Secret without Reason and Costly without Accomplishment:  
Questioning the NSA’s Metadata Program

John Mueller*  
Mark G. Stewart**

When Edward Snowden’s revelations emerged in June 2013 about the extent to which the National Security Agency was secretly gathering communications data as part of the country’s massive 9/11-induced effort to catch terrorists, the administration of Barack Obama set in motion a program to pursue him to the ends of the earth in order to have him prosecuted to the full extent of the law for illegally exposing state secrets.

However, the President has also said that the discussions about the programs these revelations have triggered have actually been a good thing: “I welcome this debate. And I think it’s healthy for our democracy. I think it’s a sign of maturity because probably five years ago, six years ago, we might not have been having this debate.”

There may be something a bit patronizing in the implication that the programs have been secret because we weren’t yet mature enough to debate them when they were put into place.

* Ralph D. Mershon Senior Research Scientist, Mershon Center for International Security Studies and Adjunct Professor, Department of Political Science, Ohio State University, and Senior Fellow, Cato Institute.

** ARC Australian Professorial Fellow, and Professor and Director, Centre for Infrastructure Performance and Reliability The University of Newcastle, New South Wales, Australia.

1 Office of the Press Secretary, The White House, Statement by the President, June 7, 2013, Fairmont Hotel, San Jose, California.
Setting that aside, however, a debate is surely to be welcomed—indeed, much overdue. It should be conducted not only about the National Security Agency’s amazingly extensive data-gathering programs to amass information on telephone and e-mail conversations—programs that have, according to the President, included “modest encroachments” on privacy—but also more generally about the phenomenal expansion of intelligence and policing efforts in the wake of 9/11.²

As Dana Priest and William Arkin have documented in their the remarkable book, *Top Secret America*, by 2009 there were something like 1,074 federal government organizations and almost 2,000 private companies devoted to counterterrorism, homeland security, and intelligence spread over more than 17,000 locations within the country. At least 263 of these were created or reorganized after 9/11.³ A simple listing of the government’s “Special Operations Programs” runs to 300 pages.⁴ Collectively this apparatus launched far more covert operations in the aftermath of 9/11 than it had during the entire Cold War.⁵

A comparison might be useful. Since 9/11, 53 cases have come to light of Islamist extremist terrorism, whether based in the United States or abroad, in which the United States itself has been, or apparently has been, targeted.⁶ The total number of real terrorists, would-be

² White House, *Statement by the President*, June 7, 2013.
⁵ Priest and Arkin, *Top Secret America*, 12.
⁶ See John Mueller (ed.), *Terrorism Since 9/11: The American Cases* (Columbus, OH: Mershon Center, Ohio State University, 2013).
terrorists, and putative terrorists populating this set of cases, excluding FBI and police undercover operatives, is less than 100. Thus, the United States has created or reorganized three entire counterterrorism organizations for every terrorist arrest or apprehension it has made of people plotting to do damage within the country.

Although much of discussion in this paper can be extrapolated more widely, it focuses primarily—and for starters—on one of the two surveillance programs revealed by Snowden. These two programs have often been mixed in, or confused, with each other.⁷

One of them, Prism, somewhat more commonly known from its section in the law as 702, permits NSA to gather electronic communication information on e-mail and phone conversations after approval by a judge if the target is both outside the United States and not an American citizen and if there is an appropriate and documented foreign intelligence purpose for the collection.

The other, known as 215, authorizes the gathering in bulk of business and communication records within the United States. It has been used in particular to amass telephone billing records—numbers called, numbers received, and conversation length—for every telephone in the

In principle, the 215 data are only supposed to be collected if there are “reasonable grounds to believe” the records are “relevant” to a terrorist investigation of a “known or unknown” terrorist organization or operative. Creatively expanding the word, relevant, to the breaking point, it has been taken in practice to mean that NSA can gather billing records for

---

every telephone conversation in the country. As many, including Senator Patrick Leahy, have pointed out, this broad approach could also be applied to banking, credit card, medical, financial, and library records, all of which could be held as reasonably to be somehow “relevant” to the decidedly wide-ranged quest to catch terrorists.

The information gathered by either program can be held for five years.

This paper primarily deals with the 215 program, the more controversial of the two, the one that involves the massive gathering of telephone billing records, or “metadata,” within the United States.

In the debate that has burgeoned since Snowden’s revelations, a number of questions have been raised about the civil liberties and privacy implications of NSA’s massive surveillance efforts. This paper focuses on three additional questions. None of these is terribly legalistic, but they are questions about the surveillance program that ought to be given more thorough examination.

The first two—why was the program secret and how much does it cost?—seem never to come up even though they are crucial if we are going to have an adult conversation on the issue. The third—what has the program accomplished?—has attracted some attention, but it clearly needs much more, and this paper examines it in the broader context of the obsessive, and massively expensive, efforts by police and intelligence since 9/11 to deal with the threat that is envisioned to be presented by terrorism, a quest that has involved following literally millions of leads that go nowhere.  

1. Why was the 215 program secret?

Under Executive Order 135256, classification is permitted if “disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism.” The order continues: “If there is significant doubt about the need to classify information, it shall not be classified.” There is also a classification level of top secret. As defined in Executive Order 12356, top secret is “applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security.”

It is difficult to see how earlier exposure of the program’s existence would have damaged national security, gravely or otherwise. No one seems to be saying that the Snowden documents put undercover intelligence operatives or operations overseas or elsewhere in danger of being exposed, or that they reveal military secrets about weapons, or that they compromise United States strategy or tactics. Instead, we get such vague, atmospheric pronouncements to the press as that from outgoing FBI Director Robert Mueller in August 2013: “Mueller said that leaks by former NSA contractor Edward Snowden ‘have impacted, and [are] in the process of impacting, capabilities around the world,’ but when asked to expand on this, he said simply, ‘No


10 Priest and Arkin, Top Secret America, 10n.

11 Actually, as will be discussed more fully in section 2, the program was essentially outed in an article in Wired in 2012 based on information supplied by a former NSA official. However, the program’s existence was firmly denied by people in charge. The later release of the Snowden materials settled the matter.
Even less helpful has been the expression of “belief” promulgated by NSA chief Keith B. Alexander: “Based on what we know to date, we believe these disclosures have caused significant and irreversible harm to the security of the nation.”

