Secrecy and Society

ISSN: 2377-6188

Manuscript 1080

# Review, Dark Mirror: Edward Snowden and the American Surveillance State, by Barton Gellman

Patrice McDermott

# Review, Dark Mirror: Edward Snowden and the American Surveillance State, by Barton Gellman

**Keywords**

national security, NSA, Edward Snowden, secrecy, surveillance, whistleblowing

# Review, *Dark Mirror: Edward Snowden and the American Surveillance State*, by Barton Gellman

Reviewed by Patrice McDermott[1]

*Dark Mirror: Edward Snowden and the American Surveillance State.* New York: Penguin Press, 2020. 448 pp. / ISBN 9781594206016 (hardcover) / 9780698153394 (ebook) / https://www.penguinrandomhouse.com/books/316047/dark-mirror-by-barton-gellman/

**Keywords:** accountability, domestic intelligence surveillance, electronic privacy, electronic surveillance, FISA, Foreign Intelligence Surveillance Act of 1978, Foreign Intelligence Surveillance Court, Graph-in-Memory, leaks, MAINWAY, oversight, PRISM, secrecy, secrecy studies, Edward Snowden, U.S. National Security Agency, warrantless surveillance, STELLARWIND

*Dark Mirror* is, in a positive sense, a "yarn." The book tells a story and much of it is about the "education" of Gellman himself as he worked through the stunning material Edward Snowden provided. This material, his work as a reporter at *The Washington Post*, and his contacts in the government enabled Gellman to understand, process, and report on the vast power of the surveillance state and the invasion of privacy it empowered itself to build. *Dark Mirror* is also an enlightening exploration of Snowden himself.

[1] Government Information Watch and former executive director, OpenTheGovernment, pmcdermott@govinfowatch.net.

I came to Gellman's book with what I thought was a reasonably good insight into what the U.S. Government was up to in digital information surveillance and some hope about the ability to curtail abuses. I came as a long-time advocate of greater transparency and accountability. I was not prepared for how deeply the rich trove of information revealed would shock me.

Gellman's book is divisible into four narratives, which are not chronological accounts of events, but rather fact-based stories. This review will address three of them: the surveillance technology; how Snowden managed to be positioned to exfiltrate the massive trove of information on that technology for government surveillance on which he blew the whistle; and the evasions, lies, misdirection, and abdication of responsibility by the constitutional authorities charged with oversight, and the executive branch's thoughts and actions about accountability.

While Gellman is relatively straightforward in his telling of Snowden's narrative, the other narratives loop around and back onto one another. This made answering the "what did we know and when did we know it" questions a challenge. Many of the details behind the stories told by Gellman (2020, 361-411) are contained in the Notes, which seem to be not endnotes, but rather Gellman's notes for the book. There is no indication of them in the body of the text, although it is possible to link from a Note *back* to the text to which it applies. There are no citations contained in the text of the book and no endnotes. The citations and links that appear in this review have been supplied by me.

In the narratives about the surveillance technology, and about the actions of government officials particularly, Gellman assumes a large degree of awareness and understanding - and memory - of events and confrontations in the early 2000s. These were widely covered in his *Washington Post* stories and by other reporters beginning, for the most part, almost ten years ago. I tried to include links to explanations that were useful to me in jogging - and enriching - my memory. I am also aware that not all potential readers of this review lived directly through this portion of American history.

I struggled with how much to share of the details of Gellman's discoveries from the Snowden archive. Not out of reluctance to share this information, but out of concern not to discourage readers from diving into Gellman's book. Even given the length of this review, it leaves most of this important story found in the book untold.

The fourth narrative is Gellman's story of how he came to receive the information, its impact on his work, his discussions with possible publishers and *The Washington Post*, and his discussions/confrontations with current and former government officials. I commend *Dark Mirror* to the reader. Here, as throughout the book, Gellman is a compelling story-teller.

## The Review

This review will look first at the surveillance technology and what we learned about it. Information comes from Snowden's archive and Gellman's interchanges and discussions with executive branch officials. Gellman uses the lower case, so I follow his format. The second section reviews Snowden's transit through the U.S. Intelligence Community (IC) as a contract employee of primarily Dell, but also of Booz Allen. This section is based on Gellman's conversations with Snowden and a few key NSA folks who interacted with Snowden. What is salient in Snowden's history is the way in which the interests of agency personnel facilitated his hacker tendencies and philosophy. This facilitation not only gave him access to and knowledge of the *uses* of the technology by the IC but also the ability to exfiltrate the information about the knowing abuse of the various surveillance collection programs and tools.

The final section is on oversight - of the executive branch by the executive branch, and to less extent by the Foreign Intelligence Surveillance Act (FISA) Court and to an even lesser extent by Congress. Some discussion of how the executive branch worked the legislative and judicial branches to accomplish its goals is included. Gellman presents a top-level presentation of the legal arguments made in an "offensive defense" (my term) of the practices of the IC.

As I looked back through Gellman's book, I realized (yet again) how much misdirection and obfuscation (the kindest word) the executive branch engaged in, how often the FISA Court was - and allowed itself to be - misled. Congress gets fairly cursory attention in Gellman's book, so this review does not go into depth. The last section also addresses the executive branch's thoughts and action on the assignment of accountability and to whom it should apply. Oversight with no follow-through, no accountability, is from a democratic point-of-view, likely (I suspect essentially) a game played behind perpetually closed doors.

The first section on technology addresses the "new revelations." The contemporaneous reporting by Gellman and others are presumed by Gellman to have been read and remembered. I had many "Oh, yeah..." moments when piecing together this segment of the review. The presentation by Gellman of the technology timeline assumes that the reader has a detailed understanding of when, why, and how various programs and tools were developed and launched. The tool that was, for me, a truly "new revelation" is MAINWAY, to which Gellman devotes much discussion. Interested readers can find a timeline of the technology on Electrospaces.net.

I tried to impose some order on this part of the story, aided by contemporaneous writings by additional journalists and experts. I include links to other sources that go into more depth on the arguments and logic of executive branch personnel in the NSA and the DOJ for those readers who may want to delve more fully.

Some readers might question why some of the discussion below is included here and not in the Oversight section. It is, I believe, necessary to understand the approach to national security of Cheney, Addington, and Bush. It is also necessary to understand the general supineness of the FISA Court in matters of use of surveillance technology on U.S. Persons. The Intelligence Community was willing - and more than ready.

## The Technology

Under orders from President George W. Bush, without judicial or legislative authority, the NSA spied on Americans in ways that Congress had expressly forbidden since 1978: tracking telephone calls made and received by Americans on U.S. soil. As exposed by *New York Times* reporters James Risen and Eric Lichtblau (2005), the domestic surveillance was conceived and overseen after the September 11 attacks by Vice President Cheney and his general counsel, David Addington. Under their auspices, the NSA and FBI began wide-ranging surveillance of Internet and telephone communications within the United States (Gellman 2020a, 70).

According to Gellman (2020a, 168) the three cover names “STARBURST,” “WHIPGENIE,” and “STELLARWIND” referred to different stages of one evolving set of operations, carried out between 2001 and 2007. The collection programs were protected as "Exceptionally Compartmented Information," the most restricted category of classification. Gellman (2020a, 170) says that they were later reflagged as STELLARWIND.

What became MAINWAY (which plays a major role later in the story) was a component of THINTHREAD**,** an intelligence-gathering prototype, developed by William Binney and others at the NSA and tested throughout the 1990s. This program involved wiretapping and sophisticated analysis of the resulting data and claimed to protect the privacy of U.S. citizens (Gellman 2020a, 175-176). THINTHREAD was discontinued on the authority of the NSA director General Michael V. Hayden three weeks before the September 11, 2001 attacks due to the "changes in priorities" and the consolidation of U.S. intelligence. Vice President Cheney's office drafted orders, signed by President Bush, to do something the NSA had never done before. The assignment, forbidden by statute, was to track telephone calls made and received by Americans on American soil (Gellman 2020a, 168).

When subordinates told him "in alarm" that his software, THINTHREAD was being adapted to analyze *domestic* calls, William Binney quit the NSA in October 2001. Gellman (2020a, 175-176) says that when he showed Binney the network diagram of American call data records being funneled to MAINWAY, Binney did a double take: "That's a name I've never spoken of. That's the program they used for STELLARWIND to reconstruct social networks" (Gellman 2020a, 175).

Gellman notes that while NSA knew how to do such tracking with foreign calls, it did not have the machinery to do it at home. As Gellman (2020, 168-169) puts it, STELLARWIND defined the operation, MAINWAY was a tool the carry it out. Gellman (2020a, 169) reports that when Hayden received the execution order on October 3, 2001 for "the vice president's special program," NSA engineers "assembled a system from bare metal and borrowed code within a matter of days." We don't know from where the code was "borrowed."

Eventually in 2004, the Justice Department ruled that some operations were illegal. This about-face for the DOJ is well-explained by Julian Sanchez (2013). In essence, Acting Attorney General James B. Comey refused to certify that the operations were lawful. Comey's May 2007 testimony before the Senate Judiciary Committee about the firings of U.S. attorneys and the alleged politicization of the Justice Department was made public in *Salon* (Salon Staff 2007).

