Reflections on the IG's Role, Stellarwind, and the Information Sharing Fiasco

Joel Brenner*

Introduction

I was sworn in as the Inspector General (IG) of the National Security Agency (NSA) in April 2002, on the heels of the 9/11 attacks. Four months later, the NSA director, Lt. Gen. Michael Hayden (USAF) read me into a top-secret collection program called Stellarwind. The program had begun the month after the attacks. It had two parts. Under the first part, NSA intercepted phone calls between persons overseas who were known to be affiliated with al Qaida and anyone in the United States. Under the second part, NSA collected bulk phone call metadata about all the phone calls made in the United States – not the content of the calls,

* Joel Brenner is a Senior Research Fellow at MIT's Center for International Studies and a member of the Intelligence Community Studies Board. He was the Inspector General of the National Security Agency (2002-2006), the National Counterintelligence Executive (2006-2009), and Senior Counsel of NSA (2009-2010). Early in his career he was a trial lawyer in the Antitrust Division of the U.S. Department of Justice.

but information about each call such as to/from and duration information. The purpose was to discover domestic terrorist networks that might exist. On the face of it, Stellarwind was a violation of the Foreign Intelligence Surveillance Act (FISA).[1] I thought avoiding FISA was a strategic blunder that would destroy the high degree of national unity that had developed, which it did, and I said so at the time;[2] but I was not calling the shots, neither was General Hayden.

The White House's rationale was that FISA applications for interceptions took too long and would cause critical delay. FISA also had no provision permitting the collection of domestic metadata. I believed the president had the power to implement the program temporarily – indeed, he would have been derelict not to do it – but like President Lincoln after suspending habeas corpus, he was obliged, I thought, to ask Congress to ratify his actions by amending FISA.[3] In early 2002, a Congress that had just approved the PATRIOT Act without reading it would have amended FISA to accommodate the metadata program too.[4] But neither Vice President Cheney (whose office ran Stellarwind) nor President Bush had any intention of asking Congress to amend FISA. Their goal was executive power. I believed the program would be unconstitutional at some point – but when? In the meantime, my duty was to oversee it.

I. WHEN A PROGRAM IS HIGHLY SENSITIVE OR LIKELY TO BE CONTROVERSIAL, THE IG SHOULD BEGIN TO REVIEW IT EARLY

My deputy, Brian McAndrew, and I decided to scrutinize Stellarwind *continually*, beginning with program reviews. Our small team (only three of us at first) demanded to see written rules and procedures that we doubted were in place, because demanding them was the best way to get them in place. Then we scrubbed them with a wire brush to tighten them up. Ultimately, we would audit the program; but it was too soon to audit something that had been up and running only a few months. Also, you can't audit systems that don't retain data, and you

1. 50 U.S.C. §§ 1801 et seq. For the act as it then existed, see Pub. L. 95–511, title I, § 101, 92 Stat. 1783 (1978); Pub. L. 106–120, title VI, § 601, 113 Stat. 1619 (Dec. 3, 1999); Pub. L. 107–56, title X, § 1003, 115 Stat. 392 (2001); Pub. L. 107–108, title III, § 314(a)(1), (c)(2), 115 Stat. 1402, 1403, (2001). For FISA's history and purpose, see Joel Brenner, *A Review of 'The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age' by Laura K. Donohue*, 9 J. NAT'L SECURITY L. & POL'Y 631, 642-647 (2017) (book review).

2. MICHAEL V. HAYDEN, PLAYING TO THE EDGE: AMERICAN INTELLIGENCE IN THE AGE OF TERROR 77, 86-87 (2016).

3. My own analysis depended on the President's powers under Article II of the Constitution. U.S. CONST. art. II. The Justice Department's Office of Legal Counsel, under Jack Goldsmith, later emphasized that Congress had authorized Stellarwind when it passed the Authorization for the Use of Military Force in Iraq of 2002, Pub. L. 107-243, 116 Stat. 1498 (2002).

4. According to U.S. District Judge Royce Lamberth, then the Chief Judge of the FISA Court, "'We could have gone to Congress, hat in hand, the judicial branch and the executive branch together, and gotten any statutory change we wanted in those days, I felt like,' he said. 'And I felt like there was a way the statute could have been tweaked in a way that they could have lived with. But they wanted to demonstrate that the president's power was supreme, and the judiciary was just a tagalong when necessary, but not appreciated.'" BARTON GELLMAN, ANGLER: THE CHENEY VICE PRESIDENCY 302 (2008).

can't audit data without a sampling plan, which would take time to develop. If we followed the orthodox IG model and waited until the supposedly temporary program had been running several years or ended entirely, we could open a formal audit, demand to see whatever we wanted, criticize the Agency's data retention practices, and accuse people of violating the terms of a presidential order *they were not even allowed to read*. That's how IGs often do things. It keeps them removed from decisions they must later review, and that's an important principle. In this case, however, if we waited, the program might not be auditable at all. You can't make people give you data they don't keep. So McAndrew and I decided we would conduct program reviews from the start. That would mean walking a tightrope, conferring with management but not making management decisions – and persuading people that seeing things our way made sense.

