- **A Security Story by Barton Gellman**
-

“What time exactly does your clock say?” asked the voice on the telephone, the first words Edward Snowden ever spoke to me aloud. (Our previous communications had all been via secure text chats over encrypted anonymous links on secret servers.) I glanced at my wrist—3:22 p.m. “Good. Meet me exactly at four. I’ll be wearing a backpack.” Of course he would; Snowden would never leave his laptop unattended.

The rendezvous point Snowden selected that day, December 5, 2013, was a gaudy casino hotel called the Korston Club, on Kosygina Street in Moscow. Enormous flashing whorls of color adorned the exterior in homage to Las Vegas. In the lobby, a full-size grand player piano tinkled with energetic pop. The promenade featured a “Girls Bar” with purple-neon decor, stainless-steel chairs and mirrors competing for attention with imitation wood paneling, knockoff Persian rugs, and pulsing strobe lights on plastic foliage. Also, feathers. The place looked like a trailer full of old Madonna stage sets that had been ravaged by a tornado.

As I battled sensory overload, a young man appeared near the player piano, his appearance subtly altered. A minder might be anywhere in this circus of a lobby, but I saw no government escort. We shook hands, and Snowden walked me wordlessly to a back elevator and up to his hotel room. For two days, throughout 14 hours of interviews, he did not once part the curtains or step outside. He remained a target of surpassing interest to the intelligence services of more than one nation.

He resisted questioning about his private life, but he allowed that he missed small things from home. Milkshakes, for one. *Why not make your own?* Snowden refused to confirm or deny possession of a blender. Like all appliances, blenders have an electrical signature when switched on. He believed that the U.S. government was trying to discover where he lived. He did not wish to offer clues, electromagnetic or otherwise. U.S. intelligence agencies had closely studied electrical emissions when scouting Osama bin Laden's hideout in Pakistan. "Raising the shields and lowering the target surface" was one of Snowden's security mantras.

On bathroom breaks, he took his laptop with him. "There's a level of paranoia where you go, 'You know what? This could be too much,'" he said when I smiled at this. "But it costs nothing. It's—you get used to it. You adjust your behavior. And if you're reducing risk, why not?"

Over six hours that day and eight hours the next, Snowden loosened up a bit, telling me for the first time why he had reached out to me the previous spring. "It was important that this not be a radical project," he said, an allusion to the politics of Glenn Greenwald and Laura Poitras, the other two journalists with whom he'd shared digital archives purloined from the National Security Agency a few months earlier. "I thought you'd be more serious but less reliable. I put you through a hell of a lot more vetting than everybody else. God, you did screw me, so I didn't vet you enough." He was referring to my profile of him in *The Washington Post* that June, in which I had inadvertently exposed an online handle that he had still been using. (After that he had disappeared on me for a while.)

When we broke for the night, I walked into a hotel stairwell and down two floors, where I found an armchair in a deserted hallway. I might or might not have been under surveillance then, but I had to assume I would be once back in my room, so this was my best chance to work unobserved.

I moved the audio files from the memory card of my voice recorder to an encrypted archive on my laptop, along with the notes I had typed. I locked the archive in such a way that I could not reopen it without a private electronic key that I'd left hidden back in New York. I uploaded the encrypted archive to an anonymous server, then another, then a third. Downloading it from the servers would require another private key, also stored in New York. I wiped the encrypted files from my laptop and cut the voice recorder's unencrypted memory card into pieces. Russian authorities would find nothing on my machines. When I reached the U.S. border, where anyone can be searched for any reason and the warrant requirement of the Fourth Amendment does not apply, I would possess no evidence of this interview. Even under legal compulsion, I would be unable to retrieve the recordings and notes in transit. I hoped to God I could retrieve them when I got home.

Were my security measures excessive? I knew the spy agencies of multiple governments—most notably the United States'—were eager to glean anything they could from Edward Snowden. After all, he had stolen massive amounts of classified material from NSA servers and shared it with Poitras, Greenwald, and me, and we had collectively published only a fraction of it. The U.S. government wanted Snowden extradited for prosecution. But I'm not a thief or a spy myself. I'm a journalist. Was I just being paranoid?