The rebellion in the Justice Department, not just with Comey against unlawful orders, forced Bush to seek authority for the warrantless programs from the FISA Court, and eventually from Congress. Bush briefly "discontinued" the bulk Internet metadata collection involving Americans.

In 2005, James Risen and Eric Lichtblau (2005) at *The New York Times* reported that

> Under a presidential order signed in 2002, the intelligence agency has *monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years* in an effort to track possible "dirty numbers" linked to Al Qaeda, the officials said. The agency, they said, *still seeks warrants to monitor entirely domestic communications*." (emphasis added)

Gellman (2020a, 123) notes that the domestic surveillance aspired to cover substantially all Americans, collecting hundreds of billions of telephone *and Internet records*, in the hope of discovering unknown conspirators (e.g., not known terrorists, emphasis added).

In 2007, Justice Department lawyers persuaded the FISA Court that it could authorize surveillance of an unlimited number of accounts with a single order. Under the decision and classified as "sensitive compartmented information," a FISA Court judge no longer needed to hear a valid foreign intelligence purpose for surveillance of each proposed target. Neither the Court nor the intelligence committees in Congress knew who the targets were. Once a year in a classified proceeding, the FISA Court approved two documents. The first laid out rules meant to govern the NSA's choice of accounts to monitor; the second specified procedures for "minimizing" or limiting (Gellman 2020a, 111).

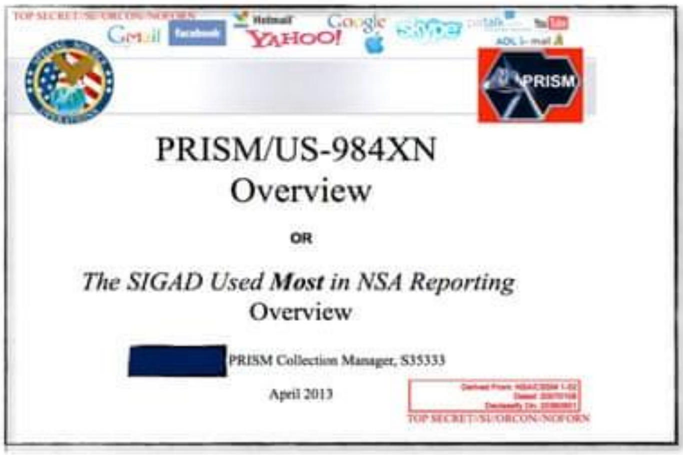
The Foreign Intelligence Surveillance Act of 1978 (FISA) Section 702 did not apply to collection abroad unless it *deliberately* targeted an American using *equipment based inside the United States*. There were other rules and regulations, however, based on Executive Order 12333 signed by President Ronald Reagan. The standards set in that executive order were more permissive, implemented in classified regulations, and rarely subject to oversight outside the executive branch.

The NSA was allowed under EO 12333 to keep "incidentally obtained information" about Americans as long as it did not target them deliberately for surveillance - and keep, it did. "Incidentally" was a specialized legal term; the NSA caught U.S. persons in nets that it cast with some other lawful purpose in mind. The NSA could, and did, tap into high-volume circuits overseas gathering data "in bulk" without discriminants. Collection remained incidental even when the NSA knew for certain that Americans would be swept in (Gellman 2020a, 286 - 287). Once in hand, the American communications could be searched and analyzed along with the foreign stuff. With U.S. identities *sometimes* masked says Gellman (2020a, 287), the information could be shared with other agencies.

### ***PRISM***

Under PRISM, NSA collects *stored Internet communications from various U.S. Internet companies* ("NSA Slides" 2013); the NSA had compulsory access to any information that Google possessed about a foreign intelligence target. Gellman notes the program allows the NSA to target communications that were encrypted as they traveled across the Internet backbone to focus on stored data, which telecommunication filtering systems discarded earlier, and to get data that is easier to handle. Under Section 702 of the FISA Amendments Act of 2008, the NSA made demands to Internet companies such as Google LLC to turn over any data that match court-approved search terms (Gellman 2020a, 283).

The PRISM slide presentation cover page dated April 2013 is an American eagle as predator with the whole world its prey (Gellman and Poitras 2013). As Gellman (2020a, 110) notes it was *the sigil of an agency that could not even conceive of a public readership* (emphasis added).


Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk
YouTube
AOL mail
PRISM

TOP SECRET//SI//ORCON//NOFORN

PRISM/US-984XN
Overview

OR

*The SIGAD Used **Most** in NSA Reporting*
Overview

[redacted] PRISM Collection Manager, S35333

April 2013

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360901

TOP SECRET//SI//ORCON//NOFORN

On the slide "PRISM Collection Manager S35333," Gellman explains S stands for Signals Intelligence Directorate, S3 for Data Acquisition, and each digit after identifies a subordinate function. S353, the "eagle people" as Special Source Operations "pulled in monumental flows of information from the main trunk lines and switches that carry voice and data around the world" (Gellman 2020a, 110). The owners of that infrastructure, mostly big corporations, were the "special sources." The NSA "paid them off, rerouted their traffic surreptitiously, hacked into their equipment, or relied on foreign allies with methods of their own" (Gellman 2020a, 110). The companies were compensated for their trouble from a classified budget for "corporate partners" that reached $394 million in fiscal year 2011;  "when the NSA cannot negotiate access, it helps itself" (Gellman 2020a, 199).

The special sources were also the American-based Internet giants: Google, Facebook, Yahoo, Microsoft, AOL, Skype, Apple and aa service called Paltalk. Unlike AT&T and other common carriers, they did not only "push data through pipes" but rather, *stored the content their users sent and received*. As Gellman (2020a, 111) put it, "the NSA did not have to chase down all those emails, videos, photographs, and documents as they raced across fiber optic cables at the speed of light; collection could wait until the data arrived somewhere and held still."  (Or, as Gellman notes, as often happened when faced with alternatives, the NSA could choose to do both).

Gellman and his research assistant Ashkan Soltani also discovered that the NSA was standing at "major intersections of the Internet" and pulling in anything that looked like an electronic address book, email contacts and instant messaging "buddy lists." As Gellman (2020a) notes,

> Address books often included more than metadata: nicknames, labels, and notes fields. Sometimes the contacts were listed in email accounts with the first few lines of their most recent messages. Taken together, the data would enable the NSA to draw detailed maps of a person's

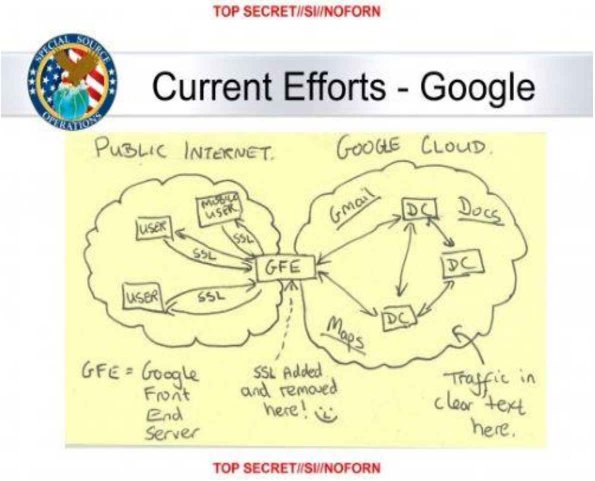
> life, as told by personal, professional, political, and religious connections. (315-316)

The NSA had no authority *from Congress or the FISA Court* to collect contact lists in bulk. High-ranking officials acknowledged that the operation would be illegal from facilities in the United States. As noted previously, EO 12333 gave legal cover to a multitude of intrusions, including the ones that happened overseas but touched Americans at home. According to Gellman (2020a, 317), one official stated that because of the method employed, the Agency was not legally required - and had no technical capacity - to restrict its intake to contact lists belonging to specified foreign intelligence targets; when information passed through "the overseas collection apparatus the assumption is you're not a U.S. person."

The result was a high volume of phone-mapping information that was "outpacing our ability to ingest, process and store" data. However, Gellman (2020a, 317) notes, "the NSA did not see being more selective as a cure it was willing to adopt."

Gellman (2020a, 314) reports that early in the debate Snowden provoked, Keith Alexander defended bulk collection as an essential counterterrorism and foreign intelligence tool: "You need the haystack to find the needle." At that point, it appeared that the haystack comprised domestic telephone records, which as Gellman points out, applied to metadata alone. *"Not to know everything, but to be capable of knowing* *anything. Any refuge against surveillance, any zone of effective privacy, had to be neutralized”* (Gellman 2020a, 314; emphasis added).

Under PRISM, the NSA already had compulsory access to any information that Google possessed about a foreign intelligence target. However, according to the NSA slide below (Gellman and Soltani, 2013), the NSA was inside the Google cloud. Google, at the point of Gellman sharing this slide with a Google engineer, only protected its data traffic with encryption outside its digital property line (Gellman 2020a, 283, 285). The Google engineer “erupted in anger” about the note at bottom center “SSL Added and Removed ☺” (Gellman 2020a, 281, 283). Every expectation of privacy on the Internet, every secure transaction, depended on SSL. If the encryption was broken in some fundamental way, says Gellman, we were living in a different world that we had been led to believe (Gellman 2020a, 281).