In fact, of course, terrorists have surely known at least since the 1990s (when Osama bin Laden ceased talking on a satellite phone) that United States intelligence is searching communications worldwide to track them down. Year after year we have heard about “chatter” that has been picked up by official agencies, and one certainly has to conclude that it has dawned on the chatterers that there are extensive efforts to listen in. The terrorists may not know the precise number, but they are likely to be at least dimly aware—and are unlikely to be surprised—that the NSA, in its tireless quest to conduct its very global war on terror intercepts and ingests 1.7 billion communication elements every day. These include, note Priest and Arkin, “telephone calls, radio signals, cell phone conversations, emails, text and Twitter messages, bulletin board postings, instant messages, website changes, computer network pings, and IP addresses.” It is possible, but unlikely, that the current revelations will impress the terrorists even further about the extent of the surveillance effort. But even if that is so, the effect would mainly be to make their efforts to communicate even more difficult and inconvenient.

Conceivably, as some maintain, there still exist some exceptionally dim-witted terrorists


15 Priest and Arkin, Top Secret America, 77.
or would-be terrorists who are oblivious to the fact that their communications are rather less than fully secure. But such supreme knuckle-heads are surely likely to make so many mistakes—like advertising on Facebook or searching there or in chatrooms for co-conspirators—that sophisticated and costly communications data banks are scarcely needed to track them down.\textsuperscript{16}

Some defenders of the program have creatively argued that exposure of the 215 program has aided terrorists because they now know that NSA is gathering only metadata on telephone calls in the United States, not their content.\textsuperscript{17} But, if terrorists or other bad people read past the first paragraph in discussions of the 215 program, they surely can also note that, if information gathered is deemed suspicious, investigators can apply for legal authority to record the content of the communications. And they can do that readily as well in the 702 program which gathers and monitors not only metadata, but also content. Moreover, like many others, terrorists are likely to suspect that, despite prominent denials to the contrary, considerably more than metadata is

\begin{flushright}
\textsuperscript{16} See, for example, cases 16, 30, 39, 40, 41, 48, 51, and 52 in Mueller, \textit{Terrorism Since 9/11}.

\textsuperscript{17} Thus General Michael Hayden on “Meet the Press,” NBC, June 16, 2013: “What I fear al-Qaeda learns about this program is not what we're \textit{allowed} to do but they learn what we're \textit{not} allowed to do, and they learn the limits of the program.” Asked on CBS’ “Face the Nation” on June 30, 2013, about what harm had been done, Hayden said, “Three things. Number one: Operational things have been disclosed. I mean you're a newsman, you know about protecting sources and methods and here now our sources and methods have been made public, so that's one. Second: Look, we cooperate with a lot of governments around the world. They expect us to be discreet about that cooperation. I can't imagine a government anywhere on the planet who now believes we can keep a secret.” He was never given an opportunity to divulge the third as his impatient interviewer rushed to move on. The second “harm” is a relevant concern for programs that are secret, but it is scarcely relevant to the issue of why the program was made secret in the first place.
\end{flushright}
gathered even under the 215 program.\textsuperscript{18}

It is also argued that the program was kept secret in order to protect the private communications companies, like AT&T, Verizon, and Sprint, that are dutifully supplying the NSA with data. If their customers find out that their billing records are being handed over to the government, it is said, they might drop their service and migrate to a company that doesn’t send its data to the NSA. However, the potential embarrassment of businesses is not usually deemed to constitute a threat, grave or otherwise, to national security. Moreover, the concern certainly appears to have been overwrought: the Snowden disclosures do not seem to have led to mass customer defections from cooperating companies. In part, perhaps, this is because it is difficult to find out which companies do not hand data over. Moreover, even if one could find out, the company to which the customer defects could at any time be forced to turn over its data anyway.

Unkind people might suggest that the real reason these programs were kept secret actually stems from the administration’s fear that public awareness of their “modest encroachments” on privacy would make further efforts to encroach more difficult.

Thus Reuters notes that a former Air Force secretary ominously warns that a “growing unease about domestic surveillance could have a chilling effect on proposed cyber legislation that calls for greater information-sharing between government and industry.” And it also notes that, \textsuperscript{18}

\textsuperscript{18} For example, when former NSA agent William Binney, was asked if he believed that the government was only collecting metadata, he responded, “Well, I don't believe that for a minute. OK? I mean, that's why they had to build Bluffdale, that facility in Utah with that massive amount of storage that could store all these recordings and all the data being passed along the fiberoptic networks of the world. I mean, you could store 100 years of the world's communications here. That's for content storage. That's not for metadata. Metadata, if you were doing it and putting it into the systems we built, you could do it in a 12- by-20-foot room for the world. That's all the space you need. You don't need 100,000 square feet of space that they have at Bluffdale to do that.” PBS NewsHour, August 1, 2013.
since the revelations, more lawmakers have signed on to legislation that would strengthen the privacy protections in the 1986 Electronic Communications Privacy Act.\textsuperscript{19} Perhaps, then, the programs were kept secret not so much to protect people from terrorism, but to protect the government from the annoying and inconvenient public and Congressional outcry that, as it happens, constitutes the untidy stuff of democracy.

The degree to which classification has been overdone is suggested more generally by the case of Bradley Manning who downloaded hundreds of thousands of classified documents that were subsequently made public by Wikileaks in 2010. As it turned out, these documents, while embarrassing to some officials, contained no really significant new disclosures—just about all the information was already essentially public, though in many cases it was less textured and nuanced.\textsuperscript{20} Although prosecutors forcefully argued in Manning’s military trial that he was guilty of “aiding the enemy”—surely the key issue in determining whether something should be classified—the judge failed to find him guilty on that charge.\textsuperscript{21} If Manning’s disclosures failed to “aid the enemy,” it would be difficult to argue that Snowden’s revelations, which are primarily about methods of data collection that were already known and/or easy to surmise, would be of much aid either.

2. How much does the 215 program cost?

\textsuperscript{19} Andrea Shalal-Esa and Joseph Menn, “U.S. domestic spying controversy complicates cybersecurity efforts,” Reuters, June 8, 2013.

\textsuperscript{20} Editor Bill Keller of the \textit{New York Times}, conversation with John Mueller, Berkeley, California, April 9, 2011.

If we are now to have a healthy debate about 215, NSA’s stupendous megadata program, it seems reasonable to suggest that debaters should be supplied with information about how much the program costs. This information would furnish a key starting point for any debate.

Presumably, that figure has thus far been classified because the program itself was classified. But now that we know only too well that the program exists, why should its cost remain secret?

It is certainly difficult to see how knowing that cost would help the terrorists—except perhaps to amaze them further. However, there is the danger, of course, that the cost of gathering and storing and evaluating huge amounts of metadata on the telephone conversations of all Americans might also amaze American taxpayers. Perhaps that’s another reason why the programs have been kept secret.