[From the November 2015 issue: If you're not paranoid, you're crazy]

Six months earlier, in June 2013, when the Snowden story was less than two weeks old, I went on *Face the Nation* to talk about it. Afterward, I wiped off the television makeup, unclipped my lapel microphone, and emerged into a pleasant pre-summer Sunday outside the CBS News studio in the Georgetown neighborhood of Washington, D.C. In the back of a cab I pulled out my iPad. The display powered on, then dissolved into static and guttered out. *Huh?* A few seconds passed and the screen lit up again. White text began to scroll across an all-black background. The text moved too fast for me to take it all in, but I caught a few fragments.

> # root:xnu ...
>
> # dumping kernel ...
>
> # patching file system ...

Wait, what? It looked like a Unix terminal window. The word *root* and the hashtag symbol meant that somehow the device had been placed in super-user mode. Someone had taken control of my iPad, blasting through Apple's security restrictions and acquiring the power to rewrite anything that the operating system could touch. I dropped the tablet on the seat next to me as if it were contagious. I had an impulse to toss it out the window. I must have been mumbling exclamations out loud, because the driver asked me what was wrong. I ignored him and mashed the power button. Watching my iPad turn against me was remarkably unsettling. This sleek little slab of glass and aluminum featured a microphone, cameras on the front and

back, and a whole array of internal sensors. An exemplary spy device.

**From Our June 2020 Issue**



I took a quick mental inventory: No, I had not used the iPad to log in to my online accounts. No, I didn't keep sensitive notes on there. None of that protected me as much as I wished to believe. For one thing, this was not a novice hacking attempt. Breaking into an iPad remotely, without a wired connection, requires scarce and perishable tools. Apple closes holes in its software as fast as it finds them. New vulnerabilities are in high demand by sophisticated criminals and intelligence agencies. Shadowy private brokers pay millions in bounties for software exploits of the kind I had just seen in action. Someone had devoted resources to the project of breaking into my machine. I did not understand how my adversary had even found the iPad. If intruders had located this device, I had to assume that they could find my phone, too, as well as any computer I used to access the internet. I was not meant to see the iPad do what it had just done; I had just lucked into seeing it. If I hadn't, I would have thought it was working normally. It would not have been working for me.

Someone had taken control of my iPad, blasting through Apple's security restrictions. I dropped the tablet on the seat next to me

as if it were contagious.

This was the first significant intrusion into my digital life—that I knew of. It was far from the last. In the first days of 2014, an NSA whistleblower, Tom Drake, told me he had received an invitation from one of my email addresses, asking him to join me for a chat in Google Hangouts. It looked exactly like an authentic notice from Google, but Drake had the presence of mind to check whether the invitation had really come from me. It had not. An impostor posing as me wanted to talk with Drake.

Shortly after that, Google started refusing my login credentials on two accounts. An error message popped up in my mail client: "Too many simultaneous connections." I looked under the hood and found that most of the connections came from IP addresses I did not recognize. On the Gmail page, a pink alert bar appeared at the top, reading, "Warning: We believe state-sponsored attackers may be attempting to compromise your account or computer. Protect yourself now."

Which state sponsor? Per company policy, Google will not say, fearing that information could enable evasion of its security protocols. I did some further reporting and later learned from confidential sources that the would-be intruder in my accounts was Turkey's national intelligence service, the Millî Istihbarat Teşkilatı. Even though I never send anything confidential over email, this was terrible news. A dozen foreign countries had to have greater motive and wherewithal to go after the NSA documents Snowden had shared with me—Russia, China, Israel, North Korea, and Iran, for starters. If Turkey was trying to hack me too, the threat landscape was more crowded than I'd feared.

Some of the hackers were probably better than Turkey's—maybe too good to be snared by Google's defenses. Not encouraging.

