THE GREAT WAR OF OUR TIME

THE CIA'S FIGHT AGAINST TERRORISM FROM AL QA'IDA TO ISIS

FORMER CIA DEPUTY DIRECTOR
MICHAEL MORELL
with Bill Harlow

CHAPTER 12

Breach of Trust

An employee of the Central Intelligence Agency liked to frequent chat rooms. His online persona was TheTrueHOOHA. Here is a chat from January 2009:

TheTrueHOOHA: HOLY SHIT
http://www.nytimes.com/2009/01/11/washington/lliran.html?_r=1&hp
[a reference to a *New York Times* article on purported US operations in Iran]

TheTrueHOOHA: WTF NYTIMES?
Are they TRYING to start a war?
Jesus Christ
They're like wikileaks

User19: they're just reporting dude.

TheTrueHOOHA: They're reporting classified shit.

TheTrueHOOHA: moreover, who the fuck are the anonymous sources telling them this?

TheTrueHOOHA: those people should be shot in the balls.

TheTrueHOOHA: I wonder how many hundreds of millions of dollars they just completely blew?

TheTrueHOOHA: these are the same people who blew the whole "we could listen to osama's cell phone" thing the same people who screwed us on wiretapping and over and over again. Thank god they're going out of business.

User19: the NYT?

TheTrueHOOHA: Hopefully they'll finally go bankrupt this year.
Yeah.

An exchange a few minutes later:

User19: is it unethical to report on government intrigue?

TheTrueHOOHA: VIOLATING NATIONAL SECURITY. No

User19: meh.
national security

TheTrueHOOHA: Um, YEEEEEEEEEEES

TheTrueHOOHA: that shit is classified for a reason

TheTrueHOOHA: it's not because "oh we hope our citizens don't find out"

TheTrueHOOHA: it's because "this shit won't work if Iran knows what we're doing."

TheTrueHOOHA was the online persona of Edward Snowden.

* * *

In the preface to this book, I explained how my final weeks as deputy director were consumed with a credible and serious threat from al Qa'ida's number one franchise—AQAP. Along with that threat, my final weeks in the job were also filled with another major issue. On June 5, 2013, the UK's *Guardian* newspaper carried a report claiming the NSA was collecting the phone records of millions of Verizon customers daily. This, of course, was a reference to the now-declassified telephony metadata program, which operates under provisions of the Patriot Act.

Under this program the telephone companies, operating under a broad court order, provided to the NSA the following information for calls made to and from US phone numbers—the number that initiated the call, the number that was called, the time of the call, and the duration of the call. The phone companies did not provide the NSA with the identities of the callers or the

content of the call—what was actually said in the conversation. It was akin to sharing what is on the outside of a letter's envelope—minus any names—without sharing what is inside the envelope.

The next day the *Washington Post* ran a story saying that the NSA was intercepting the e-mail communications of persons overseas as the messages passed through the United States. This program, which operates under Section 702 of the Foreign Intelligence Surveillance Act, focused on collecting foreign-to-foreign communications that, because of the nature of the Internet, ran through the United States.

Within four days the *Guardian* revealed that its source had been a young man named Edward Snowden. Through the *Guardian*, Snowden told his story—saying that he had become increasingly concerned about the massive NSA surveillance aimed at the public both in the United States and overseas, that he wanted there to be an open debate on the issue, and that he had taken documents from his job at the NSA in order to demonstrate his concern. Snowden said he had fled to Hong Kong on May 20.

Snowden had been an NSA contractor since 2009, working as a systems administrator. His most recent job had been at an NSA facility in Hawaii. And although he was an NSA contractor at the time of his flight to Hong Kong, we quickly learned that Snowden had worked for CIA from 2006 to 2009. Prior to that he had worked as a security specialist at the Center for Advanced Study of Language—a partnership between the University of Maryland and the intelligence community. This is where he received his first security clearance.

At a briefing in mid-June, Director Brennan and I made clear that we needed to know a number of things—as soon as possible. One, were there CIA documents or information in the materials that Snowden had stolen from the NSA? Two, had he stolen any classified information when he served at CIA? Three, how had he gotten a job at CIA and what were the circumstances of his departure in 2009, when he left to become a contractor for the NSA? And four, was Snowden working with any foreign intelligence service—either wittingly or not?