TOP SECRET//SI//NOFORN

Current Efforts - Google

TOP SECRET//SI//NOFORN

PUBLIC INTERNET.
GOOGLE CLOUD.
USER
MOBILE USER
SSL
SSL
USER
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

Google's and other providers' data traveled overseas even if you never left the country yourself (Gellman 2020a, 286). It was possible for the NSA to collect everything on everyone inside the Google Cloud. Through "the overseas collection apparatus" the "assumption is you're not a U.S. person" (Gellman 2020a, 317).

### ***Contact Chaining***

Under Presidents Bush and Obama, the Justice Department lawyers secretly persuaded the FISA Court that *every record of every call* met the relevance test because a terrorist plot might involve a party or parties unknown. The NSA proposed to find those ghosts by way of "contact chaining," a mathematical analysis of links among friends, friends of friends, and so on (Gellman 2020a, 143, 158). Gellman notes that the computational methods had implications beyond the competence of the court to assess; but "what the court knew, and chose to authorize, was that the NSA wanted access to the whole universe of domestic *telephone calls*" (Gellman 2020a, 144, emphasis added).

Working through the FBI, Gellman (2020a, 158) reports that the NSA assembled a five-year inventory of phone calls from every account it could touch that counted up to be "trillions of calls. Nobody needed to plumb that ocean to find the numbers on a bad guy's telephone bill." As Gellman puts it, the NSA was not plumbing. It was contact chaining, a sophisticated form of analysis that tried to find hidden, indirect relationships in very large data sets. Contact chaining begins with a target telephone number, such as the calls and contacts of Dzhokhar Tsarnaev (the example NSA used to justify the use of this practice), progressively widening the lens to ask whom Tsarnaev's contacts were talking to, and whom those people were talking to, and so on. Each step in the process is called a "hop."

### Metadata and "Embedded Patterns"

Ed Felten pointed out the implications of "embedded patterns" ("social graphs" in IC parlance) in any voluminous data set ; intimate secrets can be pulled from very large collections of very small clues.[2] Gellman explains that "individual pieces of data that previously carried less potential to expose private information may now, in the aggregate, reveal sensitive details about our everyday lives." Further,

> With access to the call records, Big Data methods could extract the "membership, donors, political supporters, [and] confidential sources" of human rights or protest groups. Cash donations sent by text message, an increasingly popular channel, identified contributors to political parties and religious institutions. Data mining could reliably pick out sexual orientation. It could track the telephonic fingerprints of secret love affairs as they blossomed, peaked, and died. It could distinguish bosses from employees, in part because bosses get their calls returned faster and have fewer qualms about phoning subordinates at night. (quoted in Gellman 2020a, 162)

[2] Robert E. Kahn, Professor of Computer Science and Public Affairs, who served for a time as deputy chief technology officer of the United States and with whom Gellman had a visiting fellowship while working on this book.

An example Felten (2013, 18) gave in a declaration in support of an American Civil Liberties Union lawsuit against the NSA is particularly compelling in the current political and social atmosphere:

> When you factored in time and sequences, the results were startling. "A likely storyline emerges when a young woman calls her gynecologist; then immediately calls her mother; then a man who, during the past few months, she had repeatedly spoken to on the telephone after 11 pm; followed by a call to a family planning center that also offers abortions." The government may seldom care, may never abuse that knowledge in a given year. But now, for the first time in history, it had acquired the power to do so.

In the aftermath of news stories developed in part from the Snowden archive, Stewart Baker, a former general counsel of the NSA, and Michael Hayden, weighed in about the power of the social graph:

> Baker - "Metadata absolutely tells you everything about somebody's life." For purposes of signals intelligence, "if you have enough metadata, you don't really need content."
>
> Hayden - "*We kill people based on metadata. But that's not what we do with this metadata.*" (Gellman 2020a, 162; emphasis added)

### ***MAINWAY***

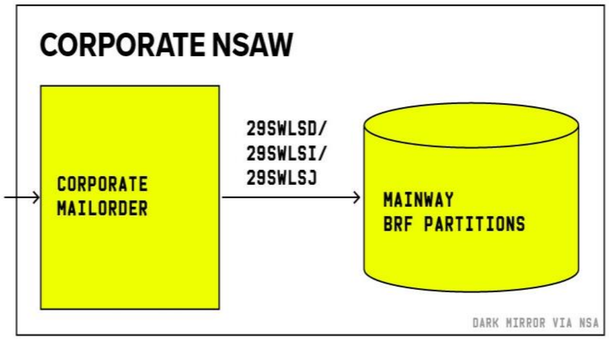
As Gellman notes, no one could predict the name or telephone number of the next Tsarnaev. From a data scientist's point of view, the logical remedy was clear. If anyone could become an intelligence target, MAINWAY should try to get a head start on everyone. And so the IC and the FBI did.

MAINWAY or, according to the classified NSA *SSO Dictionary*, "the MAINWAY *Precomputed* Contact Chaining Service" is an analytic tool for contact chaining (emphasis added).  “Precomputed” turned Gellman's (2020a, 171-172) understanding of the call records program upside down. Contact chaining on a scale as grand as a whole nation’s phone records was a prodigious computational task, even for MAINWAY.

MAINWAY, Gellman says, became the NSA’s most important tool for mapping social networks - an anchor of what the agency called Large Access Exploitation. “'Large,' Gellman (2020a, 170) notes, is not an adjective in casual use at Fort Meade; MAINWAY was built for operations at stupendous scale.” Other systems parsed *the contents* of intercepted communications: voice, video, email and chat text, attachments, pager messages, and so on. MAINWAY was queen of metadata - foreign and domestic - designed to find patterns that content did not reveal. Patterns gleaned from call records would *identify targets in email or location databases, and vice versa*. Metadata, notes Gellman (2020a, 171), was the key to the NSA’s plan to “identify, track, store, manipulate and update relationships” across *all forms of intercepted content* (emphasis added). An integrated map, presented graphically, would eventually allow the NSA to display nearly anyone’s movements and communications on a global scale.

The crucial discovery on this subject turned up at the bottom right corner of a large network diagram prepared in 2012 (Gellman 2020b, 170-172). A little box in that corner, reproduced below, finally answered his question about where the NSA stashed the telephone records that Blair and

Gellman talked about. *The records lived in MAINWAY*. The implications were startling.



The diagram as a whole traced a "metadata flow sourced from billing records" at AT&T as they wended through a maze of intermediate stops along the way to Fort Meade (Gellman 2020a, 171, 395). MAILORDER the next to last stop, was an electronic traffic cop, a file sorting and forwarding system. The ultimate destination was MAINWAY. *The "BRF Partitions" in the network diagram were named for Business Records FISA orders, among them a dozen signed in 2009 that poured the logs of hundreds of billions of phone calls into MAINWAY* (Gellman 2020a, 171).

According to Gellman (2020a, 173), the FBI brought the NSA more than a billion new records a day from the telephone companies. MAINWAY purged another billion a day to comply with the FISA Court's five-year limit on retention. Every change cascaded through the social graph, redrawing the map and obliging MAINWAY to update ceaselessly.

Bill Binney confirmed to Gellman (2020a, 176) that the techniques he devised prior to 2001 did not confine themselves to individual targets. They computed social graphs for every caller in the gargantuan data set. Social graphing for every caller called for "mapping dots and clusters of calls as dense as a star field, each linked to others by webs of intricate lines" MAINWAY's analytic engine traced hidden paths across the map, looking for relationships that human analysts could not detect (Gellman 2020a, 173).

"You have to establish all those relationships, tag them, so that when you do launch the query you can quickly get them," Rick Ledgett, the former NSA deputy director told Gellman (2020a, 173). With ceaseless purging and updating of the map, Gellman wondered how those relationships could be tagged and retrieved.  He realized that was where *precomputation* came in. Network theory called this map a social graph: it modeled the relationships and groups that defined each person's interaction with the world. Gellman (2020a, 158) notes that the NSA's analysis touched nearly all Americans because the size of the graph grew exponentially as contact chaining progressed. The whole point of chaining was to push outward from a target's immediate contacts to the contacts of contacts, then contacts of contacts of contacts.

Sophisticated software tools mapped the call records as "nodes" and "edges" on a grid so large that the human mind, unaided, could not encompass it. Nodes were dots on the map, each representing a telephone number. Edges were lines drawn between the nodes, each representing a call. A related tool called MapReduce condensed the trillions of data points into summary form that a human analyst could grasp Gellman (2020a, 158).

Constant, complex, and demanding operations fed another database called the Graph-in-Memory. When the Boston bombs exploded, the Graph-in-Memory was ready.  Gellman (2020a, 173) notes that absent unlucky data gaps, it already held a *summary map of the contacts revealed by the Tsarnaev brothers' calls. The underlying details - dates, times, durations, busy signals, missed calls, and "call waiting events" - were easily retrieved on demand. MAINWAY "precomputed" them*.

If MAINWAY had your phone records, it also held a rough and ready diagram of your business and personal life. Moreover, as noted above, the NSA planned to use metadata to "identify, track, store, manipulate and update relationships" across *all forms of intercepted content* (Gellman 2020a, 170, emphasis added).  The social graph and Graph-in-Memory were not built just from call records; they allowed the NSA to display nearly anyone's movements and communications on a global scale (Gellman 2020a, 171).