It’s possible as well that the cost figure for the program remains undisclosed in part because no one actually knows how much the program costs. This may seem a strange observation, but, as an example, the Department of Homeland Security has set up a vast array of “Fusion Centers” to police terrorism, but is unable to determine how much they cost. It estimates that somewhere between $289 million and $1.4 billion were awarded for the Centers between 2003 and 2010—an uncertainty gap of over a billion dollars that is impressive even by Washington standards.22

That this phenomenon is widespread is suggested by Priest and Arkin. In researching their

22 Majority and Minority Staff Report, Federal Support for and Involvement in State and Local Fusion Centers, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate, October 3, 2012, 3. See also John Mueller, “Confusion: What if we can't catch terrorists in America because there aren't any?” foreignpolicy.com, October 8, 2012.
book, they discovered that the spending increases on counterterrorism in the aftermath of 9/11 often took place so fast and so chaotically that no one was able to keep a count of the costs. As they put it strikingly,

American taxpayers have shelled out hundreds of billions of dollars to turn the machine of government over to defeating terrorism without ever really questioning what they were getting for their money. And even if they did want an answer to that question, they would not be given one, both because those same officials have decided it would gravely harm national security to share such classified information—and because the officials themselves don’t actually know.23

**Program, investigatory, and opportunity costs**

The direct costs of maintaining the 215 program might be quite low. However, a full accounting should include not only the actual cost of gathering and storing the surveillance data, but also the costs of constantly sorting through it to generate and develop leads. According to the NSA’s director of compliance, the agency queries its databases about 20 million times each month.24 Presumably that includes both databases and, equally presumably, it involves a great deal of human interaction, all of which must be paid for.

Costs should also include those involved in following up the leads once they have been generated, an issue to be discussed in the next section.

Also included in the tally should be the opportunity costs: what else could the money have been used for? For example, it has often been noted that there has been a downgrading by the FBI and other agencies of other priorities, including the pursuit of white collar crime like fraudulent banking practices, to focus on the pursuit of (substantially non-existent) terrorists: as


an assistant U.S. attorney put it in 2002, “This is a great time to be a white-collar criminal.”

To fully evaluate the costs of the NSA surveillance efforts, one would need to take this issue into account.

**Privacy costs: the issue of trust**

In addition, some consideration should be made for the less quantifiable costs of privacy invasion and for the potential misuse of the data.

Although the program has built-in safeguards, its operation ultimately requires us to trust those in charge. Citing unpleasant historical precedents from the days of Richard Nixon and J. Edgar Hoover and from the runup to the Iraq War of 2003, Stephen Walt has arrestingly suggested, or warned, that the program could be used to intimidate or harass whistle-blowers, dissidents, and overly-inquisitive journalists: “once someone raises their head above the parapet and calls attention to themselves by challenging government policy, they can’t be sure that someone inside government won’t take umbrage and try to see what dirt they can find.”

The current administration’s credibility on the issue of whether it can be trusted not to abuse this system has already has been strained to the point that, in a Rasmussen poll in June 2013, 57 percent of the respondents deemed it likely that the government would use data dredged up by the NSA to harass political opponents.

---


27 “57% Fear Government Will Use NSA Data to Harass Political Opponents,” Rasmussen Reports, June 13, 2013. See also Eugene Robinson, “We can handle the truth on
That wary reaction has been enhanced by the fact that officials have several times been caught in lies—or supreme exercises in Clintonian sophistry—about the NSA programs.

There is, for example, the response of NSA director Alexander to a March 2012 cover story in *Wired* magazine that reported the views of William Binney, a former NSA official.

Binney left the agency in late 2001 when it launched its warrantless-wiretapping program, but, according to the article, he retained close contact with other agency employees for several years thereafter. “They violated the Constitution setting it up,” he says, “But they didn’t care. They were going to do it anyway, and they were going to crucify anyone who stood in the way. When they started violating the Constitution, I couldn’t stay.” Binney contended that, without a warrant, the NSA was collecting “a vast trove of international and domestic billing records” from major American telephone companies and that “they’re storing everything they gather.”

In the ensuing months, Alexander blithely denied Binney’s contention. “To think we’re collecting on every US person…that would be against the law…. The fact is we’re a foreign intelligence agency.” He also categorically insisted that “we don’t hold data on U.S. citizens,” a statement that has been defended by the administration on the grounds that the NSA’s internal definition of “data” does not include “metadata”—a language-stretching nuance Alexander neglected to mention when he made his statement. As it happens, however, the agency’s actual

---


internal definition of “data” does specifically include “call event records and other Digital Network Intelligence metadata.”

In like manner, Alexander probably had a special private definition of “dossier” in mind when he vehemently stated in 2012 that the notion that the NSA has “millions or hundreds of millions of dossiers on people is absolutely false.”

Then, in March 2013, Director of National Intelligence James Clapper was asked in a Senate Intelligence Committee hearing, “Does the NSA collect any type of data at all on millions or hundred of millions of Americans?” He replied, “No, sir…. Not wittingly.” The Senator asking the question says it had been sent to Clapper’s office the day before and that Clapper was given a chance to amend his answer. After Snowden’s revelations three months later spectacularly shattered Clapper’s crisp denial (as well as Alexander’s earlier ones), Clapper sent a letter to the Committee stating that his answer had been “clearly erroneous” and that when responding he imagined that the question referred to content, not metadata which he somehow believes the NSA does not collect “wittingly.” Clapper has also said that an honest response would have required him to divulge secrets that were highly classified, and thus he came up with the “least untruthful” answer he could imagine at the time.

There is additional evidence of deception in the disclosure that the NSA illegally collected email content data on thousands, or tens of thousands, of Americans before that


32 Robinson, “We can handle the truth on NSA spying.” See also Bamford, “They Know Much More Than You Think.”
practice was closed down by the courts in 2011. The court’s opinion on this was classified, and the Obama administration fought a Freedom of Information lawsuit seeking to get it released. In the wake of the Snowden disclosures, however, the opinion was finally declassified and released in heavily redacted form. In it, the judge specifically points out that he had previously been the victim of “a substantial misrepresentation regarding the scope of a major collection program” and that the information gathered had been “fundamentally different from what the court had been led to believe.”