The first issue—had he stolen any CIA information while at the NSA—proved maddeningly difficult at first. Snowden's principal victim, the NSA, was understandably distraught at the massive security breach and initially refused to let CIA officers be part of its security review. It took a phone call from me to Chris Inglis, the NSA deputy director at Fort Meade (the NSA's headquarters), to break through that barrier. Inglis, an outstanding intelligence officer and friend, understood the importance of my request immediately, and simply

said, "I'll take care of it." Once CIA officers were given access, the news was not good. Snowden, a clever but relatively low-level computer systems administrator, had figured out how to access millions of documents. It was not clear what documents had been taken—but the scope and range of the potential loss was enormous. And as Agency officers sifted through the information to which Snowden had had access, they discovered that among the documents at risk were not just NSA secrets but CIA secrets as well.

On the issue of whether Snowden stole classified information while he worked at CIA, I am not permitted to provide the answer that was briefed to me, because of concerns about the national security implications if this information were disclosed.

I can say more about the questions involving Snowden's CIA employment. Amazingly, in 2006, this high school dropout with a GED and less than five months in the US Army Reserve—where he did not complete basic training—was hired by CIA to be a telecommunications support officer, or TISO (pronounced *tee-so*)—an important job that ensures that our officers can communicate securely with one another no matter where they are on the planet. Snowden had self-taught computer skills but little else going for him. At the time the Agency was still in the middle of a massive buildup in the aftermath of 9/11, and one of the areas of greatest need was TISOs. This is why Snowden got hired.

Snowden's employment application, work performance, and behaviors created concerns at the Agency—including security concerns. Snowden was aware of this, and he departed the Agency before they could be resolved and before the Agency could take any action against him. So the guy with whom CIA had concerns left the Agency and joined the ranks of the many contractors working in the intelligence community—before CIA could inform the rest of the IC of its worries. He even got a pay raise. He was working on the rolls of Dell and later Booz Allen Hamilton for the NSA.

On the fourth major question for us—the issue of possible foreign intelligence involvement with Snowden—we learned some very interesting things that I am not permitted to share. I can say that when Snowden stopped first in Chinese-controlled Hong Kong and later in Russia there is no doubt that the intelligence services of those countries had an enormous interest in him and the information he had stolen. Both the Chinese and the Russians would have used everything in their tool kits—from human approaches to technical attacks—to get at Snowden's stolen data as well as simply what he knew about the intelligence community.

My own view on this question is that both Chinese and Russian intelligence officers undoubtedly pitched him—offering him millions of dollars to share the documents he had stolen and to answer any questions they had about the NSA and CIA. But my guess is that Snowden said, "No, thank you," given his mind-set and his clear dislike for intelligence services of any stripe. My concern, however, is that Snowden may have unwittingly led the Chinese or, more likely, the Russians to his treasure chest of documents. Snowden thinks he is smart, but he was never in a position in his previous jobs to fully understand the immense capabilities of our Russian and Chinese counterparts and therefore not smart enough to realize when and how he might be being used.

This is not even to mention the interest that the Chinese and Russians would obviously have in the reporters to whom Snowden provided classified information. They too are undoubtedly targets of the Chinese, Russians, and others. To their credit, these reporters have refused to publish some of the most sensitive information in their possession. But not publishing it and protecting it from intelligence services are two completely different things. How well they have protected such information is open to question. They too do not understand the capabilities of our adversaries.

* * *

In my last week as deputy director I got a call from Denis McDonough, who in early 2013 had been promoted to be the president's chief of staff. "The president is thinking of putting together a commission to look into some of the issues raised as a result of the Snowden leaks. He'd like you to be a member." I promised to give the request some thought, and I discussed it with one of my mentors, a veteran of the intelligence community.

"Are you nuts?" the mentor asked. "You are about to become a civilian for the first time in thirty-three years." The last thing that I ought to do, he suggested, was agree to join a presidential commission. "Denis promises that it won't be that onerous," I told the mentor. "Yeah, that's what they always say," he advised. "Somebody needs to do this job, Michael, but as your friend, I'm telling you that it does not need to be you."

I did not follow my mentor's advice. In the end I decided that I could not say no to the president and to McDonough. And I could not say no given the enormous damage that Snowden had done to national security. So I found

myself, before I was even off the government payroll, serving as a member of the president's Review Group on Intelligence and Communications Technologies. Joining me on the group were three renowned law professors—Geof Stone from the University of Chicago, Cass Sunstein from Harvard, and Peter Swire from Georgia Tech. Also on the panel was Dick Clarke, a former senior government official with immense experience in terrorism, cyber security, and other national security issues. My mentor, of course, had in large measure been right. The panel soon took up much more time than McDonough had promised.