From the May 2014 issue: We need more secrecy

The MacBook Air I used for everyday computing seemed another likely target. I sent a forensic image of its working memory to a leading expert on the security of the Macintosh operating system. He found unexpected daemons running on my machine, serving functions he could not ascertain. (A daemon is a background computing process, and most of them are benign, but the satanic flavor of the term seemed fitting here.) Some software exploits burrow in and make themselves very hard to remove, even if you wipe and reinstall the operating system, so I decided to abandon the laptop.

For my next laptop, I placed an anonymous order through the university where I held a fellowship. I used two cutouts for the purchase, with my name mentioned nowhere on the paperwork, and I took care not to discuss the transaction by email. I thought this would reduce the risk of tampering in transit—something the NSA, the FBI, and foreign intelligence services are all known to have done. (No need to hack into a machine if it comes pre-infected.) But my new laptop, a MacBook Pro, also began to experience cascading hardware failures, beginning with a keyboard that lagged behind my typing, even with a virgin operating system. The problems were highly unusual.

I brought the machine for repair to Tekserve, a New York City institution that at the time was the largest independent Apple service provider in the United States. I had been doing business there since at least the early 1990s, a couple of years after Tekserve set up shop in a Flatiron warehouse space. I liked the

quirky vibe of the place, which had a porch swing indoors and an ancient Coke machine that once charged a nickel a bottle. But Tekserve's most important feature was that its service manager allowed me to stand with a senior technician on the repair floor as he worked on my machine. I preferred not to let it out of my sight.

The technician tested and swapped out, seriatim, the keyboard, the logic board, the input/output board, and, finally, the power interface. After three visits, the problem remained unsolved. Keystrokes would produce nothing at first, then a burst of characters after a long delay. Tekserve consulted with supervisors at Apple. Nobody could explain it. I asked the technician whether he saw anything on the circuit boards that should not be there, but he said he was not equipped to detect spy gear like that. "All I know is I've replaced every single part in the machine," he told me. "We've never seen this kind of behavior before." I gave up and got another one.

When the Snowden story broke, I was using a BlackBerry smartphone. I began to receive blank text messages and emails that appeared to have no content and no reply address. Texts and emails without visible text are commonly used to transmit malicious payloads. I got rid of the BlackBerry and bought an iPhone, which experts told me was the most secure mobile device available to the general public. I do not do sensitive business on a smartphone, but I did not like the feeling of being watched.

In January 2014, I became an early adopter of SecureDrop, an anonymous, encrypted communications system for sources and journalists. It is still the safest way to reach me in confidence,

and I have received valuable reporting tips this way. Having advertised a way to reach me anonymously, I've also gotten my share of submissions from internet trolls and conspiracy theorists, as well as run-of-the-mill malware. I never run executable files or scripts that arrive by email, so these were not a big concern. One day, however, a more interesting exploit showed up—a file disguised as a leaked presentation on surveillance. I asked Morgan Marquis-Boire, a security researcher then affiliated with the Toronto-based Citizen Lab, if he would care to have a look. "You've got a juicy one," he wrote back.

Read: The vindication of Edward Snowden

Most hacking attempts are sent to thousands, or millions, of people at a time, as email attachments or links to infected websites. This one was customized for me. It was a class of malware known as a "remote access trojan," or RAT, capable of monitoring keystrokes, capturing screenshots, recording audio and video, and exfiltrating any file from my computer. "Piss off any Russians lately?" Marquis-Boire asked. The RAT was designed to link my computer to a command-and-control server hosted by Corbina Telecom, in Moscow. If I had triggered the RAT, a hacker could have watched and interacted with my computer in real time from there. Other IP addresses the malware communicated with were in Kazakhstan. And internal evidence suggested that the coder was a native speaker of Azeri, the language of Azerbaijan and the Russian republic of Dagestan. But the moment Marquis-Boire tried to probe the RAT for more information, the command-and-control server disappeared from the internet.