All kinds of secrets - social, medical, political, professional - were precomputed, 24/7. And the government can look back as MAINWAY and the Graph-in-Memory *keep copies of every map they draw* (Gellman 2020, 174, 179; emphasis added).

## Snowden

> Not just anyone could do it, but it doesn't take super villain levels of capability to make it happen. All it would take is paying attention to how the system works, which is your job (Snowden, quoted in Gellman 2020a, 31).

The truth, Gellman (2020a, 40) says, is the story of a young man who fell short in class, refused to conform, gave no serious thought to a university degree, burned a lot of time in game arcades, and never had to pay the dues that (some of) his seniors did before ascending to six-figure salaries.  And yet, he says, it is also the story of a self-taught polymath, determined to apply his talents on his own terms, who repeatedly found his way around conventional barriers:

> He had a knack for breaking down problems, unpacking the parts, discerning how the innards worked, and shaping them to his will. He had an eye for hidden openings. It was a hacker's frame of mind, in the classic sense, applicable as much to daily life as to machines. Disregard the "normie" path. *Find a side window* if the front door is locked, skip needless steps, follow instructions out of sequence if that speeds results. *Automate a tedious task or substitute a more efficient one. Rewrite or repurpose any product, any process, if you can turn it to your own ends.* Share the recipe. (emphasis added)

In Snowden's 14 months in Hawaii [see Kunia below], he embarked on a private version of that exercise.

A full timeline for Snowden can be found in PopularTimelines (n.d.). It is a helpful reference for reading the book as Gellman almost never provides dates in his discussion of Snowden's employment and career path, and Gellman's discussion does not follow a linear path. I used it to help organize the discussion that follows.

Unless noted otherwise, I presume that most, if not all, of the descriptions of Snowden's activities come from discussions between Gellman and Snowden.

### *Side Windows*

Throughout his teens (and continuously thereafter), Snowden participated in online hacker and gaming forums. In the early 2000s, he learned something that led to his first "career hack":

> ...certified engineering skills were an easy shortcut through employment screening in the Washington area's booming tech sector. Computer skills were in high demand, and human resources departments did not know how to judge prospective hires. A Microsoft certification had become a standard proxy. Gellman (2020a, 41)

In February 2002, Snowden registered for an expensive private course in Windows system engineering. The Computer Career Institute at Johns Hopkins, a for-profit entity, "took his money without requiring proof of relevant work experience, previous training, or even the high school diploma that was still a month away" (Gellman 2020a, 41). At nineteen, with the barest minimum of coursework, he became a Microsoft- certified systems engineer (MCSE).

Gellman shares Snowden’s stories about his gaming exploits and obsessions and notes that in 2003, just after turning twenty, Snowden began digging into privacy tools called anonymous proxies which disguise the origin or destination of an Internet link. One of the other participants in the *ars Technica* discussions told Snowden, “unless this is for troubleshooting or a prank, it sounds like it might be illicit activity.” Another asked Snowden “what the hell [are] you so paranoid about here?” Snowden responded curtly, “Patriot Act”; He notes that much the same approach (use of anonymous proxies) “carried out with greater sophistication, guided him decades later as he passed classified information to me and other journalists” (Gellman 2020a, 45).

In 2004, in the post-9/11 climate, Snowden decided to enlist. After incurring leg fractures in his basic training, he accepted an administrative discharge that same year. In September, Snowden returned to Ellicott City, enrolled in community college and in 2005, accepted a job offer from the University of Maryland as a security guard at the Center for Advanced Study of Language or CASL (Gellman 2020a, 48).

The facility included classified spaces for secret NSA research so Snowden needed a TS/SCI clearance and a clean polygraph. The clearance came through alongside a July 7 letter from Q223, the NSA’s counterintelligence awareness office. “Dear Contractor Staff Security

Officer," it said. "This form is for your records to verify that the person stated below has been indoctrinated in counterintelligence" (Gellman 2020a, 48).

The clearance was presumably based, at least in part, on Snowden's Microsoft-certified systems engineer credential. As Gellman (2020a, 47-48) reports, the clearance ushered Snowden into the national security establishment. He was eligible now to apply for thousands of classified jobs in the Washington area alone.

During overnight shifts as CASL, he and his partner plugged a laptop into an Ethernet port in the lobby. The default settings for the network offered no connection to the laptop as it was an unknown machine. Snowden pulled up a command line & pinged the router, fiddled with the host control settings, and assigned himself an IP address on the subnet. Members of the IT staff offered him a job when they learned how he had managed to bypass network controls (Gellman 2020a, 48-49). The position, however, required a college degree which Snowden did not have. One man on the IT staff suggested that he go to the job fairs for security-cleared personnel because some of those companies don't care about degrees*.*

Snowden did so - and was offered a job on the spot by a small contractor *and his client would be the CIA*. As Gellman (2020a, 49) puts it, "Snowden stumbled onto the career hack that enabled all the rest.

The Microsoft certificate, the clearance, and a satisfactory interview were all he needed." All without a security clearance.

In March 2007, the CIA stationed Snowden with diplomatic cover in Geneva, Switzerland, where he was responsible for maintaining computer-network security. He received a diplomatic passport. In February 2009, Snowden resigned from the CIA (Gellman 2020a, 54). But the CIA never revoked his clearance credentials at this point or later.

In 2009, Snowden began work as a contractee for Dell, which manages computer systems for multiple government agencies. He worked for Dell for four years. Assigned to an NSA facility at Yokota Air Base near Tokyo, Snowden instructed top officials and military officers on how to defend their networks from Chinese hackers. As was his wont, Snowden automated the larger part of his routine work in Japan. Gellman (2020a, 58) notes that in the free time that automation created, he returned to his time in Geneva, from where Snowden had watched as Serbian protesters set fire to the U.S. embassy in Belgrade. Damage to the CIA station there led to discussion in the Geneva station as to whether important intelligence materials had been destroyed. Snowden began to think about where, if anywhere, the Belgrade station preserved real-time copies of its files? How would a well-designed backup system efficiently transmit and store data? In his free time he began work on a side project which he called EPICSHELTER (Gellman 2020a, 59):

> Some of the features he contemplated were available in the commercial world, but they were not easy to reproduce across interlocking classified networks. "De-duplication" would save storage space by backing up each file only once, even if there were multiple copies on the source networks. *"Block level" updates would save bandwidth by synchronizing only new bits and bytes when a source file changed, rather than sending a new copy of the whole file*. (emphasis added)

According to Gellman (2020a, 60), in late 2009 or early 2010, Snowden briefed Lonny Anderson, NSA's chief technical officer, when Anderson passed through Yokota. That meeting brought an invitation to Fort Meade, and the NSA's Technical Directorate took ownership of EPICSHELTER. When a proof-of-concept budget came through, the NSA chose Hawaii as the pilot site.

Snowden continued to accrue credentials. One, the EC-Council's certified ethical hacker, he completed his eligibility for Level III access under DoD Directive 8570 to the innermost security level (the "Enclave) of DoD networks.

In 2010, Dell offered him a transfer home and a return to the CIA in a much more substantial role. In 2011, he returned to Maryland, where he spent a year as lead technologist on Dell's CIA account (Gellman 2020a, 61). In March 2012, Dell reassigned Snowden to Hawaii as a concession to Snowden's health. A series of small blackouts over several months preceded a serious epileptic seizure in the middle of a phone call with his boss at Dell. Dell offered him a sleepy billet in HT322—Hawaii Technical Directorate, Office of Information Sharing

(Gellman 2020a, 35). Snowden reported for duty at the Kunia Regional Security Operations Center. His job was to configure and maintain classified network servers, enforcing access restrictions on each account. Within weeks, Snowden automated most of the job, writing scripts for maintenance and other routine tasks that his predecessor had performed by hand (Gellman (2020a, 35).

Snowden's NSA manager, a career civilian employee, assigned him to help out in "busier precincts" of the Windows network division. As Gellman (2020a, 36) points out, off-the-books arrangements of that sort were commonplace in the NSA, which deployed its people where needed and could not realistically seek a contract amendment for each new task. And Snowden's supervisors did not intend to waste his already-noted skills as a Microsoft-certified systems engineer with real-world network management experience.

"I was also helping out the Linux team," Snowden told Gellman, referring to a rival operating system used widely in networking; "so you know, I had Linux boxes, Linux credentials, virtual servers, all that stuff. *So basically, I had the keys to everything. I had the keys to all the data sharing. I had access to all the servers* (Gellman 2020a, 36; emphasis added).