Operating from a federal office building on K Street in D.C., I began digging into the issue. The first thing that struck me was that there were a handful of causes of the "Snowden affair," which I defined as Snowden's successful theft over time of vast amounts of significant information coupled with the sharp negative reaction at home and abroad to the NSA's work. The first cause was, ironically, the enormous success of the National Security Agency in collecting information. Government agencies usually get in trouble for failing to do their jobs. In this case the NSA got in trouble, at least in part, for doing its job, as Snowden had in part been motivated by the breadth and depth of the NSA's collection capabilities.

I would argue that in the decade after 9/11, of all the agencies that make up the US intelligence community, none was more successful than the National Security Agency. And that is a significant statement for a CIA officer to make, because there is a bit of professional rivalry among intelligence organizations. In fact, I was a little chagrined by how well the NSA was doing relative to the Agency. The amount of critical intelligence the NSA was collecting was staggering, and that agency was—and remains—the collector of some of the most important pieces of the intelligence puzzle presented to the president and national security decision-makers every day.

It is important to note that all of the NSA operations that resulted in this treasure trove of intelligence collection were approved by the executive branch and overseen by Congress. Some of the operations were even overseen by the Foreign Intelligence Surveillance Court, made up of federal judges appointed by the chief justice of the Supreme Court. And the NSA did not disseminate anything to the rest of the intelligence community and to policy-makers that they had not been asked to collect by a rigorous requirement process managed by the director of national intelligence (DNI). In short, the NSA was not in any way acting as a rogue agency. Rather, it was doing the job that the DNI had given it and it was doing that job well.

Another cause of the Snowden affair was that, despite its great success, the NSA had two internal problems—one of which had contributed directly and one indirectly to Snowden's ability to steal the amount of information he did. The first problem was that the NSA—the world's most capable signals intelligence organization, an agency immensely skilled in stealing digital data—had had its pocket thoroughly picked. You would have thought that of all the government entities on the planet, the one least vulnerable to such grand theft would have been the NSA. But it turned out that the NSA had left itself vulnerable.

At its facility in Hawaii, where Snowden had gone to work every day, the NSA did not have the audit functions on its computer network that would have made Snowden's theft all but impossible. Like the audit function on personal credit cards, such software raises flags when people access information outside their normal pattern of type and volume. In fairness, the NSA had safeguards at its headquarters at Fort Meade—but it was vulnerable at the outer regions of its network, in places like Hawaii, where it had not yet installed the latest security technologies. It was simply an issue of the timetable for which NSA facility received security upgrades at what time. Hawaii was low on the list.

The second internal problem was that the NSA—an organization renowned for its secrecy—was remarkably transparent among its own people. The culture at the NSA was for personnel to freely talk among themselves about issues on which they were working. The NSA had its own wikis where its employees could post, for their colleagues to see, information about their projects—including those on which they worked hand in hand with CIA officers. The idea was to spread knowledge and learn from the successes of others, but it created an enormous security vulnerability, given the always-existing risk of an insider committed to stealing secrets. Snowden took advantage of this vulnerability, scooping up much of the information on these wikis. This kind of internal openness was anathema to the typical attitude in the intelligence community that information should be shared only with those who have a legitimate need to know.

The final cause of the Snowden affair was the failure of some in the media to accurately describe what they were seeing in the Snowden documents. Many of them went to the darkest corner of the room, and it had political impact. This was sloppy reporting. On June 6, CNN led with a story titled "Spying on Your Calls," and the story contained the following line: "When you call Grandma in Nebraska, the NSA knows." Fox noted that "NSA

knows your calling habits." MSNBC said that NSA is "screening your calls." The Associated Press said, "The government knows who you are calling. Every day. Every call." Glenn Greenwald, the reporter who broke the initial story, wrote, "Do you want to live with a government that knows everything you are doing?"

All of this was complete nonsense, but you could forgive the average citizen for not knowing that. Such reporting created the impression that NSA surveillance in the United States was much more intrusive than it really was. Media accounts created the impression that the NSA was listening to phone calls and reading e-mails—neither of which it was doing. Polling makes it clear that these inaccurate perceptions were immensely influential in shaping the ensuing political debate.

As I continued to read in our K Street office, the second thing that struck me was that the fundamental problem with which we were dealing was a loss of trust on several fronts—the loss of trust by a significant percentage of Americans in their own government, the loss of trust by some of our allies in the United States, and the loss of trust by overseas customers in a number of US companies—customers who were now concerned that the NSA had secret deals with these companies to compromise their products by placing "back doors" in their software and hardware.