II. YOU CANNOT BE RESPONSIBLE FOR OVERSEEING A PROGRAM IF YOU DO NOT HAVE A COMPLETE UNDERSTANDING OF ITS TERMS

When General Hayden read me into Stellarwind, he showed me the President's authorizations and said I could review them in my office but could not copy them. Some days later, after sober reflection, I copied them anyway. Every subsequent order I also copied. We kept them in a safe in the Office of the Inspector General (OIG), and only three people saw them: my deputy, my head of intel oversight, and me. I disobeyed General Hayden reluctantly. He and I enjoyed an unusually high degree of trust between an agency head and an IG, but the implicit message when he read me into the program was that I would review it, and I was not going to be responsible for overseeing a massive SIGINT program when I did not have a record of its terms. I suspect the general knew I would copy the Authorizations, but I never asked him and never will. Some things are best left unsaid.

III. WHEN PEOPLE KNOW YOU HAVE A BIG STICK, YOU RARELY NEED TO SWING IT. PERSUASION OFTEN GETS BETTER RESULTS

NSA program managers laboring in the bowels of the Fort were not accustomed to the level of intrusion we were pushing. We wanted more and better data and we wanted it fast. We wanted rules about how long the data would be kept and who had access to it. We wanted a written record of who approved every interception and the facts on which every decision to intercept was based. And we wanted everybody in the program to understand that *nobody* outside the NSA chain of command could decide that an interception was justified.

Unfortunately, we weren't getting what we wanted. The program manager was slow-rolling us. She was too smart to tell us no; she just made excuses and iced the puck. The IG carries a big stick and everyone knows it, but I wanted willing cooperation, not grudging compliance.

I called a meeting with program officials and their lawyers. Ordinarily, if anyone other than the director or his deputy meets with IG, they come to the IG; but pulling rank would not get us where we wanted to be. I called this meeting in the

program's workspace. I didn't send subordinates. I went myself. "We need this information. Quickly," I said. "Your pace is too leisurely."

"Leisurely?" came the angry reply. Did I have any idea of the hours they were working? How long it had been since any of them had a day off? They were chasing people planting roadside bombs, killing our troops, and blowing up girls' schools. The man was broiling and red-faced, and strung out. My requests, he said, could wait.

Deep breath.

I knew how hard they were working. "I also understand something you guys in the trenches do not understand," I said. "I know what this Agency looks like from downtown, and you don't. And I know what this program is going to look like when people find out about it." I didn't know whether that would happen next week, or next year, or the year after that, but it was going to happen. And when all the laundry was hung out, it wouldn't matter how heroically they'd worked. Half the people in this country they were trying to protect were going to think we were all scoundrels. There's going to be a storm, I said, and when it breaks, I wanted the brown stuff flying between one end of Pennsylvania Avenue and the other – not between Congress and the Agency. It would be like the intelligence scandals in 1976 – or didn't they know about that? If my office couldn't account for what they were doing – if we couldn't *prove* they were following the president's Authorizations to the letter, we'd all be up on the Hill in front of the TV cameras, under oath, looking like public enemies. Which may happen anyway. "Which of you will want to testify?"

I waited. No hands went up.

"And that," I said, barely above a whisper, "is why you're going to find the time to give us the information we want, faster than you want to do it."

The room went dead quiet, the anger bled out. This was a turning point. From that day, a remarkable level of trust began to develop between the IG's office and the program officials.

IV. THE RULES GOVERNING INTELLIGENCE COLLECTION – NOT OPERATIONAL OR TARGETING INFORMATION, BUT THE RULES ABOUT WHAT CAN AND CANNOT BE COLLECTED – MUST BE MADE IN PUBLIC

The White House did not want a public debate in Congress over surveillance. They feared alerting our enemies to our collection rules. That concern was not foolish. Osama bin Laden had abandoned all telephonic communications following a leak. But a massive program like Stellarwind could not long remain secret, and it didn't. The revelations beginning in December 2005 resulted in a predictable political fire storm and dramatically more publicity than any Congressional debate would have done in early or mid-2002. When FISA was changed in 2008 to permit what Bush had unilaterally done starting in 2001, a vigorous public debate did follow, but even then "the inner workings of the program were *not* exposed."[5]

5. HAYDEN, *supra* note 2, at 87 (emphasis in the original).

Stellarwind was run from the Office of the Vice President, which took secrecy to perverse extremes. The Justice Department's Office of Legal Counsel (OLC) produced a legal opinion endorsing the program's legality – but nobody could see it. It was written by a subordinate OLC official known to favor virtually unlimited executive power.[6] Even the then-head of OLC was not permitted to see it. Nor was the director of NSA or NSA's general counsel, or the Pentagon's general counsel; nor was I as NSA's IG. The result was that everyone qualified to review OLC's opinion for factual accuracy, for its assumptions about how collection mechanisms actually worked, or for its legal analysis was prohibited from seeing it. So far as I know, this had never happened before, and the effort led the administration into a dark corner. This wasn't merely the executive's attack on a particular legal doctrine; it was an attack on the culture of law itself, and it was coming straight out of the White House.