The NSA's access control system specified fine-grained clearances and permissions in a digital certificate for every authorized user. The certificate was known in shorthand as the PKI, for public key infrastructure. At the NSA, the certificates were stored in each user's computer network profile (Gellman 2020a, 67). According to Gellman, the credentials in Snowden's PKI were close to the worst-case scenario for the NSA's internal defenses. The risk he posed was a nightmare of acronyms TS//SI//G//TK//HCS:

> ...Top Secret clearance, ... "Special intelligence," the control system for compartmented information about surveillance sources and methods, was the bread and butter of Kunia's mission. Not all of Snowden's colleagues held the third credential, short for Gamma, which opened the door to the contents of intercepted communications. The fourth credential may also have been less common. Talent Keyhole covered secrets about spy satellites and other overhead collection systems. Rarest at the NSA was Snowden's clearance for HCS, the HUMINT Control System. ... HUMINT meant "human intelligence," the clandestine work of U.S. case officers. That one came as a legacy of Snowden's time at the CIA, which did not revoke his credentials upon departure. (Gellman 2020a, 67)

On top of this, Gellman (2020a, 67) notes, came the privileged access of a top-tier system administrator where Snowden could *disable, edit, or erase some of the activity logs that would otherwise leave evidence of his digital movements. He could move or copy files and override restrictions on the use of external storage devices such as thumb drives* (emphasis added).

Before Snowden could be "read into" any given compartment and examine the files inside, proper authorities had to certify his need to know. His final job in Hawaii, for example, cleared him to read files marked BYZANTINEHADES and SEEDSPHERE, which were concerned with Chinese government hacking (Gellman 2020a, 68).

That, at any rate, was how the limits were supposed to work. As Gellman (2020a, 68) notes, Snowden, by lifelong habit, looked for side channels. He borrowed a classic method of misdirection: *his official duties, openly performed, provided "cover for presence" and "cover for action" in digital neighborhoods where he might attract suspicion*.

An old NSA maxim, one analyst told Gellman (2020a, 66), is that "*there is no access fairy"; no one magically intuits what data you want & intercepts it on your behalf. The lesson for newbies, the analyst said, is supposed to be that "you have to cultivate your own collection, not rely on other people to get it for you without being asked*" (emphasis added).

Early on, Snowden repurposed a routine security audit that performed in the Windows engineering division - to find misfiled secrets, e.g., restricted information that had migrated somehow to less restricted locations on the network. He was supposed to delete those files, but... Once Snowden took possession, according to Gellman (2020a, 68), the NSA's chief technical officer, Lonny Anderson, "...used his sys admin privileges to exfiltrate. He would move the data as part of the sys admin job to a place that he was comfortable, 'Here I can exfil the data.'"

Snowden also ran “dirty word searches” - a search that was supposed to come up empty if everyone followed security protocols. But, as Gellman (2020a, 68) points out, the NSA’s digital machinery is operated by humans who make mistakes and also take shortcuts when the approved procedures get too much in the way of their jobs.

In one case, a group of analysts who curated and shared their working copies of files drawn from a large, restricted database of raw intelligence wanted to collaborate and avoid redundant work. Each of them had authority to read the material, *but the files did not belong in the system they used for sharing*. Snowden found and copied them and told Gellman (2020a, 69) later that he did so in order to show the way in which many innocent people are swept into the NSA’s net.

Snowden told Gellman (2020a, 69) that he looked for files marked “ECI,” or exceptionally controlled information. Nothing classified at that level belonged on the network servers. Information that sensitive was supposed to be stored in a cipher-locked room on a system that required special access credentials. Similar restrictions applied to files labeled “FISA” or “FAA 702,” a reference to communications intercepted within the United States under authority of the FISA Amendments Act, Section 702.

Snowden’s dirty word searches improved when he turned up a list of cover names for ECI compartments. He was not cleared to look inside the compartments, but his credentials, his PKI certificate, allowed him to see what those compartments were called (Gellman 2020a, 69). One day, such a search produced hits on "STARBURST,""WHIPGENIE," and "STELLARWIND" (Gellman 2020a, 70). Snowden's reaction to this discovery is covered in the Oversight section of this review.

NSA's Anderson told Gellman (2020a, 69) that in general, Snowden was authorized for reports and presentations, "not access to what we would call data, so he's not going into repositories and getting access to raw data." Gellman points out that this description was true, officially, at Kunia though not in his final position: "It was a poor description of what he could reach in practice."

By April 2012, ejsnowd had joined the short list of "super users" in Kunia's Windows Server Engineering Division. *He could override the restrictions on ordinary user accounts, see further and deeper into the network, and make changes to its fundamental workings*. Snowden, according to Gellman (2020a, 36), reached the top tier called PRIVAC, for "Privileged Access." Inside the Tunnel, he had the run of every Windows machine with an IP address.

Snowden contemporaneously created a new project he called Heartbeat, coded from scratch in plain sight of his colleagues (Gellman 2020a, 72). Anyone at Kunia could follow his progress on an intranet page that listed his name and system identifier, ejsnowd, as the point of contact.

At the top of the page, titled “The NSA Heartbeat,” Snowden placed a logo of his own design.

Even if this were just another side project, like EPICSHELTER, Snowden now had a legitimate reason to automate the transfer of thousands, then hundreds of thousands of files, and then more. That is far from saying he took away copies of all those files for himself, notes Gellman (2020a, 73).

Heartbeat was, as Gellman notes, an enormous undertaking. Kunia had no budget for it. Snowden’s employer had no contract to perform the work. “This was a self-generated idea,” Richard Ledgett, the former deputy director, told Gellman (2020a, 74); “it was not something ‘Big NSA’ thought was needed, so his local managers had some latitude. ‘Sure, that sounds like a good idea.’” Snowden’s boss allowed him to give it a try. The NSA was paying Dell, and Dell was paying Snowden to do a different job. In reality, Heartbeat began to swallow the bulk of his time, but, as one of Snowden’s coworkers later told *Forbes*, “If you had a guy who could do things nobody else could, and the only problem was that his badge was green instead of blue, what would you do?” (Gellman 2020a, 75).

One “thing” was a one-stop portal for intelligence that spanned multiple sources. Within their assigned roles and specialties, Kunia workers might draw upon records maintained by the CIA, the FBI, the State Department’s Bureau of Intelligence and Research, or any of the other thirteen branches of the U.S. Intelligence Community. The networks crossed the turf lines of rival agencies each of which used different software, data formats, and access protocols. Each had its own intricate set of security controls. Heartbeat, if it worked correctly would have to reproduce these exactly (Gellman 2020a, 74).

Some of Heartbeat's early evaluators asked whether Snowden could retrieve new files on remote systems that did not list them automatically. The idea on the table was to create "an always-up-to-date mirror of all the latest content from all the different internal sites and networks*." In order to accomplish that, Heartbeat would have to create and update its own index of systems that belonged to other agencies* (Gellman 2020a, 76; emphasis added). Each time the index showed something new, Heartbeat would import a copy. Gellman (2020a, 76) notes that, while self-updating indexes are commonplace in the civilian world, it was an audacious idea to do anything of this sort on somebody else's TS/SCI network.

Among other impediments, the plan required credentials that Snowden did not possess (Gellman 2020a, 76). Every day - or every hour, or many times an hour - Heartbeat knocked on a long line of doors through which it could not enter without an invitation, or a PKI digital identity certificate. As a prototype with no official status, Heartbeat was not eligible for its own PKI and the system itself could not be added to the guest list. Instead, Snowden embedded his certificate into Heartbeat's Digital Identity Store. Some doors would not open for his digital identity and some doors led to places that only a government employee (not a contractor) could go.  Snowden asked his supervisor if he would add his digital identity to Heartbeat alongside Snowden's. The supervisor agreed after, according to Snowden, consulting "multiple levels of NSA and corporate management," including the information systems security manager for all of Hawaii. Nobody objected, by Snowden's account, but nobody put permission in writing; *projects built with a nod and a wink do not rate formal exceptions to security policy* (Gellman 2020a, 77; emphasis added).

Gellman (2020a, 71) notes that Snowden appears to have made some of his most consequential finds by taking advantage of an efficiency feature in the NSA's configuration of user accounts. You could sign on to any NSA workstation in the world and your "active directory profile" - working files and folders, browser settings, identity certificates - would appear, same as always. For visitors to Kunia, however, remote access to other NSA offices, such as Fort Meade, could be balky and slow. The system was designed to *copy* the visitor's profile to a temporary local cache. *The consequence was this: each time a VIP arrived at Kunia, memos and spreadsheets and slide decks poured into a folder under Snowden's administrative control* (Gellman 2020a 72; emphasis added).

At the time, Joseph J. Brand, NSA's Associate Director for Community Integration, Policy, and Records, unknowingly contributed one collection. Based on Gellman's (2020a, 71-72) analysis of the metadata, *Brand's temporary folder supplied Snowden with the STELLARWIND report*.

By April 2012, ejsnowd had joined the short list of "super users" in Kunia's Windows Server Engineering Division; h*e could override the restrictions on ordinary user accounts, see further and deeper into the network, and make changes to its fundamental workings* (Gellman 2020a, 36). Snowden had reached the top tier, called PRIVAC, for "Privileged Access." Inside the Tunnel, he had the run of every Windows machine with an IP address.

In 2013, Snowden turned down a job with NSA's Tailored Access Operations unit (TAO) which would have shifted him from Dell back to U.S. government employ. He had his eye, Gellman (2020a, 83) reports, on a contract at Booz Allen Hamilton which supplied "infrastructure analysts" to the NSA Threat Operations Center. Snowden became one of them, transferring out of the Kunia Tunnel to a big open-plan workspace in the Rochefort building nearby.