Similar concerns were raised in a 2009 ruling that had originally been classified as top secret—that is, deemed to be information “the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security.” The ruling concerned the way the NSA probed phone numbers on an “alert list.” When it was finally declassified under pressure in 2013, the ruling included declarations that the government had failed to comply with the court’s orders and had compounded this by “repeatedly submitting inaccurate descriptions of the alert process” and that court-approved privacy safeguards had “been so frequently and systematically violated” that they “never functioned effectively.” A senior official explained rather lamely, but entirely plausibly, that any violations were “unintentional” because “there was nobody at N.S.A. who really had a full understanding of how the program was operating at the


34 Gellman, “NSA broke privacy rules.”

35 Ellen Nakashima, “NSA gathered thousands of Americans’ e-mails.”
time.”

It might be wondered, then, what intentional violations, keeping Walt’s admonition in mind, could lead to. Senator Dianne Feinstein, who chairs the Senate Intelligence Committee, insists that her committee “has never identified an instance in which the NSA has intentionally abused its authority to conduct surveillance for inappropriate purposes.” However, the agency’s director of compliance, has indicated that there have been a very small number (perhaps one every five years) of “willful errors.”

Relevant as well to a discussion of credibility is the disclosure that in 2006 the NSA deliberately weakened an encryption standard accepted both nationally and internationally in a systematic effort to defeat privacy protections for Internet communications, a venture that compromised the National Institute of Standards and Technology in the process.

In all this, an assessment of the privacy costs attendant on the NSA’s surveillance efforts should hold in mind, to the degree to which they apply, warnings suggested in this passage from George Orwell’s novel, 1984:

> There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.


37 Savage, “N.S.A. Calls Violations of Privacy, ‘Miniscule’”

38 Shane, “Court Upbraided N.S.A. on Its Use of Call-Log Data.”

39 Quoted, Bamford, “They Know Much More Than You Think.”
3. What has the 215 program accomplished?

Once one knows the cost of the program, one is in a position to weigh that figure against the benefit the program has generated. The President insists that the privacy-encroaching programs “help us prevent terrorist attacks” and therefore “on net, it was worth us doing.”

However, they are worth us doing only if their benefit, on net, outweighs their cost. And that is a calculation that should be made, not simply declared.

The 9/11 atmosphere: consequences and persistence

To begin an appraisal of this issue, one must assess the program in context. It has been only one cog in the massive intelligence-gathering machine impelled by the trauma of 9/11. The trauma is certainly understandable. But the fears, and therefore the hasty and expensive actions they inspired, have clearly been substantially inflated. As anthropologist Scott Atran puts it, “Perhaps never in the history of human conflict have so few people with so few actual means and capabilities frightened so many.”

In the immediate aftermath of the September 11 attacks, recalls Rudy Giuliani, who was mayor of New York at the time, “anybody, any one of these security experts, including myself, would have told you on September 11, 2001, we’re looking at dozens and dozens and multiyears...

________________________

40 White House, Statement by the President, June 7, 2013.


17
of attacks like this.” Or, as journalist Jane Mayer observes, “the only certainty shared by virtually the entire American intelligence community” in the months after September 11 “was that a second wave of even more devastating terrorist attacks on America was imminent.”

The fears and concerns were, of course, plausible extrapolations from the facts then at hand. However, that every “security expert” should hold such erroneous views and that the intelligence community should be certain about them is fundamentally absurd. It was also an entirely plausible extrapolation from facts then at hand that 9/11 could prove to be an aberration rather than a harbinger. Yet it appears that no one in authority could even imagine that proposition to be true even though it could have been taken to fit the available information fully as well as the passionately-embraced alarmist perspective.


46 In his book, George F. Kennan, John Lewis Gaddis, observes that no one at the summit of foreign policy in 1950 anticipated most of the major international developments that were to take place in the next half-century. Among these: “that there would be no World War” and that the United States and the USSR, “soon to have tens of thousands of thermonuclear weapons pointed at one another, would agree tacitly never to use any of them” (New York: Penguin, 2012, 403). However, the absence of further world war, whether nuclear or not, was compatible with the fairly obvious observation that those running world affairs after World War II were the same people or the intellectual heirs of the people who had tried desperately to prevent that cataclysm. It was entirely plausible that such people, despite their huge differences on many issues, would manage to be capable of keeping themselves from plunging into a self-destructive repeat performance. Although this perspective was not, of course, the only possible one, there was no definitive way to dismiss it, and it should accordingly have remained on the table. For the suggestion that, if no one anticipated this distinct possibility in 1950, the US might
At any rate, operating under that apparently unanimous mentality, US intelligence extravagantly imagined that the number of trained al-Qaeda operatives in the United States was between 2,000 and 5,000.\textsuperscript{47} 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.”\textsuperscript{48}

Over the years, such thinking has been internalized and institutionalized in a great many ways, and it has proved to be notably resistant to counter-information. Indeed, officials often seem to live in what might be called “I think, therefore they are” denial.\textsuperscript{49} Thus, on February 11, 2003, a year and a half after 9/11, FBI Director Robert Mueller assured the Senate Intelligence Committee that “the greatest threat is from al-Qaeda cells in the US that we have not yet identified.” He somehow judged the threat from those unidentified entities to be “increasing” and claimed to know that “al-Qaeda maintains the ability and the intent to inflict significant casualties in the US with little warning.” On February 16, 2005, he testified before the same

---


\textsuperscript{48} Sale, “US al Qaida Cells Attacked.” 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.” Andy Lines, “War on Terror: Bin Laden Army: 11,000 Terror Agents Set to Strike,” \textit{Mirror} (London), September 24, 2001.

\textsuperscript{49} On this issue, see also Mueller and Stewart, “The Terrorism Delusion.”
committee that he remained “very concerned about what we are not seeing,” a sentence rendered in bold lettering in his prepared text.\(^{50}\) By that time, however, an FBI report had concluded that, despite years of well-funded sleuthing, it had yet to uncover a single true al-Qaida sleeper cell in the United States. For some, or no, reason, this report was kept secret although it managed to be leaked.\(^{51}\) However, some in the FBI remained unmoved, telling Fox News at the time that “just because there’s no concrete evidence of sleeper cells now, doesn’t mean they don’t exist.”\(^{52}\)

Since the number of al-Qaeda operatives actually in the country came out to be zero or nearly so, and since the threat of terrorism in the country proved to be far more limited than initially feared—not even one of the “dozens and dozens” of attacks like 9/11 ever materialized of course—there might logically have been some judicious cutbacks to the funds devoted to dealing with the issue in subsequent years. However, despite the fact that initial perspectives have proven to have been much overblown, the FBI will continue to engage, perhaps forever, in the exhaustive, and exhausting, pursuit of terrorists in what some in the bureau call “ghost chasing.”\(^{53}\) Thus, Director Mueller: “I’ll fight tooth and nail for more criminal agents, but I’ll never at the end of the day take an agent out of counterterrorism and national security.”\(^{54}\)

---

\(^{50}\) Director Mueller’s testimony can be found at [http://www.fbi.gov/congress/congress.htm](http://www.fbi.gov/congress/congress.htm).