Illustration: Cristiana Couceiro; Barton Gellman / Getty

Overtures of another kind came to my colleague Ashkan Soltani soon after his byline appeared alongside mine in *The Washington Post*. “Within the span of a week, three hot, really attractive women messaged me out of the blue” on OkCupid, he later told

me over beers. Two of the women made their intentions known right away.

He pulled out screenshots of their messages. “Excuse my brazen demeanor but i find you incredibley cute and interesting,” one of them wrote. “Let’s meet up?”

Then, on the day they set, she proposed getting together at his place. “It’s gloomy out. makes me want to cuddle,” she wrote.

“The fact that two girls in a row were making themselves available on the first date, I was like, *What the fuck?*” he told me. “*Am I being*, what—there’s a word for that—”

“Honey trapped,” I said.

“Yeah, honey trapped. I do okay, but it usually involves going out on a couple dates or whatever,” he said. “I don’t think I’m a bad-looking guy, but I’m not the kind of guy women message out of the blue and invite me to cuddle.” He decided to cancel.

**Related Stories**

- My Family Story of Love, the Mob, and Government Surveillance
- Mass Surveillance Is Coming to a City Near You

Soltani suspected an intelligence-agency setup—“the Chinese government trying to get up on me”—in an effort to elicit information about the NSA documents, or to steal digital files. A well-known information-security attack known as the “evil maid”

relies on brief physical access to a computer to steal its encryption credentials. As it happened, the Snowden files were at that time locked in a *Washington Post* vault, and kept separate from the electronic keys that allowed access to them, but outsiders would not know that. And an attractive spy might assume that, with the right enticements, anything was possible.

When Soltani returned to OkCupid to document these interactions in more detail, he searched for the two women who had pursued him so aggressively. Their online profiles no longer existed.

Soltani did go out with the third woman who had reached out to him around the same time, "but for the longest time I would not bring her back to my house," he said. "I wasn't comfortable. I remember that feeling. I would never leave my phone when I went to the bathroom. It's weird to have opsec when you're dating."

By the time we had this conversation, in the late fall of 2015, Soltani and I had stopped writing stories for the *Post*. I was working on a book. Soltani had moved on to other things. He had retired his old laptop, returned an encryption key fob to me, and shed his last connection to classified materials. "When we were wrapping up, it felt really good that I didn't have to carry this burden anymore," he told me. "I mean, from the perspective of the duty to protect this stuff—there's still stuff in there that I think should absolutely never see light of day."

"You still constantly have to be diligent," he said to me. "You've been doing it for, like, three years. How do you do on vacation?"

Well, about that. Preoccupation with surveillance had distorted my professional and personal life. I had balked at the main gate of Disney World when I realized I would have to scan a fingerprint and wear a radio-tagged wristband everywhere in the park. My partner, Dafna, standing with our 7-year-old son, dared me with her eyes to refuse. I caved, of course. I brought my laptop almost everywhere I went, even on beach and hiking trips. I refused to leave my bag at coat checks at parties. The precautions I took to protect my electronics inconvenienced my friends and embarrassed my family. "You're moving further and further into a world that I'm not a part of, and that I don't understand and I don't want to be a part of," Dafna said one night. I had not come to terms, until that moment, with how abnormal my behavior had become. I never felt safe enough.

From the November 2016 issue: What surveillance will look like in the future

I built ever-thicker walls of electronic and physical self-defense. At one point in the spring of 2013, I requested a dedicated locked room at the *Post* for use by the reporters who worked with the Snowden documents. On a subsequent visit, a facilities staff member proudly showed me and Soltani the new space, in a place of honor beside the company president's office. The room had one feature I had specifically asked to avoid: a wall full of windows. If you craned your neck you could see a beaux-arts mansion half a block to the west—the Russian ambassador's residence in Washington. "You have to be kidding me," Soltani said. Crestfallen, I asked for a windowless space. The *Post* found one, installed a high-security lock, put a video camera in the hall outside, and brought in a huge safe that must have weighed 400 pounds.