To be clear, I was much less concerned about the loss of trust on the part of our allies than I was in the other two issues. Governments typically act in their own interests, and I was confident that the citizens of friendly nations would get over the temporary insult and that their governments were realistic enough to know that they too collect intelligence on friend and foe alike. Spying is the world's second-oldest profession and most of our allies have been at it since long before our nation was formed. A little harrumphing would be necessary for domestic political consumption—but this was not a major hurdle. From my time at the Agency, I am not aware of a single spying scandal that has had a long-term impact on a bilateral relationship, and I was convinced that the Snowden disclosures would not do so either.

The Review Group offered forty-six recommendations. Because of the strong public reaction to the Snowden leaks, I became convinced that our panel would have to make a number of strong recommendations if the country was to begin taking the first steps toward restoring public support for our government. If we had conducted a comprehensive review of NSA programs prior to the wholesale dumping out of intelligence secrets, I would have been in favor of just a few changes to the way the NSA was doing business. But in

light of the public outcry, modest steps would never work now. We would have to make some dramatic proposals if we were to have any hope of regaining lost support.

Two recommendations stood out to me as much more important than the rest—and I believe we would have made these recommendations with or without Snowden. The first was the group's recommendation about the 215 metadata program—that the government no longer hold the data and that it be required to obtain a court order prior to querying the data each time, as opposed to the then-current situation in which the NSA was holding the data and could query it at will under a broad court order. This recommendation, and the president's acceptance of it, was absolutely necessary, I thought, to winning back the trust of the American people and keeping the program alive. Without winning back that trust, I was concerned that Congress would kill the entire program—in essence throwing the baby out with the bathwater.

And it also made sense. While the NSA did nothing illegal and committed no abuses under the 215 program, the group's law professors, particularly Geof Stone, convinced me that such power in the hands of the government creates the potential for abuse, and that we therefore had to recommend steps that would make it much harder for future administrations—or even rogue elements within administrations—to overstep their bounds.

The second recommendation that made great sense to me was to put in the hands of senior policy-makers decisions on what intelligence to collect and how to collect it—particularly for collection that carries significant political, economic, or foreign policy risks. The NSA had largely been collecting information because it could, not necessarily in all cases because it should. To be sure, some oversight was already in place, but it was not broad enough to cover all the collection activities that carried special risks, and it rarely dealt with the question of how intelligence would be collected. The best example of such risky activity, of course, is spying on the senior leadership of allies. Only senior policy-makers looking at all the benefits and risks can make decisions on what to collect and how. At the end of the day, only senior policy-makers can decide on the "should."

There was also a set of recommendations that I thought absolutely critical—not for winning back trust but for making sure that another Edward Snowden does not happen. These recommendations—outlined in a chapter of our report called "Protecting Data"—received no media coverage. In this chapter we recommended two fundamental changes—that the government move from assessing the security risks of its employees every five years to

doing it continuously, and that classified computer networks have state-of-the-art security software. It turns out that the best network security is not in the intelligence community—it is on Wall Street. This, of course, should not be surprising, as Wall Street is protecting something very important—your money.

But this chapter also called for another change—a revolutionary change that is not likely to see the light of day. Our Review Group felt that the tightest security practices should apply not only to intelligence community employees and networks but also to any government employees with access to secrets—including political appointees in the White House and elsewhere—and any computer networks that contain classified information. After all, Private Chelsea Manning was not an IC employee and was not operating on an IC computer network when she stole information and passed it to WikiLeaks. All of these steps are necessary in order to ensure that another Snowden or Manning affair does not happen. And they are essential to ensure that secrets stay secrets. If our recommended changes are not implemented, I fear it will happen again.

I worked hard when we were crafting our recommendations to see that there was language attached that would permit reasonable accommodation for the business of intelligence, albeit generally with more oversight. My colleagues were very supportive of this. After all, the balance we were trying to strike was in winning back trust—and advancing privacy and civil liberties—without doing damage to the intelligence community's ability to do its critically important job.

The Review Group was surprisingly unified in its recommendations. Very little argument, very little drama.

In the end the president was supportive of a large majority of the Review Group's recommendations. He accepted 70 percent of the recommendations—including the two that I saw as the most important; he agreed to study 15 percent; and he rejected 15 percent. The ones he rejected had to do with the organizational structure of the NSA. And while I did not disagree with these recommendations, I did not see them as integral to the effort to win back trust. How many of our recommendations ultimately get adopted and the extent to which they help restore public confidence in the NSA, intelligence community, and government remains to be seen.