\(^{52}\) “FBI Can’t Find Sleeper Cells,” Fox News, March 10, 2005.


\(^{54}\) Graff, *Threat Matrix*, 524.
Far overdue, clearly, are extensive and transparently-presented studies seeking rationally to evaluate the massive increases in homeland security expenditures that have taken place since 9/11—increases that total well over $1 trillion. But virtually none of this has been done by the administrators in charge.\textsuperscript{55}

Instead, initial, if clearly alarmist, perspectives have been essentially maintained and the vast and hasty increases in spending on homeland security continue to be perpetuated. Important in this have been increases in intelligence and policing as the questing enterprise continues to be expanded, searching for the needle by adding more and more hay.

The NSA has been central to this expansion of course, but it is only part of the process.

For example, there are those Fusion Centers—clusters of state and local law enforcement people set up to collect intelligence on terrorist and other criminal activity in their area and then to send reports on their findings to DHS for evaluation. In 2012, DHS Secretary Janet Napolitano called them “one of the centerpieces of our counterterrorism strategy.”\textsuperscript{56}

Considerable hackles were raised by a 2012 report from the Permanent Subcommittee on Investigations of the Senate Committee on Homeland Security and Governmental Affairs that concluded the utility of the terrorism-related reporting from the Fusion Centers had been at best “questionable.” Investigators shuffled through 610 Fusion Center intelligence reports submitted to DHS over a 13 month period. Of the 574 unclassified reports filed, 188 were “cancelled” by DHS reviewers generally because they contained “nothing of value” or simply failed to be devoid

\textsuperscript{55} For a discussion, see Mueller and Stewart, \textit{Terror, Security, and Money}, 1-9.

of “any actual intelligence.” While the overall cancellation rate for the reports was around 30 percent, nearly half of those dealing with terrorism were rejected out of hand. That didn’t leave many. Of the 386 reports accepted, only 94—considerably less than two a week—related “in some way” to potential terrorist activity. Moreover, more than a quarter of these simply duplicated information already known to the FBI, and “some were based on information drawn from publicly available websites or dated public reports.” One, in fact, simply relayed information from a Department of Justice press release that had been published months earlier.57

Moreover, continues the report, DHS has “struggled” to identify a clear example in which a Fusion Center provided intelligence that helped disrupt a terrorist plot. And, when investigators looked at the four “success stories” touted by DHS, they were “unable to confirm” that the Fusion Centers’ contributions were “as significant as DHS portrayed them; were unique to the intelligence and analytical work expected of fusion centers; or would not have occurred absent a fusion center.”58

However, it apparently never occurred to the investigators that the reason intelligence reporting on terrorists is so limited in quantity and so abysmal in overall quality is that there was virtually nothing to report. Absence of evidence, it implies, cannot possibly be evidence of absence. Accordingly, the report recommends that even more money should be spent on them.

Local intelligence reporting efforts, it suggests, should be reformed to eliminate

57 Majority and Minority Staff Report, Federal Support for and Involvement in State and Local Fusion Centers. On hackles, see Smith, “Senate Report.”

58 Majority and Minority Staff Report, Federal Support for and Involvement in State and Local Fusion Centers, 83.
duplication, the training and numbers of intelligence reporters should be improved, and better efforts to evaluate their output should be put into place.\textsuperscript{59}

Another instance of substantially unproductive hay-heaping is the establishment by the New York Police Department of a trademarked and extensively promoted “If You See Something, Say Something\textsuperscript{TM}” terrorism hotline. It has received tens of thousands of tips, but not one of these, it appears, has led to a terrorism arrest.\textsuperscript{60}

For its part, the FBI celebrated (or acknowledged) the receipt of its 2 millionth terrorism tip from the public in August 2008.\textsuperscript{61} There is no record whether these have been more productive than the tips supplied to the NYPD. However, they have all been dutifully scrutinized in the post-9/11 atmosphere under the admonition of Director Robert Mueller that “No counterterrorism lead goes uncovered.”\textsuperscript{62} Or, as the assistant chief for the FBI’s National Threat Center puts it extravagantly, it’s the lead “you don’t take seriously that becomes the 9/11.”\textsuperscript{63}

The bureau has folded this information into a “Threat Matrix,” an itemized catalogue of all the “threats”—or more accurately “leads”—needing to be followed up. As Garrett Graff

\begin{flushright}
\footnotesize
\textsuperscript{59} Majority and Minority Staff Report, \textit{Federal Support for and Involvement in State and Local Fusion Centers}, 106. On this issue, see also Mueller, “Confusion.”


\textsuperscript{61} Donna Leinwand, “Psst—Leads from Public to FBI Rise,” \textit{USA Today}, August 15, 2008.

\textsuperscript{62} Graff, \textit{Threat Matrix}, 579.

\textsuperscript{63} Leinwand, “Psst—Leads from Public to FBI Rise.”
\end{flushright}
explains, the government pursues “upwards of 5,000 threats per day.” The Threat Matrix, or selected excerpts from it, form the centerpiece of the two hours of briefings on terrorism the FBI director undergoes each day. Impelled by what some have called “The 9/11 Commission Syndrome”—an obsession with the career dangers in failing “to connect the dots”—it is in no one’s interest to cull the threats “because it was possible you’d cull the wrong threat and end up, after the next attack, at the green felt witness table before the next congressional inquiry.” Consequently, the Threat Matrix “tracks all the unfolding terrorist plots and intelligence rumors” and is “filled to the brim with whispers, rumors, and vacuous, unconfirmed information.” In result, “claims that ordinarily wouldn’t have made it past the intake agent, claims that wouldn’t even be written down weeks earlier, suddenly became the subject of briefs to the President in the Oval Office.”

Graff supplies an example. One entry in the Threat Matrix is crisply cited as “a threat from the Philippines to attack the United States unless blackmail money was paid.” It turns out that this entry was based on an e-mail that said, “Dear America. I will attack you if you don’t pay me 999999999999999999999999999999999999999999 dollars. MUHAHAHA.”

