government, especially the need to privatize Social Security and Medicare.

The second lesson is that we continue to over-react to the "terrorist threat." Here I recommend you read John Mueller and Mark G. Stewart’s The Terrorism Delusion: America’s Overwrought Response to September 11, in the latest issue of International Security. Mueller and Stewart analyze 50 cases of supposed "Islamic terrorist plots" against the United States, and show how virtually all of the perpetrators were (in their words) "incompetent, ineffective, unintelligent, idiotic, ignorant, unorganized, misguided, muddled, amateurish, dopey, unrealistic, moronic, irrational and foolish." They quote former Glenn Carle, former deputy national intelligence officer for transnational threats saying "we must see jihadists for the small, lethal, disjointed and miserable opponents that they are," noting further that al Qaeda’s "capabilities are far inferior to its desires."

Further, Mueller and Stewart estimate that expenditures on domestic homeland security (i.e., not counting the wars in Iraq or Afghanistan) have increased by more than $1 trillion since 9/11, even though the annual risk of dying in a domestic terrorist attack is about 1 in 3.5 million. Using conservative assumptions and conventional risk-assessment methodology, they estimate that for these expenditures to be cost-effective "they would have had to deter, prevent, foil or protect against 333 very large attacks that would otherwise have been successful every year." Finally, they worry that this exaggerated sense of danger has now been "internalized": even when politicians and "terrorism experts" aren’t hyping the danger, the public still sees the threat as large and imminent. As they conclude:

… Americans seems to have internalized their anxiety about terrorism, and politicians and policymakers have come to believe that they can defy it only at their own peril. Concern about appearing to be soft on terrorism has replaced concern about seeming to be soft on communism, a phenomenon that lasted far longer than the dramatic that generated it … This extraordinarily exaggerated and essentially delusional response may prove to be perpetual."

Which is another way of saying that you should be prepared to keep standing in those pleasant and efficient TSA lines for the rest of your life, and to keep paying for far-flung foreign interventions designed to "root out" those nasty jihadis.

#### No nuclear terrorism — the neg’s impact is irresponsible fearmongering. No means, motive, or opportunity.

Mueller and Stewart 12 — John Mueller, Ph.D., Senior Research Scientist at the Mershon Center for International Security Studies and Adjunct Professor in the Department of Political Science at Ohio State University, and Senior Fellow at the Cato Institute, and Mark G. Stewart, Australian Research Council Professorial Fellow and Professor and Director at the Centre for Infrastructure Performance and Reliability at the University of Newcastle, 2012 (“The Terrorism Delusion: America’s Overwrought Response to September 11,” International Security, Vol. 37, No. 1, Summer, pp. 81-110, Available Online at <http://politicalscience.osu.edu/faculty/jmueller//absisfin.pdf>, Accessed 08-10-2015)

It seems increasingly likely that the official and popular reaction to the terrorist attacks of September 11, 2001, has been substantially deluded—massively disproportionate to the threat that al-Qaida has ever actually presented either as an international menace or as an inspiration or model to homegrown amateurs.

Applying the extensive datasets on terrorism that have been generated over the last decades, we conclude that the chances of an American perishing at the hands of a terrorist at present rates is one in 3.5 million per year—well within the range of what risk analysts hold to be “acceptable risk.”40 Yet, despite the importance of responsibly communicating risk and despite the costs of irresponsible fearmongering, just about the only official who has ever openly put the threat presented by terrorism in some sort of context is New York’s Mayor Michael Bloomberg, who in 2007 pointed out that people should “get a life” and that they have a greater chance of being hit by lightning than of being a victim of terrorism—an observation that may be a bit off the mark but is roughly accurate.41 (It might be noted that, despite this unorthodox outburst, Bloomberg still managed to be re-elected two years later.)