Snowden's position at the Threat Operations Center granted him what the NSA calls "dual authorities," a set of combined credentials that few other jobs required (Gellman 2020a, 84). At the time, the Agency encompassed two principal directorates, Information Assurance and Signals Intelligence. The first defended U.S. government secrets. The other stole foreign secrets. Each had its own arsenal of classified legal powers, and each had its own limits. Defenders could look inside (some) U.S. communications networks for evidence of foreign intrusion. *Attackers could spy overseas under the president's Executive Order 12333 and use domestically based collection from PRISM and Upstream* (Gellman 2020a, 84; emphasis added).

In April 2013, the NSA flew Snowden to its Fort Meade headquarters to meet with the NTOC (National Threat Operations Center) chain of command and compare notes with Maryland-based colleagues on the China beat. Gellman reports (2020a, 84-85) that while he was there, Snowden sat through the required training some of which qualified him to dip into a special category of content intercepted inside the U.S. This surveillance, *"with the assistance of an electronic communication service provider," took place under a classified interpretation of Section 702 of the FISA Amendments Act of 2008. Some of the content belonged to U.S. citizens, companies, and green card holders, all entitled to Fourth Amendment protection. That stuff went into a close-hold data repository. Information drawn from it had to be specially marked* (Gellman 2020a, 85-86; emphasis added). One presumes this repository was the BRF Partitions in the MAINWAY image earlier. As a result of the training, he was cleared for the FISA compartment. *He could "task" or assign new surveillance targets*.

Gellman (2020a, 86) notes that, because of his new job and training, Snowden could see and manipulate data intercepted overseas under presidential authority and at home under the judicial and congressional authority of FISA.

One month later, Snowden was permitted temporary leave from his position at the NSA in Hawaii on the pretext of receiving treatment for his epilepsy. On May 20, 2013 he flew to Hong Kong, where he was staying when the initial articles based on the leaked documents were published, beginning with *The Guardian* on June 5 (PopularTimelines n.d.).

## Oversight and Accountability

Gellman's book is not a revisit of everything that became publicly known or at least publicly available in the relatively contemporaneous aftermath of Snowden's provision of massive amounts of information and data to two journalists and the filmmaker. Nor should it be read as a comprehensive critique of what was learned.

Many journalistic analyses are referenced and linked to in this section. One extensive review (McDermott 2018) centers on the question, "Why would or should we trust the Intelligence Community?" It draws on the work of journalists, results of FOIA litigation by NGOs, and research, and looks at what we had learned and how that fits with what we had been told.

### ***Special Access Programs***

As noted earlier, Cheney ordered that STELLARWIND be concealed from the judges of the FISA Court, from members of the intelligence committees in Congress, and from most of Bush's national security staff. Judicial and legislative oversight and any authority but Cheney's were thus precluded.

In 2008, Julian Sanchez (2008) wrote in *ars Technica* that the central bone of contention wasn't warrantless wiretapping, but rather some form of data mining. And in 2013, via reporting in *The Washington Post* (Gellman 2013) and a March 2009 near-final draft classified NSA report (Office of the Inspector General 2009) made public and reported on by *The Guardian* (Greenwald and Ackerman 2013a), we learned that the controversy specifically involved Internet, not telephone, metadata.

STELLARWIND had four components, each corresponding to types of information that President Bush authorized the NSA to collect without a court order (Sanchez 2008):

- Internet content
- Internet metadata
- telephone content (e.g., warrantless wiretapping)
- telephone metadata (i.e., the massive call records database)

In broad outline, this much had been made public by *Salon* (Salon Staff 2007) well before Snowden arrived in Hawaii in March, 2012. What Snowden found, and *The Guardian* made public in June 2013, was something new: a near-final draft of the NSA Inspector General’s report on the episode, classified and compartmented as ECI. The fifty-seven pages of the draft IG report laid out a detailed history of the warrantless surveillance programs, culminating in the collapse of Justice Department legal support (Gellman 2020a, 70).

According to the report, when the Acting Attorney General James Comey refused to certify that the operations were lawful (Sanchez 2013), Addington telephoned Michael Hayden:

> On 11 March 2004, General Hayden had to decide whether NSA would execute the Authorization without the Attorney General’s signature. General Hayden described a conversation in which David Addington asked, “Will you do it?” Hayden said yes. (Gellman 2020a, 71)

The rebellion in the Justice Department forced Bush to seek authority for the warrantless programs from the FISA Court and eventually from Congress. Bush briefly "discontinued" the bulk Internet metadata collection involving Americans (Gellman 2020a, 123). The NSA IG report notes that "DoJ and NSA immediately began efforts to recreate this authority" (Greenwald and Ackerman 2013b). DOJ quickly convinced the FISA Court to authorize ongoing bulk collection of email metadata records. On 14 July 2004, FISA Court chief judge Colleen Kollar-Kotelly legally blessed it under a new order – the first time the surveillance court exercised its authority over the two-and-a-half-year-old surveillance program (Greenwald and Ackerman 2013b).

Gellman notes that during this period, Cheney and his lawyer maintained that no one in the executive, judicial, or legislative branches had the power to limit the president's warmaking authority (also see Gonzales 2006). Intelligence gathering, which is inherent in war, was the exclusive prerogative of the commander in chief (Gellman 2020a, 70).

### ***PRISM***

In 2005, Risen and Lichtblau (2005) reported that "under a presidential order signed in 2002, the intelligence agency *monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years* in an effort to track possible "dirty numbers" linked to Al Qaeda. The agency, Risen and Lichtblau (2005) said, *still seeks warrants to monitor entirely domestic communications* (emphasis added):

> Administration officials are confident that existing safeguards are sufficient to protect the privacy and civil liberties of Americans, the officials say. In some cases, they said, the Justice Department eventually seeks warrants if it wants to expand the eavesdropping to include communications confined within the United States. The officials said the administration had briefed Congressional leaders about the program and notified the judge in charge of the Foreign Intelligence Surveillance Court, the secret Washington court that deals with national security issues.

There was the presidential order of 2002, and then there was mostly secret law and policy. Gellman (2020a, 170) cites the NSA's position that until 2007, the Agency had to apply for an individual warrant for every surveillance order "simply because the Government was collecting off a wire in the United States"; "the government could not search a Skype or AOL account without a warrant from the Foreign Intelligence Surveillance Court (Gellman 2020a, 122). *Each warrant required probable cause to believe that a specific account belonged to an agent of a foreign power*. Gellman (2020a, 122) notes the Court nearly always granted those warrants, but it did perform an individual review.

After Congress passed the Protect America Act and the FISA Amendments Act in 2007, Justice Department lawyers persuaded the FISA Court that it could authorize surveillance of an unlimited number of accounts with a single order. The Court's decision, based solely on government briefs, was classified as "sensitive compartmented information" (Gellman 2020a, 123).

Under the Court's decision, Gellman reports (2020a, 112) a FISA Court judge no longer needed to hear a valid foreign intelligence purpose for surveillance of each proposed target. Neither the Court nor the intelligence committees in Congress even knew who the targets were. Once a year, in a classified proceeding, the Court approved two documents. The first laid out rules meant to govern the NSA's choice of accounts to monitor. The second specified procedures for "minimizing," or limiting.

Under Presidents Bush and Obama, Justice Department lawyers secretly persuaded the FISA Court that *every record of every call* met the relevance test because a terrorist plot might involve a party or parties unknown (Gellman 2020a, 143).

Gellman (2020a, 124) is careful to stipulate that PRISM was not a mass surveillance program. The NSA chose target accounts by way of individual taskings:

> Analysts identified those accounts by email address or a comparably specific factor such as telephone number used for registration. ... PRISM users were forbidden to spy deliberately on U.S. persons...If Americans turned up "incidentally"...NSA operators were obliged to "minimize," or restrict access to, those names. ... Nothing in the Snowden archive, and nothing I learned independently, offered reason to doubt that the NSA workforce did its best to follow the rules in good faith."

And yet, Gellman (2020a, 342) also quotes Rick Ledgett, the former NSA deputy director as having used the term "gates," not "prohibitions," to describe the limits imposed by minimization procedures.

Under PRISM, Gellman (2020a, 125) notes, the NSA sent selectors to Silicon Valley by the tens of thousands, more than a hundred thousand accounts "on cover" at a time, unreviewable in volume, and in fact unreviewed by any independent authority. When the FISA Court approved the targeting procedures, it did not ask and was not told the account names under surveillance or the number of Americans swept in. As Gellman (2020, 126) observes, "the acquisition of Americans' content under PRISM was 'incidental' to surveillance aimed at foreigners, but that did not mean it was unforeseen." The Privacy and Civil Liberties Oversight Board, or PCLOB, concluded in 2014 that

> certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness. Such aspects include the unknown and potentially large scope of the incidental collection of U.S. persons' communications, the use of "about" collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search for the communications of specific U.S. persons within the information that has been collected. (9)

In November 2009, Attorney General Michael Mukasey approved new and more permissive rules for the Signals Intelligence Directorate. The rules allowed the NSA staff to calculate the social graphs discussed in the Technology section "from and through any selector, irrespective of nationality or location." That is, a U.S. telephone number could be used at the beginning, middle, or end of a contact chain, under no more restriction than a foreign intelligence target; Gellman (2020a, 176) points out that the "same change applied to British, Australian, and other allied Five Eyes nationals who were normally off-limits."