I acquired a heavy safe for my office in New York as well. I will not enumerate every step I took to keep my work secure, but they were many and varied and sometimes befuddled me. The computers we used for the NSA archive were specially locked down. Soltani and I used laptops from which we'd removed the Wi-Fi and Bluetooth hardware, and disconnected the batteries. If a stranger appeared at the door, we merely had to tug on the quick-release power cables to switch off and re-encrypt the machines instantly. We stored the laptops in the vault and kept encryption keys on hardware, itself encrypted, that we took away with us each time we left the room, even for bathroom breaks. We sealed the USB ports. I disconnected and locked up the internet-router switch in my New York office every night. I dabbed epoxy and glitter on the screws along the bottom of all my machines, to help detect tampering in my absence. (The glitter dries in unique, random patterns.) A security expert had told me that detection of compromise was as important as prevention, so I experimented with ultraviolet powder on the dial of my safe in New York. (Photographing dust patterns under a UV flashlight beam turns out to be messy.) I kept my digital notes in multiple encrypted volumes, arranging the files in such a way that I had to type five long passwords just to start work every day.

At a farewell party for Anne Kornblut, who oversaw the *Post*'s Snowden coverage, my colleagues put on a skit that purported to depict our story meetings. The reporter Carol Leonnig, playing the role of Anne, pulled out blindfolds for everyone in the pretend meeting. They had to cover their eyes, she explained, before Bart could speak. Funny and fair, I had to admit. I was a giant pain in the ass.

But I felt I had to be, and my fear was that any single barrier could be breached. A friend who runs a lock and safe company told me that an expert safecracker could break into just about any commercial vault in less than 20 minutes. Intelligence agencies have whole departments working on how to stealthily circumvent barriers and seals. Special antennae can read the emanations of a computer monitor through walls. Against adversaries like this, all I could do was make myself a less appealing target. I layered on so many defenses that navigating through them became a chronic drain on my time, mental energy, and emotional equilibrium.

Years later Richard Ledgett, who oversaw the NSA's media-leaks task force and went on to become the agency's deputy director, told me matter-of-factly to assume that my defenses had been breached. "My take is, whatever you guys had was pretty immediately in the hands of any foreign intelligence service that wanted it," he said, "whether it was Russians, Chinese, French, the Israelis, the Brits. Between you, Poitras, and Greenwald, pretty sure you guys can't stand up to a full-fledged nation-state attempt to exploit your IT. To include not just remote stuff, but hands-on, sneak-into-your-house-at-night kind of stuff. That's my guess." Because I'd been one of Snowden's principal interlocutors, Ledgett told me he was sure there was "a nice dossier" on me in both Russia and China.

"If some of those services want you, they're going to get you. As an individual person, you're not going to be able to do much about that."

Illustration: Cristiana Couceiro; Digitalglobe / Getty

On January 29, 2014, James Clapper, then the director of national intelligence, sat down at a Senate witness table to deliver his annual assessment of worldwide threats, covering the gravest dangers facing the United States. He did not open his remarks with terrorism or nuclear proliferation or Russia or China. He opened with Edward Snowden, and within a few words he was

quoting one of my stories. “Snowden claims that he’s won and that his mission is accomplished,” Clapper said. “If that is so, I call on him and his accomplices to facilitate the return of the remaining stolen documents that have not yet been exposed, to prevent even more damage to U.S. security.”

Read: The latest Snowden leak is devastating to NSA defenders

I pretty much stopped listening after the word *accomplices*. This was not an off-the-cuff remark. It was prepared testimony on behalf of the Obama administration, vetted across multiple departments, including Justice. *Accomplice* has a meaning in criminal law.

“I had in mind Glenn Greenwald or Laura Poitras,” Clapper told me years later. “They conspired with him, they helped him in protecting his security and disseminating selectively what he had, so to me they are co-conspirators.”

“I wouldn’t distinguish myself categorically from them,” I said.

“Well, then maybe you are too. This is the whole business about one man’s whistleblower is another man’s spy.”