Indeed, much of the reaction to the September 11 attacks calls to mind Hans Christian Andersen’s fable of delusion, “The Emperor’s New Clothes,” in which con artists convince the emperor’s court that they can weave stuffs of the most beautiful colors and elaborate patterns from the delicate silk and purest gold thread they are given. These stuffs, they further convincingly explain, have the property of remaining invisible to anyone who is unusually stupid or unfit for office. The emperor finds this quite appealing because not only will he have splendid new clothes, but he will be able to discover which of his officials are unfit for their posts—or in today’s terms, have lost their effectiveness. His courtiers, then, have great professional incentive to proclaim the stuffs on the loom to be absolutely magnificent even while mentally justifying this conclusion with the equivalent of “absence of evidence is not evidence of absence.”

Unlike the emperor’s new clothes, terrorism does of course exist. Much of the reaction to the threat, however, has a distinctly delusionary quality. In Carle’s view, for example, the CIA has been “spinning in self-referential circles” in which “our premises were flawed, our facts used to fit our premises, our premises determined, and our fears justified our operational actions, in a self-contained process that arrived at a conclusion dramatically at odds with the facts.” The process “projected evil actions where there was, more often, muddled indirect and unavoidable complicity, or not much at all.” These “delusional ratiocinations,” he further observes, “were all sincerely, ardently held to have constituted a rigorous, rational process to identify terrorist threats” in which “the avalanche of reporting confirms its validity by its quantity,” in which there is a tendency to “reject incongruous or contradictory facts as erroneous, because they do not conform to accepted reality,” and in which potential dissenters are not-so-subtly reminded of career dangers: “Say what you want at meetings. It’s your decision. But you are doing yourself no favors.”42

Consider in this context the alarming and profoundly imaginary estimates of U.S. intelligence agencies in the year after the September 11 attacks that the number of trained al-Qaida operatives in the United States was between 2,000 and 5,000.43 Terrorist cells, they told reporters, were “embedded in most U.S. cities with sizable Islamic communities,” usually in the “run-down sections,” and were “up and active” because electronic intercepts had found some of them to be “talking to each other.”44 Another account relayed the view of “experts” that Osama bin Laden was ready to unleash an “11,000 strong terrorist army” operating in more than sixty countries “controlled by a Mr. Big who is based in Europe,” but that intelligence had “no idea where thousands of these men are.”45 Similarly, FBI Director Robert Mueller assured the Senate Intelligence Committee on February 11, 2003, that, although his agency had yet to identify even one al-Qaida cell in the United States, “I remain very concerned about what we are not seeing,” a sentence rendered in bold lettering in his prepared text. Moreover, he claimed that such unidentified entities presented “the greatest threat,” had “developed a support infrastructure” in the country, and had achieved both the “ability” and the “intent” to inflict “significant casualties in the US with little warning.”46

Over the course of time, such essentially delusionary thinking has been internalized and institutionalized in a great many ways. For example, an extrapolation of delusionary proportions is evident in the common observation that, because terrorists were able, mostly by thuggish means, to crash airplanes into buildings, they might therefore be able to construct a nuclear bomb. Brian Jenkins has run an internet search to discover how often variants of the term “al-Qaida” appeared within ten words of “nuclear.” There were only seven hits in 1999 and eleven in 2000, but the number soared to 1,742 in 2001 and to 2,931 in 2002.47 By 2008, Defense Secretary Robert Gates was assuring a congressional committee that what keeps every senior government leader awake at night is “the thought of a terrorist ending up with a weapon of mass destruction, especially nuclear.”48

Few of the sleepless, it seems, found much solace in the fact that an al-Qaida computer seized in Afghanistan in 2001 indicated that the group’s budget for research on weapons of mass destruction (almost all of it focused on primitive chemical weapons work) was $2,000 to $4,000.49 In the wake of the killing of Osama bin Laden, officials now have many more al-Qaida computers, and nothing in their content appears to suggest that the group had the time or inclination, let alone the money, to set up and staff a uranium-seizing operation, as well as a fancy, super-high-technology facility to fabricate a bomb. This is a process that requires trusting corrupted foreign collaborators and other criminals, obtaining and transporting highly guarded material, setting up a machine shop staffed with top scientists and technicians, and rolling the heavy, cumbersome, and untested finished product into position to be detonated by a skilled crew—all while attracting no attention from outsiders.50