MAINWAY and the Graph-in-Memory keep copies of every map they draw. Remember that the FISA Court allowed the NSA to hold on to telephone logs for five years. As Gellman (2020a, 179) realized, that offers no protection now, because the government can look back "as soon as it judges my work to pose a risk to protected national security information." It is easier for investigators to spy on his sources than on him: there is a lower legal bar for surveillance of someone who signs the security contract.

As Gellman notes, "there was no reason to track my contacts before the leak, but MAINWAY and associated tools could do it just as well in retrospect; the real MAINWAY is, in essence, a surveillance time machine" (Gellman 2020a, 179-180).

### ***Oversight as "Trust Us"***

At an Aspen Institute event in the late 2000s, Gellman served as a moderator for a panel with Ambassador John Negroponte and Admiral Dennis Blair, in what developed into an exchange about bulk collection and contact chaining (Gellman 2020a, 160-161). In the exchange, Negroponte asserted that maybe bulk collection of telephone records empowered the NSA to map the communications of anyone...in America - but the people who possessed that power used it with discipline and restraint. "They check themselves every step of the way," Blair said, "and they are not rummaging around in trillions of records to try to see if they can find something interesting" (Gellman 2020a, 161).

*They check themselves* (emphasis Gellman). As Gellman notes, there were supervisors and compliance officers, an inspector general, a general counsel, and a director of national intelligence who made classified certifications that the NSA followed its rules – the rules were also classified (Gellman 2020a, 160-161). Moreover, the official government position in court, in *United States v. Moalin*, was that there is no privacy interest in this kind of "metadata" (*United States Court of Appeals for the Ninth Circuit* 2020).

Indeed, the NSA's oversight and compliance directorate generated many reports, but seldom found abuse, in large part because the agency defined the term narrowly:

> Abuse was a knowing breach of regulations by a rogue employee for reasons such as personal gain, vengeance, or romance gone bad. ... Corrupt use of PRISM was not the issue. The hard questions arose from its fine print and everyday practice, when the system worked exactly as intended. (Gellman 2020a, 126)

The Bush and Obama administrations defended the FISA Amendments of 2008 and 2012 as modest technical adjustments for changing times, with constitutional protections and judicial review intact. However, as Gellman (2020a, 126-127) observes, deep layers of secrecy, alongside careful deflection of questions about the government's intent, "had left a major shift of legal boundaries invisible outside the privileged world of classified knowledge." Here Gellman (2020a, 126) quotes James Brenner, who supported the change in law, but acknowledged in an invited Fort Meade audience in 2015 that its import was concealed from the public; NSA was operating under statute, but ordinary, intelligent, educated Americans could not have looked at that statute and understood that it meant what the FISA Court interpreted it to mean.

After Gellman's tense encounter with Admiral William McRaven at a previous Aspen Security Forum, McRaven agreed in July 2013 to meet him in person. In what Gellman (2020a, 154) called an attempt to find some common ground, McRaven said “I’m a big believer in transparency, so please do quote me on that. And the processes are out there that allow the transparency to occur at the right level.” The right level, as he meant it, did not fall within the public domain. Quite the reverse:

> McRaven believed in transparency inside the walled precincts of the FISA Court and the House and Senate intelligence committees. The public had no need to know or contribute outside views on policy or law. *Classified transparency*, in other words. McRaven saw no contradiction in that. (Gellman 2020a, 155; emphasis added)

This model, as Gellman (2020a) notes, is the prevailing one among McRaven’s peers, and extended far beyond surveillance policy:

> How many noncombatants died in special operations raids? Did the rules of engagement conform to American values or international law? Should U.S. drones be allowed to make autonomous decisions of life and death? All those things were classified, exempt from debate. (155)

Gellman (2020a, 262) asks a simple question: How often does the NSA break its own privacy rules? We can’t know. The agency keeps internal statistics of those “compliance incidents.” The statistics are classified CONFIDENTIAL, which is supposed to mean that disclosure would damage national security.

Gellman cites the finding of the Moynihan Commission's *Report of the Commission On Protecting And Reducing Government Secrecy* (Commission on Protecting and Reducing Government Secrecy 1997) that the classification system is used too often to deny the public an understanding of the policymaking process, rather than for the necessary protection of intelligence activities and other highly sensitive matters.

Gellman (2020a) argues that it is hard to justify the mere number, a simple count of the errors, being treated as a state secret as other than an attempt of the sort the Commission noted, in particular to deter congressional oversight and legislation:

> Quite a lot harder to justify: the Justice Department, which prepares a similar compliance report for Congress and the FISA Court, classified exactly the same statistics as TOP SECRET//SI. That had a very practical impact. High-level clearances are rare among members of congressional staffs. Most offices had nobody eligible to read the compliance reports. You might suspect that someone preferred it that way.
>
> Members of Congress often express frustration at their impotence to oversee secret bureaucracies in the executive branch. It is difficult, even with constitutional authority, to induce a person to tell you what you do not know how to ask. (263-264)

### *Who Should Be Held Accountable?*

In 2001, Gellman (2020a, 274-275) notes that according to NSA documents, the Agency "stood up" a staff of leak trackers, under Joseph Brand, a senior NSA executive who was also among the leading advocates of a crackdown on leaks. The agency allocated new positions for that purpose to an interagency Foreign Denial and Deception Committee (FDDC) established by the director of Central Intelligence in 1994.

Under George Tenet, Gellman (2020a, 274-275) reports, the project began compiling records in May 1999, and grew large enough, according to Brand, that it "hired [a] contractor with FDDC funds to build [a] foreign knowledge database (FIRSTFRUITS)"; One of its major purposes was to feed information about harmful news stories to the "Attorney General task force to investigate media leaks."

Gellman (2020a, 274-275) notes that in forty-nine cases, three of them involving him, the FIRSTFRUITS produced "crime reports to DOJ." This, he says, left the FBI with a conundrum: What crime, exactly, was it being asked to investigate? Congress has never passed a law that squarely addressed unauthorized disclosures to reporters from public officials.

When it comes to criminal law, there are potential charges of theft or unlawful possession of government property. The nearest analogy in the law, however, and the charge most commonly prosecuted in such cases, is espionage.  From the NSA's point of view, a loss is a loss as Gellman

(2020a, 275) notes: "it may not matter whether a foreign adversary learns the secret from a spy or a published news report. The cryptologic insecurity is the same. Before the disclosure, the NSA had a valuable source or method. Afterward, it does not."

In other ways, Gellman (2020a) says, espionage is a terrible analogy for a news media leak; spying and talking to a journalist are not the same behavior at all:

> The charge [espionage] is nonetheless a fiction enacted as law. The underlying conduct, which may be whistleblowing of the purest kind, is disfigured by forcing the whistleblower into the mold of a spy. If news is conceived as espionage, then it is logical for George Ellard to call me an agent of the adversary and James Clapper to call me an accomplice. It is no stretch at all, from that point, to deployment of the government's most intrusive counterintelligence powers against a journalist. (275)

### ***Snowden***

Gellman reports that after the first stories were published, Snowden would tell him he had in fact raised concerns repeatedly with NSA colleagues and supervisors: "I had no way to confirm that. NSA officials told me they found no evidence that Snowden reported a violation of law or rules, but they could not exclude that he spoke of his doubts to colleagues in less formal ways" (Gellman 2020a, 20).

The reality was that he was a contractor and therefore might not be covered by the limited whistleblower protections of the then-current presidential directive (PPD-19). On my reading of the PPD, Snowden was correct. In the first exchange with Gellman (2020a, 20), Snowden's emphasis was on futility; whistleblowers are commonly crushed when they challenge the leaders or priorities of their agencies.

As noted earlier by Gellman (2020a, 70), when Snowden was doing his "dirty word searches" in Kunia in 2012, one of them produced hits on "STARBURST," "WHIPGENIE," and "STELLARWIND." "It was the STELLARWIND memo that really affected me" Snowden told Gellman; "the fact that Hayden knew there was no statutory authority" (Gellman 2020a, 71). Hayden's career, Snowden noted, continued to thrive in the aftermath. He was not disciplined, charged with an offense, or subjected to hard questions about his choice in a public hearing. *When Congress learned of the secret programs, it gave retroactive legal immunity to those who carried them out and authority for future presidents to keep them going. The lesson Snowden drew was that even in the most extreme case, when an NSA director knowingly broke the law as the attorney general defined it, no branch of government was prepared to hold him accountable* (Gellman 2020a, 71; emphasis added). The public had no idea what transpired. Snowden believed it should.

Snowden's shift of allegiance from the government to the public at large, as he conceived its interests, was years in the making. But, as Gellman (2020a, 32) says, "By the time he left the CIA, fantasies of rebellion had taken on the character of planning." Snowden had worked for the CIA from approximately 2006 -2009. His shift seems to have concretized at Kunia. Gellman (2020a, 31) writes that “(m)onths would pass before Snowden approached news reporters, but he had reached the staging point.” Snowden's riskiest intrusions into NSA files took place the following year while he was working as a Booz Allen contractor at the agency’s new Captain Joseph J. Rochefort command center (Gellman 2020a, 32).