I asked Clapper whether I was a valid counterintelligence target.

“Theoretically you could be,” Clapper said. “Given how Snowden is viewed by the intelligence community, someone who’s in league with him, conspiring with him, that’s a valid counterintelligence—and for that matter law-enforcement—target.”

Twice in February 2014, George Ellard, then the NSA inspector general, referred to journalists on the story as Snowden’s

"agents." We had done more damage, he said at a Georgetown University conference, than the notorious FBI traitor Robert Hanssen, who'd helped Soviet security services hunt down and kill U.S. intelligence assets.

It became a running joke among U.S. officials that Bart Gellman should watch his back. In May 2014, I appeared on a panel alongside Robert Mueller, the former FBI director, to talk about Snowden. Mueller cross-examined me: Were the NSA documents not lawfully classified? Were they not stolen? Did I not publish them anyway? I held out my arms toward him, wrists together, as if for handcuffs. The audience laughed. Mueller did not.

I know perfectly well that government agencies prefer not to read their secrets on the front page. Sometimes they resent a story enough to investigate. *How in the blazes did the reporter find that out?* In serious cases maybe the Justice Department steps in. I knew all that—but despite years of reporting on government secrets, I had not often experienced it personally. So, in the summer of 2013, when I came across my own name in the NSA archive Snowden had shared with me, I gawped at the screen and bit back an impulse to swear.

The document with my name on it was part of an NSA memo for the attorney general of the United States about "unauthorized disclosures … of high-level concern to U.S. policy makers," referring in part to three *Washington Post* stories of mine about an intelligence operation gone wrong in the aftermath of the Gulf War. Reading the Snowden files, I learned that my reporting had been referred to the Justice Department for criminal investigation in early 1999. The FBI had been put on the case. I'd had no inkling at the time. How much did the bureau find out

about me and my confidential sources? The memo did not say. No harm, as far as I knew, had come to my sources, but I realized that for some I could not really say. It had been a long time.

The most intriguing part of the memo was the framing of the harm that the NSA ascribed to my stories. “Press leaks could result in our adversaries implementing Denial and Deception (D&D) practices,” the agency wrote. If adversaries know how the United States spies on them, in other words, they can do a better job of covering their tracks. That is a legitimate concern. But good journalism sometimes exposes deception by the U.S. government itself—not only in tradecraft but in matters of basic policy and principle.

One whole folder in the Snowden archive was devoted not to foreign spies but to journalists and the people who gave us information. The memos and slide decks laid out the grave dangers posed by news reporting. They also sketched the beginnings of a plan to do something about it: Every file in the folder mentioned a cryptonym that seemed to be the cover name for an effort to track and trace journalistic leaks.

The first time I heard the name firstfruits, years before the Snowden leak, a confidential source told me to search for it on the internet. All I turned up were ravings on blogs about spooky plots. The George W. Bush administration, according to these accounts, had an off-the-books spying program akin to the work of the East German Stasi. firstfruits allegedly listened in on journalists, political dissenters, members of Congress, and other threats to the globalist order. In some versions of the story, the program marked its victims for arrest or assassination. As best I

could tell, these stories all traced back to a series of posts by a man named Wayne Madsen, who has aptly been described as "a paranoid conspiracy theorist in the tradition of Alex Jones." I did a little bit of reading in these fever swamps and concluded that firstfruits was a crank's dark fantasy.

Then came the day I found my name in the Snowden archive. Sixteen documents, including the one that talked about me, named firstfruits as a counterintelligence database that tracked unauthorized disclosures in the news media. According to top-secret briefing materials prepared by Joseph J. Brand, a senior NSA official who was also among the leading advocates of a crackdown on leaks, firstfruits got its name from the phrase *the fruits of our labor*. "Adversaries know more about SIGINT sources & methods today than ever before," Brand wrote. Some damaging disclosures came from the U.S. government's own official communications, he noted; other secrets were acquired by foreign spies. But "most often," Brand wrote, "these disclosures occur through the media." He listed four "flagrant media leakers": the *Post*, *The New York Times*, *The New Yorker*, and *The Washington Times*. The firstfruits project aimed to "drastically reduce significant losses of collection capability" at journalists' hands.