64 Graff, Threat Matrix, 399.  
65 Graff, Threat Matrix, 339.  
66 Graff, Threat Matrix, 400.  
67 Graff, Threat Matrix, 345. Also: “Every time the CIA picked up a squib of information, it tossed it into the Threat Matrix” (405).  
68 Graff, Threat Matrix, 344.  
69 Graff, Threat Matrix, 398. Graff says that the FBI dutifully ran down the e-mail’s author and sent information to Philippine police who then paid a visit to the would-be
If, aided by the Threat Matrix, the government pursues some 5000 “threats” or leads each day, and if each lead takes an average of a half a week to investigate, the FBI has pursued some ten million of them over the years since 9/11—a process that has led to, at the very most, a few hundred prosecutions, most of them on quite minor charges.\(^{70}\)

**The NSA: efforts and accomplishments**

In the panicky aftermath of 9/11, the National Security Agency, the institution of central concern here, has also expanded massively, and its computerized surveillance programs have been a central part of that process. As of 2011, the floor space it occupied matched that of the Pentagon, and its buildings are surrounded by 112 acres of parking space. There are plans to add 10,000 workers by 2026, and the price tag for just the first phase of this expansion is $2 billion.\(^{71}\)

It is important to evaluate what these programs have accomplished—to determine whether “on net” they have been “worth us doing” in their central mission of countering extortionist’s parents.

\(^{70}\) Karen J. Greenberg (ed.), *Terrorism Trial Report Card: September 11, 2001-September 11, 2009*, New York University School of Law, Center on Law and Security, 2010. Moreover, whatever the ratio of needle to hay, living with the Threat Matrix seems to take a psychological toll on its daily readers. As Graff vividly describes the process, the Threat Matrix comes off as “a catalogue of horrors” (19), as the “daily looming prognoses of Armageddon” (489), and as “a seeming tidal wave of Islamic extremist anger that threatened to unhinge American society” (345). It could become “all-consuming and paralyzing” (345), and he quotes former CIA Director George Tenet: “You could drive yourself crazy believing all or even half of what was in it” (344). Or as another reader puts it, “Your mind comes to be dominated by the horrific consequences of low-probability events” (400). Obsessed by the implied imminence and certainty of doom, one overworked reader, Special Agent Brad Doucette, was led to commit suicide in 2003 (411). “Present fears,” observes Macbeth, “are less than horrible imaginings.”

\(^{71}\) Priest and Arkin, *Top Secret America*, 74.
terrorism.

When asked in June 2013 at Senate hearings if NSA’s massive data-gathering programs were “crucial or critical” in disrupting terrorist threats, the agency’s head, General Alexander, doggedly testified that in “dozens” of instances the databases “helped” or were “contributing”—though he did seem to agree with the word “critical” at one point.72 The key issue for evaluating the programs, however, given their costs and privacy implications, would be to determine not whether the huge databases were helpful or contributing, but whether they were necessary.73

After his testimony, Alexander provided Congress a list of terrorism cases in which his surveillance measures have help to disrupt terrorist plots or to identify suspects. The list reportedly numbers 54—unsurprisingly, the list itself is classified. On the surface, this seems to be an amazingly small number for several years’ work. There have been hundreds of terrorism cases in the United States since 9/11. Some 53 of these, as noted earlier, have led to full-bore prosecutions for plotting to attack targets in the United States.74 And there are dozens more that have led to prosecutions for sending, or plotting to send, support to terrorists overseas, while a few hundred have involved terrorism investigations that led to prosecutions on lesser charges.75


73 NSA operatives sometimes suggest the program “ultimately completes the picture” or, in the words of FBI Deputy Director Sean Joyce, “closes the gap” on information on a case. These formulations ingeniously, if deceptively, create the impression that the information was necessary. Ellen Nakashima, “NSA cites case as success of phone data-collection program,” Washington Post, August 8, 2013.

74 See Mueller, Terrorism Since 9/11.

75 The bulk of people convicted in “terrorism-associated” prosecutions, are sentenced to less than four years, and most of these less than one year. Federal inmates generally serve 85 percent of their sentences. Greenberg, Terrorism Trial Report Card, 13-14; see also 59.
There have also been hundreds—or perhaps even thousands—of terrorism cases overseas. If the NSA programs were so valuable, one would think that investigators on just about every case would routinely run their information by the NSA. Even if the NSA comes up blank, that would be helpful to know because it would close off some avenues of potential investigation that, if pursued, would have proven to be a waste of time and effort, allowing investigators to follow leads more likely to be productive.

That they apparently have not done so suggests either that investigators and prosecutors have only occasionally found the NSA to be a helpful ally or else that they were afraid that if they queried the NSA on the case at hand, the agency would spew out a raft of leads that would unproductively clutter and distract their investigation while greatly increasing its costs.

The experience at the FBI with NSA leads is likely relevant here. Explains Walter Pincus, if operatives at NSA, sorting through their 215 metadata collection or other sources, uncover “a questionable pattern” such as “calls to other suspect phones,” they send a report to the FBI for investigation.\textsuperscript{76} The FBI, then, is routinely supplied with what Graff calls “endless lists of ‘suspect’ telephone numbers.” When followed up, these “leads” virtually never go anywhere: of 5000 numbers passed along, only 10—two-tenths of one percent—“panned out enough for the bureau to bother” to get court permission to follow them up. At the FBI, the NSA tips are often called “Pizza Hut” leads because, following them up, FBI agents “inevitably end up investigating the local pizza delivery guy.” At one point, the generally diplomatic Robert Mueller bluntly told NSA director Alexander, “You act like this is some treasure trove; it’s a useless time suck.” An agent in the trenches puts it a bit less delicately: “You know how long it takes to chase 99 pieces

\textsuperscript{76} Pincus, “NSA should be debated on the facts.”
This resonates with the experience of the CIA. Using its wealth of data, the NSA under Alexander has been fond of presenting massive, even supreme, exercises in dot-connecting in which hundreds or even thousands of people, places, and events are linked together in what some call BAGs, or “big ass graphs.” For all their (presumed) awesomeness, these have reportedly produced very few useful leads. “I don’t need this,” said an exacerbated senior CIA official.

Because the BAGs include people who are three layers removed from the putative terrorist of interest, the number of people in any one full picture could number in the tens of millions. Even before coming to the NSA, Alexander had applied such massive data networks in the Army. Detractors say there was an absence of data and verifiable sources behind the leads, that a quarter of the people on the charts were already dead, and that about the only thing the people in the networks were connected to was, as it happens, “pizza shops.”