In January 2014, Snowden told Gellman his "breaking point" was "seeing the Director of National Intelligence, James Clapper, directly lie under oath to Congress":

> There's no saving an intelligence community that believes it can lie to the public and the legislators who need to be able to trust it and regulate its actions. Seeing that really meant for me there was no going back. Beyond that, it was the creeping realization that no one else was going to do this. The public had a right to know about these programs. (PopularTimelines n.d.)

This quote referred to testimony on March 12, 2013 in which Clapper denied to the U.S. Senate Select Committee on Intelligence that the NSA wittingly collects data on millions of Americans.

Clapper was performatively lying to Congress, and actually said “not wittingly,” which he later said was the “least untruthful” answer he could give. Senator Ron Wyden, Chair of the Senate Intelligence Committee, already knew the answer (some oblique version of “yes”, one assumes). As Gellman (2020a, 164) puts it, Clapper knew that Wyden knew; he had briefed the Committee in a classified session. But Wyden wanted a yes-or-no answer with the cameras rolling.

Clapper's testimony was nine months after the NSA says Snowden made his first illegal downloads during the summer of 2012, and three months after Snowden first sought to share thousands of NSA documents with Greenwald (PopularTimelines n.d.). In March 2014, Snowden said he had reported policy or legal issues related to spying programs to more than ten officials, but as a contractor had no legal avenue to pursue further whistleblowing (PopularTimelines n.d.).

In May 2014, U.S. officials released a single email that Snowden had written in April 2013 inquiring about legal authorities, but said that they had found no other evidence that Snowden had expressed his concerns to someone in an oversight position (PopularTimelines n.d.).

In June 2014, the NSA said it had not been able to find any records of Snowden raising internal complaints about the agency's operations. That same month, Snowden explained that he had not produced the communiqués in question because of the ongoing nature of the dispute, disclosing for the first time that "I am working with the NSA in regard to these records and we're going back and forth, so I don't want to reveal everything that will come out" (PopularTimelines n.d.).

In a closed briefing not long before Gellman's 2015 trip to Moscow, Clapper briefed members of Congress on the fallout from the first several months of Snowden leaks. “History suggested” Clapper said, “that early analysis overstated the harm...Signals intelligence generally found ways to reacquire its targets. People must communicate. They want to communicate. They will make mistakes, and we will exploit them” (Gellman 2020a, 266).

***What are the Rules and Limitations on the NSA Now?***

From my reading of the Obama PPD-28, its Partial Revocation (Biden 2022a), and Executive Order 14086 (Biden 2022b), there is no way to tell what, if any, rules and limitations are imposed. My skeptical view is largely informed by the very careful wording of the Privacy and Civil Liberties Oversight Board (n.d.) in its oversight reports. The PCLOB has access to most, if not all, of the classified materials behind and related to the Intelligence Community practices.

Slightly more generous in-depth analyses of Executive Order 14086 from the civil liberties community can be found in Goitein (2022) and Gorsky (2022).  In terms of the FISA Court opinions and the Court itself, analyses from the civil liberties community can be found in Laperruque (2021), Sanchez (2021), and Patel and Raya (2020).

For myself, the more I re-read the discussions in Gellman’s book, especially about the technology and Snowden’s time in Hawaii, the more certain I became that the executive branch was/is still just moving the same few chess pieces – sometimes with different code names assigned – around an “avoid oversight and accountability” chessboard.

I stated in the beginning of this review that I was shocked by what I learned, e.g., the beginnings, duration, and expansion of MAINWAY. Readers should definitely read *Dark Mirror* to get the full story and form their own points-of-view. Gellman is a deeply-informed and compelling story-teller (especially if one goes with his flow) and this book is an important addition to our understanding of the reach and scope of the American Surveillance State.

**References**

Biden, Joseph R. 2022a. *National Security Memorandum on Partial Revocation of Presidential Policy Directive 28.* National Security Memorandum/NSM-14. The White House. October 7. https://www.presidency.ucsb.edu/documents/national-security-memorandum-partial-revocation-presidential-policy-directive-28

____________. 2022b. *Executive Order 14086: Enhancing Safeguards for United States Signals Intelligence Activities.* The White House. October 7. https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities

Commission on Protecting and Reducing Government Secrecy. 1997. *Report. S. Doc. 105-2*. March 3. https://sgp.fas.org/library/moynihan/title.html

Electrospaces.net. 2020*. Edward Snowden and the STELLARWIND Report.* March 26, updated June 10, 2020. https://www.electrospaces.net/2020/03/edward-snowden-and-stellarwind-report.html

Felten, Edward W. 2013. *Declaration of Professor Edward W. Felten. United States District Court Southern District of New York.* August 23. http://ia801902.us.archive.org/21/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf

Gellman, Barton, and Laura Poitras. 2013. "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program." *The Washington Post*, June 7. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-Internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Gellman, Barton. 2013. "U.S. Surveillance Architecture includes Collection of Revealing Internet, Phone Metadata." *The Washington Post*, June 15. https://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-Internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html

Gellman, Barton, and Ashkan Soltani. 2013. **"**NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say." *The Washington Post*, October 30**.** https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Gellman, Barton. 2020(a). *Dark Mirror: Edward Snowden and the American Surveillance State.* New York: Penguin Press.

_____________. 2020(b). "Inside the NSA's Secret Tool for Mapping Your Social Network." *Wired*, May 24. https://www.wired.com/story/inside-the-nsas-secret-tool-for-mapping-your-social-network/

Goitein, Elizabeth. 2022. **"**The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance." *Just Security*, October 31. https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/

Gonzales, Alberto R. 2006. *Letter to William H. Frist, Majority Leader, United States Senate.* January 19. http://www.justice.gov/ag/readingroom/surveillance9.pdf

Gorski, Ashley. 2022. "The Biden Administration's SIGINT Executive Order, Part II: Redress for Unlawful Surveillance." *Just Security*, November 4. https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii/

Greenwald, Glenn, and Spencer Ackerman. 2013(a). "NSA Inspector General Report on Email and Internet Data Collection under STELLARWIND." *The Guardian*, June 27.

https://www.theguardian.com/nsa-inspector-general-report-document-data-collection

___________________________________. 2013(b). “NSA Collected US Email Records in Bulk for More Than Two years Under Obama.” *The Guardian*, June 27. https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama

Laperruque, Jake. 2021. “Key Takeaways From Latest FISA Court Opinion on Section 702 and FBI Warrantless Queries.” *Just Security*, April 28. https://www.justsecurity.org/75917/key-takeaways-from-latest-fisa-court-opinion-on-section-702-and-fbi-warrantless-queries/

McDermott, Patrice. 2018. "Secrets and Lies — Exposed and Combatted: Warrantless Surveillance Under and Around the Law 2001-2017." *Secrecy and Society* 2(1). DOI: https://doi.org/10.31979/2377-6188.2018.020102 https://scholarworks.sjsu.edu/secrecyandsociety/vol2/iss1/2

“NSA Slides Explain the PRISM Data-Collection Program. Cover Slide of PRISM.jpg.” 2013. *The Washington Post*, June 6, updated July 10. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Obama, Barack. 2014. *Policy Directive/PPD-28. Presidential Policy Directive - Signals Intelligence Activities.* The White House, January 17. https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

Office of the Inspector General. 2009. “NSA Inspector General Report on Email and Internet Data Collection under STELLARWIND.” ST-09-0002.*The Guardian*, March 24. https://www.theguardian.com/nsa-inspector-general-report-document-data-collection

Patel, Faiza, and Raya Koreh. 2020. “Improve FISA on Civil Liberties by Strengthening Amici.” *Just Security*, February 26. https://www.justsecurity.org/68825/improve-fisa-on-civil-liberties-by-strengthening-amici/

PopularTimelines. n.d. *History of Edward Snowden in Timeline*. https://webcache.googleusercontent.com/search?q=cache:https://popu lartimelines.com/timeline/Edward-Snowden

Privacy and Civil Liberties Oversight Board. n.d. *Oversight Reports*. https://www.pclob.gov/Oversight

Privacy and Civil Liberties Oversight Board. 2014. *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign*

*Intelligence Surveillance Act.* July 2. https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf

Risen, James, and Eric Lichtblau. 2005. "Bush Lets U.S. Spy on Callers Without Courts*." The New York Times*, December 16. https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html

Sanchez, Julian. 2008. "Behind the Legal Fight over NSA's 'STELLARWIND' Surveillance." *ars Technica*, December 16. https://arstechnica.com/tech-policy/2008/12/behind-the-legal-fight-over-nsas-stellar-wind-surveillance/

____________. 2013. "What the Ashcroft 'Hospital Showdown' Was About." *Cato at Liberty Blog*, July 19. https://www.cato.org/blog/what-ashcroft-hospital-showdown-was-about

____________. 2021. "Reforming the FISA Process: Tweak or Overhaul?" *Just Security*, June 30. https://www.justsecurity.org/77146/reforming-the-fisa-process-tweak-or-overhaul/

United States Court of Appeals for the Ninth Circuit. 2020. *United States v. Moalin.* September 2. https://www.aclu.org/legal-document/united-states-v-moalin-ninth-circuit-opinion