In the aftermath of the public release of the report, I felt that the media generally mischaracterized both the breadth of the report and our key recommendations regarding the 215 program. A number of media outlets were

calling the recommendations "sweeping reforms of the intelligence community," and they were saying that the Review Group had recommended an end to the 215 program. Neither was true.

While our recommendations were many, they were not sweeping. Where we suggested change, it was most often a recommendation to add layers of scrutiny and review—making certain kinds of operations more cumbersome, but not impossible.

The 215 program was the best example. We saw real value in the program and we recommended to the president a change in approach, not a wholesale rejection of the program. We recommended that the 215 database should be taken out of the hands of the government and each query should require an individual court order.

Although we did not discuss it as a group, I also thought the database should actually be expanded to include all calls made in the United States and should include e-mails as well. Today the database does not contain the metadata from *all* calls and does not contain the metadata from *any* e-mails. It should. Imagine a scenario in which AQAP in Yemen sends multiple operatives to the United States to conduct attacks, and the intelligence community learns of the plot and runs a search of Yemen-based phone numbers against the 215 database. But the search is a dry hole—because AQAP is using a phone system outside the 215 program. Imagine the outrage of the American public when these facts became public following a successful attack.

* * *

Two final thoughts—one on the damage done by Snowden and the other on Snowden as an individual. I believe that the Snowden disclosures will go down in history as the greatest compromise of classified information ever. Period. Full stop. The damage done has already been significant and it will continue to grow. While great attention and angst have been devoted to the loss he created by exposing the 215 telephony metadata program, Snowden damaged a much more important program involving the collection of e-mail information from foreign-based terrorists, the 702 program mentioned earlier.

Within weeks of the leaks, terrorist organizations around the world were already starting to modify their actions in light of what Snowden disclosed. Communication sources dried up, tactics were changed. Terrorists moved to more secure communication platforms, they are using encryption, and they

are avoiding electronic communications altogether. ISIS was one of the terrorist groups that learned from Snowden, and it is clear his actions played a role in the rise of ISIS. In short, Snowden has made the United States and our allies considerably less safe. I do not say this lightly: Americans may well die at the hands of terrorists because of Edward Snowden's actions.

The damage caused by Snowden is not limited to terrorists' adjusting their tactics. Foreign intelligence services have been studying the tremendous amount of intelligence data now available to them in the media and deriving work-arounds to thwart US collection efforts. You can bet that outfits like the Iranian MOIS—Iran's CIA—have cells of smart young people studying the news articles and working on countermeasures. What is more, we know that foreign intelligence services will export their lessons learned. Outfits like the Russians and Chinese will study our tactics and then go to other, less sophisticated foreign intelligence services and offer tips about how to frustrate the American collection effort. In return they will be given access and influence that will only add to our woes.

One of the most troublesome leaks in this regard was the publication in the *Washington Post* of the intelligence community's Congressional Budget Justification Book (CBJB) for Fiscal Year 2013. This is the IC's so-called black budget. It lists where we are putting our priorities, where we think we are having our greatest intelligence successes, and where we still need to do more work. For our enemies, having it is like having the playbook of the opposing NFL team. I guarantee you that the SVR, the Russian foreign intelligence service, would have paid millions of dollars for such a document. Instead they didn't even have to invest $1.25, the cover price of the *Washington Post*, since the document is available free online. To its credit, the *Washington Post*, at the request of the DNI, did not publish the document in its entirety—protecting the most sensitive secrets—but still the damage was enormous.

This just refers to the material that has been disclosed. We don't know what other documents Snowden and his media allies have in their possession that they will publish at some point. It is a good bet that there is more to come—and therefore more damage (material from the Snowden leaks was still being published at the writing of this book—in early 2015—eighteen months after Snowden walked away from the United States). And we do not know what information foreign intelligence services have already acquired of what was stolen but not yet disclosed.

One more word about damage and that relates to the earlier point about a loss of trust on the part of foreigners in American products. As a result of that

lack of trust, US information technology companies have lost hundreds of millions of dollars in sales overseas. People now shy away from US IT products over a concern that the US government is using those products to collect intelligence. This will be the hardest loss of trust to restore. Apple's move in the fall of 2014 to encrypt all data on its products so even Apple can't get at it is a response to that loss of trust. We can only hope, for the sake of the American economy, that US firms will win that trust back.