The cases

According to the testimony of an NSA official, of the 54 cases that were supposedly disrupted by NSA surveillance data, more than 90 percent involved 702 information. Thus, 215 data presumably played a role in around 5 cases over the course of the program. According to General Alexander, only 13 of the 54 cases on the classified list had a “homeland nexus,” the

77 Graff, Threat Matrix, 527.
78 Harris, “Cowboy of the NSA.”
79 Harris, “Cowboy of the NSA.”
80 Pincus, “NSA should be debated on the facts.”
others having occurred in Europe (25), in Asia (11), and in Africa (5).\textsuperscript{81}

Four of the cases, all presumably from the “homeland nexus” subset, were publically discussed on June 18, 2013, by Alexander and by Sean Joyce, Deputy Director of the FBI at the rather tendentiously titled “Hearing of the House Permanent Select Committee on Intelligence on How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries.” Insofar as NSA surveillance played a role at all in these cases, it seems that it was the 702 program, not the 215 one, that was relevant.\textsuperscript{82}

First, they suggested that the NSA programs helped apprehend an American who had done surveillance work (the value of which seems to have been fairly limited) for terrorist gunmen who killed 166 in a suicidal rampage in Mumbai, India, in 2008. He was later arrested as he was engaged in a plot to do terrorist damage in Denmark, a plot that was beset by many planning and financial difficulties at the time. According to \textit{ProRepublica} reporter Sebastian Rotella who has done extensive research and reporting on the case, British intelligence already had the American under surveillance—suggesting that the Danish enterprise would never have been allowed to be carried out. The arrest resulted from a tip from the British, not from NSA intercepts. It does appear, however, that previously stored NSA intercepts, presumably from the 702 program, aided in building the legal case against the man.\textsuperscript{83}

\textsuperscript{81} Peter Finn, “NSA chief says surveillance programs helped thwart dozens of plots,” \textit{Washington Post}, June 27, 2013.

\textsuperscript{82} Carlo Muñoz, “NSA chief cites 50 foiled plots in defense of spying program,” \textit{The Hill}, June 18, 2013.

\textsuperscript{83} 83 Sebastian Rotella, “Did NSA Surveillance Help Thwart Plotter of Mumbai Attack?” www.pbs.org/wgbh/pages/frontline, June 12, 2013. See also Nick Gillespie, “Do the Zazi and Headley Arrests Prove the Power of NSA Total Surveillance?” reason.com, June 13,
The second case involves a San Diego cab driver from Somalia who has been convicted of sending the decidedly non-princely sum of $8,500 to help a designated terrorist group in Somalia fight Ethiopians who, with US support, had recently invaded the country. The government had been tapping his telephone for months, and Director Mueller appears to have singled out this case as the only one in which the collection of phone data had been “instrumental,” a word, of course, that is not as strong as “crucial” or “critical” or “necessary.”

Joyce says that an investigation of the potential case with 215 information that began in October 2007 “did not find any connection to terrorist activity,” but that there was a breakthrough when NSA connected a San Diego number with a suspicious contact outside the country using 215. However, it is not clear they needed any sort of data bank to sort through. Says Senator Ron Wyden, investigators had all the information they needed to get a court order to investigate.

A correspondent for The Hill breathlessly characterizes the cab driver culprit as “a top terrorist financier in San Diego, who was supporting militant extremist groups in Somalia.”

However, it certainly appears that the crime prosecuted at great effort and cost was, overall, a

2013. Joyce testified that the terrorist operative was uncovered “through 702 coverage of an al-Qaeda-affiliated terrorist.” Hearing of the House Permanent Select Committee on Intelligence on How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries, Washington, DC: IC on the Record, Office of the Director of National Intelligence, June 18, 2013.


85 Hearing of the House Permanent Select Committee on Intelligence.

86 Nakashima, “NSA cites case.”

87 Muñoz, “NSA chief cites 50 foiled plots.”
rather trivial one.

The third case seems to be even more trivial. It involves three Muslim men, all naturalized American citizens, one in Kansas City and two in New York. At the time of the American invasion of Iraq in 2003, they decided they needed to fight for their “faith and community,” in the words of one of them. Four years later, one of the men was able to connect to two apparently experienced al-Qaeda terrorists in Yemen. Hoping to join the fight in Iraq, Afghanistan, or Somalia, the American men sent money and equipment to their new friends in Yemen under the impression that these would be set aside for their military training. Over several months they sent thousands of dollars—one of them says it totaled more than $23,000—as well as watches, cold-weather gear, some Garmin GPS units, and a remote-controlled toy car. However, the recipients divided the physical loot among themselves and spent the money on (real) cars and as awards to families of Islamic martyrs. In 2008, the scam artists requested further payments of $45,000 which one of them planned to use to open an appliance store. They also suggested that the Americans were better suited to an operation in the United States and cajoled one of them into casing the New York Stock Exchange for a possible bombing—a “plot” that they never had any intention of carrying out, according to the testimony of one of them. The American did do a walk around the target, and then, several months later, submitted a one-page report on his adventure consisting of information that could have been gotten from Google maps and from tourist brochures. It was summarily trashed in disgust by his handlers. 88

In his June 2013 testimony, Joyce said identification in the case was made not through

At the same time, he raised interest, and then eyebrows, by dramatically proclaiming this to be a case “that was in the very initial stages of plotting to bomb the New York Stock Exchange.” Another official said, “It was, as Deputy Director Joyce states, in its nascent stages and could have progressed well beyond that if it wasn’t for our ability to obtain FISA material.” However, when asked whether the plot was “serious,” Joyce deftly dodged the issue: “I think the jury considered it serious because they were all convicted.” As it happens, there were no jury trials: the three men all pleaded guilty and then only to providing support to terrorism, not to the NYSE plot (such as it was). According to the other official, FBI Deputy Director Joyce “misspoke.”\(^90\) Alexander nonetheless appears to have been delighted with Joyce’s performance at the hearings. An open microphone reportedly captured him asking Joyce to tell his boss, FBI director Robert Mueller, “I own him another friggin’ beer.”\(^91\)

Only the fourth case involves a serious potential for terrorism within the United States. This was the Zazi case of 2009 in which three Afghan-Americans received training in Pakistan before returning to the United States, plotting to set off bombs on the New York subway system.

Joyce testified that a connection was made through “702 authority.”\(^92\) But, as Justin

\(^{89}\) *Hearing of the House Permanent Select Committee on Intelligence.* Ken McCarthy, “NSA chief says exposure of surveillance programs has ‘irreversible’ impact,” theguardian.com, June 18, 2013.


\(^{91}\) Harris, “FBI Concocted Bomb Plot.”

\(^{92}\) *Hearing of the House Permanent Select Committee on Intelligence.*
Heilmann points out in a study of the episode and as others have more recently noted, the plot in the United States does not appear to have been disrupted so much by NSA data-dredgers, but rather by standard surveillance procedures implemented after the British provided a hot tip about Zazi based on his e-mail traffic to a known overseas terrorist address that had long been under surveillance. At that point, US authorities had good reason to put the plotters on their radar and, as Senator Ron Wyden has pointed out, “the government had all the information it needed to go to the phone company and get an individual court order.” Having NSA’s megadata collection might have been helpful, but it seems scarcely to have been required.