If the miscreants in the American cases have been unable to create and set off even the simplest conventional bombs, it stands to reason that none of them were very close to creating, or having anything to do with, nuclear weapons—or for that matter biological, radiological, or chemical ones. In fact, with perhaps one exception, none seems to have even dreamed of the prospect; and the exception is José Padilla (case 2), who apparently mused at one point about creating a dirty bomb—a device that would disperse radiation—or even possibly an atomic one. His idea about isotope separation was to put uranium into a pail and then to make himself into a human centrifuge by swinging the pail around in great arcs.51

Even if a weapon were made abroad and then brought into the United States, its detonation would require individuals in-country with the capacity to receive and handle the complicated weapons and then to set them off. Thus far, the talent pool appears, to put mildly, very thin.

### Extend: “No Encryption Link”

#### Encryption doesn’t jeopardize counter-terrorism operations — their link is fearmongering.

Landau 15 — Susan Landau, Professor of Cybersecurity Policy in the Department of Social Science and Policy Studies at Worcester Polytechnic Institute, serves on the Computer Science Telecommunications Board of the National Research Council, former Senior Staff Privacy Analyst at Google, former Distinguished Engineer at Sun Microsystems, former faculty member at the University of Massachusetts at Amherst and at Wesleyan University, has held visiting positions at Harvard, Cornell, Yale, and the Mathematical Sciences Research Institute, holds a Ph.D. in Mathematics from the Massachusetts Institute of Technology, 2015 (“Director Comey and the Real Threats,” *Lawfare*, July 3rd, Available Online at <http://www.lawfareblog.com/director-comey-and-real-threats>, Accessed 07-06-2015)

Conflation obscures issues. That's what's happening now with FBI Director Comey's arguments regarding ISIS, Going Dark, and device encryption. On Wednesday, Ben, quoting the director, discussed how the changes resulting from ISIS means we ought to reexamine the whole encryption issue. "Our job is to find needles in a nationwide haystack, needles that are increasingly invisible to us because of end-to-end encryption," Comey said. "This is the 'going dark' problem in high definition."

Nope. Comey is looking at the right issue but in the wrong way. The possibility of ISIS attacks on US soil is very frightening. But as the New York Times reports, though the organization inspires lone wolf terrorists, it doesn't organize them to conduct their nefarious acts.

Encryption is not the difficulty in determining who the attackers might be and where their intentions lie. But encryption is important in combating our most serious national security concerns. I've quoted William Lynn here before, but the point he made is directly relevant, and it bears repeating. The Deputy Director of Defense wrote, "the threat to intellectual property is less dramatic than the threat to critical national infrastructure, [but] it may be the most significant cyberthreat that the United States will face over the long term."

The way you protect against such threats is communications and computer security everywhere. This translates to end-to-end encryption for communications, securing communications devices, etc. This is why, for example, NSA has supported technological efforts to secure devices, communications, and networks in the private sector.

Thoughts of an armed thug wielding a machete or shooting a semiautomatic rifle at a Fourth of July parade or picnic are terrifying. But one thing we expect out of government officials is rational thought and a sense of priorities. Tackling ISIS domestically is difficult, but there is no evidence that being able to listen to communications would have helped prevent the attacks on Charlie Hebdo, in Tunisia, or other ISIS-inspired efforts. Meanwhile there is plenty of evidence that securing our communications and devices would have prevented the breaches at Anthem, OPM, and elsewhere. The latter are serious long-term national security threats.

Securing the US means more than protecting against a knife-wielding fanatic; it includes securing the economy and developing the infrastructure that protects against long-term threats. We expect our leaders to prioritize, putting resources to the most important threats and making the choices that genuinely secure our nation. Director Comey's comments mixing ISIS with discussions about communications security and encryption do not rise to that level.