What were Snowden's motives? One thing I am sure of is that he was not acting out of a simple desire to protect the privacy and civil liberties of Americans or even citizens overseas. And this takes any idea that he was a whistle-blower off the table. The vast amount of information he stole and disclosed to journalists had nothing to do with privacy. Legitimate arguments can be had about how far our intelligence community should go in collecting information that potentially could touch US citizens. I would suggest, however, that the appropriate place for those discussions to occur is before the congressional oversight committees. Every one of the hundreds of thousands of people who have access to classified information cannot be allowed to individually decide to disclose information just because they do not like a particular program. If Snowden felt that privacy rights were being trampled, there were avenues available for him to make his concerns known to our elected representatives of Congress. If he didn't trust congressional overseers, departmental ombudsmen, and inspectors general to act, he could have easily taken one or two documents that solely addressed the privacy issue, put them in a plain brown envelope, and mailed them to the *Washington Post* (an action I am in no way endorsing, by the way). Instead he backed up a virtual tractor trailer and emptied a warehouse full of documents—the vast majority of which he could not possibly have read and few of which he would likely understand. Then he delivered the documents to a variety of international news organizations and God only knows who else.

So if is his primary motivation was not the protection of privacy and civil liberties, what was it? I don't know for sure, but I strongly suspect that his actions were all about his favorite subject: Edward J. Snowden. It is clear that Snowden has an enormous ego—one that had to be quite large for him to convince himself that he knew better than two presidents (of different parties), the intelligence committees of multiple congresses, the Justice Department of two administrations, and tens of FISA court judges appointed by the chief justice of the Supreme Court. That is arrogance.

A full answer to the question of why he did what he did would require

that he sit down for months with counterintelligence debriefers and top-notch psychologists. But my hunch is that Snowden is someone who felt underappreciated and insufficiently recognized for his self-perceived brilliance while working for CIA and the NSA, a feeling that left a huge chip on his shoulder. This is a classic attitude that intelligence officers try to exploit among the enemy. You find someone working for the other side and tell him that he is not receiving the recognition, pay, and honors due him, and you provide those in return for the individual's betrayal of his country. This was the psychology that led Aldrich Ames and Robert Hanssen to commit espionage. Let me stress that I am not suggesting here that Snowden was encouraged by a foreign intelligence service to act as he did—only that the same psychological dynamic can motivate someone to act alone and still do as much damage. In short, I think he wanted to show the world how smart he was by crippling the agencies that did not recognize his brilliance.

As big as his ego was in June 2013, it must have grown exponentially since. The media and international organizations have relentlessly pumped hot air into his inflated self-esteem. Institutions ranging from the European Union to politicians musing about putting him forward for the Nobel Peace Prize have undoubtedly added to his sense of worth. Some news organizations have awarded him icon status. I recall seeing one media outlet seek his wisdom on what foreign intelligence targets would be appropriate for the United States to collect against. The absurdity of this is stunning. It would be like going to the equipment manager for the Dallas Cowboys and asking him what plays the team should run on Sunday.

* * *

On June 21, 2013, the US Department of Justice charged Edward Snowden with espionage. If I could have a conversation with Snowden, I would ask him only one question. That question would be, "Edward, you had enough trust in the American people that you thought they could and should judge for themselves the right balance between liberty and security. If you really believe that, then surely you must believe that those same Americans could and should judge your behavior with regard to the disclosures you made possible. So why don't you come home and be judged before a jury of your peers?"

I know some readers will think, "Of course you say bad things about Snowden because he exposed systemic wrongdoing by the intelligence

community, a place you worked for thirty-three years." My answer is that the programs he disclosed were legal and approved at the highest levels of the US government and that the damage he did was huge. As someone who was uniquely positioned to evaluate that damage, I can tell you that the costs of Snowden's actions will be enormous. If he truly thought his actions were those of civil disobedience, the honorable approach would have been to take his stand and then accept the consequences.

* * *

Throughout this entire affair, the people I have worried most about are the men and women of the National Security Agency. The media and some politicians have demonized the organization for which they work and, to an extent, the officers of the NSA themselves. They do not deserve this. They go to work every day for a government salary, they work long hours for no public acclaim, and they execute tasks that keep the country safe and that literally save lives. They are talented, professional, and dedicated.

In collecting intelligence, the NSA and its officers in no way did anything wrong. The NSA never undertook a program without the approval of the executive branch and the oversight of the congressional intelligence committees or the courts. The NSA never broke the law and never abused the power that it had been given in the 215 program. In short, the NSA and its officers were doing the job that they had been asked to do.

NSA officers are patriots. Edward Snowden is a traitor.