In NSA parlance, exposure of a source or method of surveillance is a "cryptologic insecurity." If exposure leads to loss of intelligence collection, that is "impairment." I was fully prepared to believe that some leaks cause impairment, but Brand's accounting—like many of the government's public assertions—left something to be desired.

By far the most frequent accusation invoked in debates about whether journalists cause "impairment" to the U.S. government is that it was journalists' fault that the U.S. lost access to Osama bin Laden's satellite-phone communications in the late 1990s. It is hard to overstate the centrality of this episode to the intelligence community's lore about the news media. The accusation, as best as I can ascertain, was first made publicly in 2002 by then–White House Press Secretary Ari Fleischer. After a newspaper reported that the NSA could listen to Osama bin Laden on his satellite phone, as Fleischer put it, the al-Qaeda leader abandoned the device. President Bush and a long line of other officials reprised this assertion in the years to come.

But the tale of the busted satellite-phone surveillance is almost certainly untrue. The story in question said nothing about U.S. eavesdropping. And one day before it was published, the United States launched barrages of cruise missiles against al-Qaeda training camps in Afghanistan and a factory in Sudan, including a facility that bin Laden had recently visited. After this, bin Laden went deep underground, forswearing electronic communications that might give his location away. Blaming a news story for this development, rather than a close miss on bin Laden's life, strained all logic. Yet somehow it became an article of faith in the intelligence community.

In 2001, according to Brand's NSA documents, the agency "stood up" a staff of leak trackers, and the CIA director hired a contractor "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."

The firstfruits project produced 49 “crime reports to DOJ,” three of them involving me. The FBI, in turn, was left with a conundrum. What crime, exactly, was it being asked to investigate? Congress has never passed a law that squarely addresses unauthorized disclosures to reporters by public officials. The United States has no counterpart to the United Kingdom’s Official Secrets Act. Government employees sign a pledge to protect classified information; if they break that pledge, they can lose their security clearance or their job. Those are civil penalties. When it comes to criminal law, they may be subject to 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.

Some people will see a kind of sense in that. A secret has been spilled, and damage potentially done. From the NSA’s point of view, a loss is a loss, regardless of whether a foreign adversary learns the secret from a spy or a published news report. Before the disclosure, the NSA had a valuable source or method. Afterward, it does not.

But in other ways, espionage is a terrible fit for a news-media leak. Talking to a journalist is hardly tantamount to spying. Spies steal American secrets on behalf of some other country. They hope our government, and the general public, never learn of the breach. They intend, as the Espionage Act defines the crime, for the information “to be used to the injury of the United States or to the advantage of [a] foreign nation.” News sources, on the other hand, give information to reporters for the purpose of exposure to the public at large. They want everyone to know. They may have self-interested motives, but they commonly

believe, rightly or wrongly, that their fellow citizens will benefit from the leak.

Yes, news sources have on occasion been tried and convicted of espionage—but in general forcing a whistleblower into the mold of a spy is disfiguring. If news is espionage, then George Ellard is right to call me an “agent” of the adversary, and James Clapper is right to call me an “accomplice.” From that basis, deploying the government’s most intrusive counterintelligence powers against a journalist is but a short step.

I’ve thought a lot over the years about what the public’s “right to know” is in the context of national security. Clearly there are circumstances in which the careful journalistic disclosure of certain classified facts is the right thing to do.

What if the U.S. government deliberately exposed American troops to nuclear radiation in order to learn more about the medical effects? That really happened after World War II, and the public didn’t learn about it until 1994. If reporters had known the truth in the ’40s and ’50s, should they have suppressed it?

What about if the U.S. government deliberately infected sex workers in Guatemala with gonorrhea and syphilis? That happened too, in wildly unethical experiments from 1946 to 1948, which the government did not fully acknowledge until 2010.