Actually, it is not clear that even the tip was necessary. Given the perpetrators’ limited capacities, it is questionable whether the plot would have ever succeeded. For example, the plotters foolishly called attention to themselves by used stolen credit cards to purchase large quantities of potential bomb material thereby guaranteeing that the sales would be scrutinized and security camera information preserved. Moreover, even with his training and a set of notes at hand, Zazi, described by a step-uncle as “a dumb kid, believe me,” still apparently couldn’t figure it out, and he frantically contacted his overseas trainer for help several times. Each of these

93 Justin Heilman, “Case 28: Zazi,” in Mueller, Terrorism Since 9/11, 347-55. More recent: Ben Smith, “Public Documents Contradict Claim Email Spying Foiled Terror Plot,” buzzfeed.com, June 7, 2013; British tip: “British Spies help prevent attack,” Telegraph, November 9, 2009. It is conceivable that the 702 program, Prism, played a role in this process, but is not at all clear that this is so or that, if so, its role was necessary. For a discussion, see Dan Amira, “Did Controversial NSA Spy Programs Really Help Prevent an Attack on the Subway?” nymag.com, June 10, 2013. Alexander has said that 702 was “critical,” but that 215 was not essential to the case: McCarthy, “NSA chief says exposure.” See also Molotch, Against Security, 56, 58; Matt Apuzzo and Adam Goldman, Enemies Within: Inside the NYPD’s secret spying unit and bin Laden’s Final Plot against America (New York: Touchstone, 2013), 53-55; Gillespie, “Do the Zazi and Headley Arrests;” Dilanian, “NSA faces backlash.”

94 Nakashima, “NSA cites case.”
communications was “more urgent in tone than the last,” according to court documents.\textsuperscript{95}

It was these communications that alerted the authorities.

When presenting his four cases at the Congressional hearings in June 2013, Alexander explained that he couldn’t make the details of all the cases on his secret list public because “If we give all those out, we give all the secrets of how we’re tracking down the terrorists as a community, and we can’t do that.”\textsuperscript{96} The remaining 50 will remain shrouded in secret, then, presumably because it is believed that discussing them publicly would result in damage, perhaps even grave damage, to national security. Accordingly, so protected, we will never be able to examine them in our “healthy” debate on the issue of NSA surveillance.

Absent such information, and keeping in mind the impressive record of dissembling that NSA has so far amassed, it does seem to be a reasonable suspicion that the four cases discussed represent not a random selection from the list, but the best they could come up with. It that it so, the achievements of 215 do seem to be decidedly underwhelming.

In this regard, one could also examine that set of case studies of the 53 post-9/11 plots that have come to light by Islamist terrorists to damage targets in the United States.\textsuperscript{97} Since these have resulted in public arrests and trials, there is quite a bit of information available about them. Overall, where the plots have been disrupted, the task was accomplished by ordinary policing methods. The NSA programs do not seem to come up at all.

\textsuperscript{95} John Mueller, “Mueller on the Zazi Case: ‘This is It?’” Informed Comment, juancole.com, November 4, 2009.

\textsuperscript{96} Hearing of the House Permanent Select Committee on Intelligence.

\textsuperscript{97} Mueller, \textit{Terrorism Since 9/11}.  

34
At the June 2013 hearings, one committee member, Representative Jim Himes of Connecticut, noting that his constituents were mainly concerned about 215, tried to get Alexander and Joyce to indicate how many plots would have been carried out but for that program: “How essential, not just contributing to, but how essential are these authorities to stopping which terrorist attacks?” Alexander irrelevantly responded that 702 contributed to 90 percent of the cases, and in half of these it was “critical.” Further pressed about 215, the issue at hand, he said that “just over 10 of the cases had a “domestic nexus” and therefore 215 would apply, and that 215 “had a contribution” to the “vast majority” of these. Joyce then added more verbiage, proclaiming that every tool in the kit was both “essential” and “vital”: “I think you ask an almost impossible question to say how important each dot was….Our mission is to stop terrorism, to prevent it….And I can tell you, every tool is essential and vital. And the tools [under discussion] have been valuable to stopping some of those plots. You ask, how can you put a value on an American life? And I can tell you, it’s priceless.” Himes, out of time, ended by expressing his “hope” that “you’ll elucidate for us specifically case by case how many stopped terrorist attacks” the 215 program was “essential to.”

Abandoning 215

It certainly appears, then, that any benefit of the 215 program is considerably outweighed by its cost even assuming that the unknown, and perhaps unknowable, cost figure is quite small. That is, the program would very likely fail a full cost-benefit analysis handily even without taking into consideration privacy and civil liberties concerns. Representative Adam Schiff has done his own “on net” assessment. Even if the program is “occasionally successful,” he

98 Hearing of the House Permanent Select Committee on Intelligence.
concludes, “there’s still no justification that I can see for obtaining that amount of data in the first place.”

In the past, NSA has actually closed down such programs—though not without characteristic dissembling. That is, it was persuaded to conclude that some tools in its kit were not necessarily all that “essential and vital.” James Bamford reports that the agency had a nationwide program to store e-mail and Internet metadata in bulk for years. It was ended in 2011 for “operational and resource reasons,” according to the director of national intelligence. But, notes Bamford, a statement issued in 2013 by senators Ron Wyden and Mark Udall contends that:

the real reason the program was shut down was that the NSA was “unable” to prove the usefulness of the operation. “We were very concerned about this program’s impact on Americans’ civil liberties and privacy rights,” they said, “and we spent a significant portion of 2011 pressing intelligence officials to provide evidence of its effectiveness. They were unable to do so, and the program was shut down that year.” The senators added, “It is also important to note that intelligence agencies made statements to both Congress and the [FISA court] that significantly exaggerated this program’s effectiveness. This experience demonstrates to us that intelligence agencies’ assessment of the usefulness of particular collection program—even significant ones—are not always accurate.”

It seems likely that, “on net” (as the President puts it) the highly-controversial 215 program could also safely be retired for “operational and resource reasons” with little or no negative security consequences. In 2002, risk analyst Howard Kunreuther proposed that a key question in evaluating terrorism security measures should be “How much should we be willing to

99 Nakashima, “NSA cites case.”

100 Bamford, “They Know Much More Than You Think.”
pay for a small reduction in probabilities that are already extremely low?”\textsuperscript{101} If the 215 program has done little (and probably nothing) special to prevent or disrupt terrorist attacks in the United States, and if we are now having a healthy debate about the NSA programs, it seems reasonable to suggest that, even without full information about how the program costs, we are paying too much.

And, just possibly, there are other elements in the vast intelligence and policing empire spawned in panic and in unseemly haste after 9/11 that might also be retired.