In the common law tradition, reasoning takes place in the open based on a transparent evaluation of legal authorities. Common law courts don't hand down *diktats*. Even in the case of a classified program, OLC may issue a classified opinion, and anyone with the proper classification can see it; or a court may issue an opinion with a classified annex, but the reasoning is publicly set forth. Intelligence sources and methods are opaque and meant to be so, but our laws are public and transparent. When you decided that *the law itself constituted an intelligence method* and could not be disclosed without tipping off the enemy – this was the administration's view on Stellarwind – it followed that you had to make law in secret. And if the real law could therefore not appear on the statute books, then real law would be made off the books, on a moonless night. You had to keep it unknown and unreviewable, preferably forever. And with what result? Little or no tactical advantage was gained from Stellarwind that could not have been gained using FISA as ultimately amended. It was a strategic blunder that helped destroy the public's trust in government. It divided the country. That was about all it did.

V. INTELLIGENCE AGENCIES MUST CONTINUE TO HONOR THE "NEED TO KNOW" PRINCIPLE. SEPARATING THE DUTY TO DISSEMINATE CLASSIFIED INFORMATION AFTER 9/11 FROM THE DUTY TO PROTECT IT WAS A FAILURE OF JUDGMENT THAT DIRECTLY CONTRIBUTED TO STRATEGIC LOSSES OF INFORMATION

The IC used to work on Ben Franklin's principle that three people can keep a secret if two of them are dead. Given institutional rivalries, however, that salutary precept had led to disaster on 9/11, as the government's left hand had no idea what the right hand was doing. And so "need to know" became a dirty word even as we were putting supposedly secret information into systems to which thousands of people had access. The need-to-know principle had indeed been grossly abused before 9/11, and sometimes it still is, but it is not possible to run an

6. Charlie Savage, *George W. Bush Made Retroactive N.S.A. 'Fix' After Hospital Room Showdown*, N.Y. TIMES (Sept. 20, 2015), https://perma.cc/V86D-LZ7R.

intelligence agency without it. After 9/11, however, the federal government consciously separated the duty to "share" – I prefer to say disseminate – classified information from the duty to protect it. We did this doctrinally through executive orders,[7] and we did it organizationally through a statutory office within the Office of the Director of National Intelligence (ODNI)[8] whose entire purpose was to further the "information sharing environment" – with no serious attention, let alone responsibility, for protecting secrets. High officials waxed eloquent about sharing as if they thought intel agencies operated in Mr. Rodgers' Neighborhood.

Information hoarding was indeed a serious problem. The Congress, the President, and the Director of National Intelligence (DNI) were trying to change institutional culture. That's hard. They knew that if you want to do that, your messaging must be relentlessly focused. But therein lay the dilemma: *You cannot make good policy if you cannot keep more than one important idea in your head at the same time*. We weren't doing that. Doctrinally and organizationally, we had separated the duty to share information from the duty to protect it. This was a mandated and predictable disaster in the making.

In early 2010, a U.S. Army private now known as Chelsea Manning worked as a low-level analyst in Iraq and spilled a trove of classified information to WikiLeaks. Some of it dealt with the ugly result of an airstrike on journalists, but much of the leaked information had nothing to do with Manning's responsibilities – diplomatic cables about Iceland's economy, for instance, and a diplomatic read-out of a meeting with the kind of Saudi Arabia. Why did Manning have access to that traffic? It was a prime instance of an agency dumping classified information into systems where it didn't belong. Even then, however, it took nearly two more years before the White House sharing rhetoric began to change,[9] and it was too little, too late.

A far more consequential shock was delivered in May 2013 by Edward Snowden, from Hong Kong, where he had fled on his way to Russia after engineering the largest compromise of top-secret information from this or any country. The scope of his leaks was vast. He identified foreign sources. He disclosed the specific overseas locations from which NSA collected information, and he identified specific foreign systems our agencies had penetrated. He disclosed specific electronic methods and tools. He ruined critical relations with companies and nations that had been helpful to our services. This was an intelligence disaster of a high order. It disrupted relations with allies. It caused an immense international loss of trust in U.S. technology and billions of dollars of lost business. And it crippled U.S. influence in international standards setting bodies. No foreign

7. *E.g.,* Exec. Order No. 13356, 69 Fed. Reg. 53599 (2004-05) *reissued as* Exec. Order No. 13388, 70 Fed. Reg. 62023 (2005).

8. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108–458, § 1016, 118 Stat. 3664 (2004).

9. *See* Press Release, Office of the Press Sec'y, The White House, National Strategy for Information Sharing and Safeguarding (Dec. 19, 2012), https://perma.cc/34AS-F8C3.

power could have managed this body blow to the United States. It had been done by an insider.

Snowden intended to harm the United States and should therefore be regarded as a spy. Indeed he was a penetration agent; that is, he sought contract work at NSA in order to leak top-secret material before he knew what he would find.[10] The vast majority of the information he leaked had nothing to do with the meta-data collection program. Yet nearly all the public attention Snowden received in the United States focused only on his disclosure of that program. Had that been the extent of his leaks, I believe he would already be back in the United States and out of jail. In fact, that was a small part of what he disclosed. The Snowden debacle had many causes, but it is relevant here because a great deal of what he compromised was available to him only because it was found in systems created to foster sharing after 9/11 and that had weak means of safeguarding it.

VI. TRUST IS EASY TO DESTROY AND HARD TO CREATE. EXPLAIN YOURSELF

Americans don't like rules. They especially don't like rules whose purpose they don't understand, and they don't follow them if they can help it. People want explanations. So early in my tenure I addressed the global workforce on closed circuit TV. I told them about the post-Watergate revelations of intelligence abuses. "The entire intelligence community had lost the public's trust in the '70s, and it took us a generation to get it back," I said. "Trust is easy to destroy and hard to create. Institutions are easy to cripple and hard to create." I reminded them that we worked in an agency that was powerful and secret in a culture that deeply distrusts power and secrecy, but wants intelligence. "That paradox," I said, "can be resolved only when the public believes we're doing our jobs in conformity with the laws and Constitution of the democratic nation we represent." My office later proposed and collaborated with the agency's lawyers, historians, and video techs to create new training materials that emphasized *why* we regulate surveillance, not just what the rules are.

VII. IGS CAN BE MORE EFFECTIVE BY REVIEWING OR AUDITING SOME PROGRAMS WHILE THEY ARE ON-GOING, AND BEFORE MILESTONE DECISIONS ARE MADE

The NSA IG's office was required to spend a large portion of its resources on statutorily required reports to Congress, most of which were read perfunctorily by a few staff, if at all. We also dealt with serious allegations of contract irregularities and with discrimination, timecard fraud, abusive bosses, and so forth. Some of this effort is reactive, but IGs, like prosecutors, must decide what to focus on, and I thought our substantial audit capabilities, especially our contract

10. After Snowden had already stolen thousands of classified documents while working for Dell, he switched jobs to Booz Allen Hamilton. When Laura Poitras asked him why he switched, he said: "'My position with Booz Allen Hamilton granted me access to lists of machines all over the world the NSA hacked.' Snowden told her that he deliberately went to Booz Allen Hamilton to get access to the 'lists' revealing the NSA's sources in foreign countries.'" Edward J. Epstein, How America Lost Its Secrets: Edward Snowden, the Man and the Theft (Knopf, 2017), at 97.

audits, were being squandered on reports that had no effect on how the agency did business.[11]

We were writing the histories of ancient train wrecks, I told my audit chief, and nobody cared. No contract got terminated or adjusted because of what we were doing. No money was saved. Nobody got promoted or demoted, got a bonus or lost a job. From now on, OIG was going to audit active contracts, and we would issue audit reports 60 days in advance of milestone decisions. These were decisions about whether to continue a contract, and if so, on what terms. Whether my old office is still doing that, I have no idea, but I'm sure it was a prudent course correction. It was another example of how early intervention by an IG, consistent with the duty as an oversight official to remain aloof from management, could make an agency work better. In my view, making the agency work better should be an IG's strategic goal. All the rest is tactics.

VIII. REGARDLESS OF WHAT THE STATUTES SAY, YOU'RE NOT INDEPENDENT IF YOU CAN'T AFFORD TO QUIT

IGs have wide but not complete statutory independence because they are executive branch officials, not free agents. Regardless of what the law says about independence, however, all government officials must have lines beyond which they will resign rather than follow an order or (in the case of an IG) be restricted in what they are permitted to examine. To be truly independent, however, you must be an ascetic with no family responsibilities, or you must have a financial cushion that allows you to quit. Mortgaged to the hilt? Groaning under tuition bills? No safe place to land in a hurry? You may think you're independent, but I hope you don't have to prove it. Always figure out in advance where you could go next if you must resign.

11. These were program audits, not financial audits, which were GAO's job.