Homeland Security had produced a 76-page report of every international flight I’d taken since 1983. Customs inspectors had secretly searched my checked baggage. Government spokesmen were forwarding my emails to the FBI.

What if a classified military investigation found “numerous incidents of sadistic, blatant, and wanton criminal abuses” against foreign detainees, in violation of the Geneva Conventions and the Uniform Code of Military Justice? That happened at the Abu Ghraib prison in 2003. Much the same sequence of events, with classification stamps employed to conceal information that public officials could not or did not wish to justify, took place after the government tortured al-Qaeda suspects in secret prisons, authorized warrantless surveillance of U.S. citizens, and lied about intelligence on weapons of mass destruction in Iraq. These were history-making events, full of political and legal repercussions, but they were hidden from public scrutiny until news stories broke through barriers of classification.

At heart, national-security secrecy presents a conflict of core values: self-government and self-defense. If we do not know what our government is doing, we cannot hold it accountable. If we do know, our enemies know too. That can be dangerous. This is our predicament. Wartime heightens the case for secrecy because the value of security is at its peak. But secrecy is never more damaging to self-government than in wartime, because making war is the very paradigm of a political choice.

But our government clearly doesn’t see it that way. Here are some facts I’ve learned, through Freedom of Information Act requests and a lawsuit I filed to enforce them, about various government actions that involve me. The Office of the Director of National Intelligence said it had completely withheld 435 documents about me, but its explanation was classified and my lawyers at the Reporters Committee for Freedom of the Press were not allowed to read it. Homeland Security personnel, I

learned from one document, had produced a 76-page report of every international flight I'd taken since 1983. Customs inspectors had secretly searched my checked baggage when I returned from more than one overseas reporting trip. The reasons for and results of those searches were redacted. Hundreds of emails recorded behind-the-scenes reactions and internal debates about how to respond to my questions or stories. The government asked the court to withhold all of those on grounds of deliberative privilege.

I learned something else by way of FOIA. It turned out, according to internal government correspondence I received in the course of my lawsuit, that government spokesmen were forwarding my emails to the FBI. The NSA public-affairs shop subsumed its work entirely to law enforcement. The spokesmen did not even have to be asked. They volunteered. "Below please find correspondence between reporter Bart Gellman and NSA & ODNI public affairs," a senior intelligence official, whose name is redacted in the FOIA release, wrote on December 21, 2013, to a manager in the Office of the National Counterintelligence Executive, or NCIX. "In the email, Gellman references conversations he has with Edward Snowden … Are these emails useful for NCIX?"

The manager replied, "Yes, these types of correspondence are useful. We will ensure they get to the FBI investigations team."

According to an affidavit from David M. Hardy, the section chief in the FBI's Information Management Division, my name appears in files relating to "investigations of alleged federal criminal violations and counterterrorism, counterintelligence investigations of third party subjects." Not only the Snowden

case, that is—*investigations* and *third-party subjects*, plural. Some of those files, Hardy said, may appear in an electronic-surveillance database that includes "all persons whose voices have been monitored." Turns out I wasn't being paranoid.

Equally unsettling were the redactions themselves and the reasons given for them. Even the names of the FBI files, Hardy told the court, would give too much away. The file names specify "non-public investigative techniques" and "non-public details about techniques and procedures that are otherwise known to the public." The FBI is especially concerned about protecting one unspecified intelligence-gathering method. "Its use in the specific context of this investigative case is not a publically known fact," Hardy wrote. The bureau wants to protect "the nature of the information gleaned by its use."

Those are not comforting words.

---

*This article was adapted from Barton Gellman's book* Dark Mirror: Edward Snowden and the American Surveillance State *(Penguin Press). It appears in the June 2020 print edition with the headline "Operation FIRSTFRUITS."*

Barton Gellman is a staff writer at *The Atlantic* and author of *Dark Mirror: Edward Snowden and the American Surveillance State* and *Angler: The Cheney Vice Presidency*.