#### There’s *no evidence* that encryption empowers terrorists like ISIS.

Wheeler 15 — Marcy Wheeler, independent journalist writing about national security and civil liberties, has written for the *Guardian*, *Salon*, and the *Progressive*, author of Anatomy of Deceit about the CIA leak investigation, Recipient of the 2009 Hillman Award for blog journalism, holds a Ph.D. in Comparative Literature from the University of Michigan, 2015 (“Jim Comey May Not Be a Maniac, But He Has a Poor Understanding of Evidence,” *Empty Wheel*—Dr. Marcy Wheeler’s blog, July 6th, Available Online at https://www.emptywheel.net/2015/07/06/jim-comey-may-not-be-a-maniac-but-he-has-a-poor-understanding-of-evidence/, Accessed 07-20-2015)

Apparently, Jim Comey wasn’t happy with his stenographer, Ben Wittes. After having Ben write up Comey’s concerns on encryption last week, Comey has written his own explanation of his concerns about encryption at Ben’s blog.

Here are the 3 key paragraphs.

2. There are many benefits to this. Universal strong encryption will protect all of us—our innovation, our private thoughts, and so many other things of value—from thieves of all kinds. We will all have lock-boxes in our lives that only we can open and in which we can store all that is valuable to us. There are lots of good things about this.

3. There are many costs to this. Public safety in the United States has relied for a couple centuries on the ability of the government, with predication, to obtain permission from a court to access the “papers and effects” and communications of Americans. The Fourth Amendment reflects a trade-off inherent in ordered liberty: To protect the public, the government sometimes needs to be able to see an individual’s stuff, but only under appropriate circumstances and with appropriate oversight.

4. These two things are in tension in many contexts. When the government’s ability—with appropriate predication and court oversight—to see an individual’s stuff goes away, it will affect public safety. That tension is vividly illustrated by the current ISIL threat, which involves ISIL operators in Syria recruiting and tasking dozens of troubled Americans to kill people, a process that increasingly takes part through mobile messaging apps that are end-to-end encrypted, communications that may not be intercepted, despite judicial orders under the Fourth Amendment. But the tension could as well be illustrated in criminal investigations all over the country. There is simply no doubt that bad people can communicate with impunity in a world of universal strong encryption.

Comey admits encryption lets people lock stuff away from criminals (and supports innovation), and admits “there are lots of good things about this.” He then introduces “costs,” without enumerating them. In a paragraph purportedly explaining how the “good things” and “costs” are in tension, he raises the ISIL threat as well as — as an afterthought — “criminal investigations all over the country.”

Without providing any evidence about that tension.

As I have noted, the recent wiretap report raises real questions, at least about the “criminal investigations all over the country,” which in fact are not being thwarted. On that ledger, at least, there is no question: the “good things” (AKA, benefits) are huge, especially with the million or so iPhones that get stolen every year, and the “costs” are negligible, just a few wiretaps law enforcement can’t break.

I conceded we can’t make the same conclusions about FISA orders — or the FBI generally — because Comey’s agency’s record keeping is so bad (which is consistent with all the rest of its record-keeping). It may well be that we’re not able to access ISIL communications with US recruits because of encryption, but simply invoking the existence of ISIL using end-to-end encrypted mobile messaging apps is not evidence (especially because so much evidence indicates that sloppy end-user behavior makes it possible for FBI to crack this).

Especially after the FBI’s 0-for-40 record about making claims about terrorists since 9/11.

It may be that the FBI is facing increasing problems tracking ISIL. It may even be — though I’m skeptical — that those problems would outweigh the value of making stealing iPhones less useful.

But even as he calls for a real debate, Comey offers not one bit of real evidence to counter the crappy FBI reporting in the official reports to suggest this is not more FBI fearmongering.