THE NEW YORKER

A REPORTER AT LARGE

THE SECRET SHARER

Is Thomas Drake an enemy of the state?

BY JANE MAYER

MAY 23, 2011

Drake, a former senior executive at the National Security Agency, faces some of the gravest charges that can be brought against an American citizen. Photograph by Martin Schoeller.

On June 13th, a fifty-four-year-old former government employee named Thomas Drake is scheduled to appear in a courtroom in Baltimore, where he will face some of the gravest charges that can be brought against an American citizen. A former senior executive at the National Security Agency, the government's electronic-espionage service, he is accused, in essence, of being an enemy of the state. According to a ten-count indictment delivered against him in April, 2010, Drake violated the Espionage Act—the 1917 statute that was used to convict Aldrich Ames, the C.I.A. officer who, in the eighties and nineties, sold U.S. intelligence to the K.G.B., enabling the Kremlin to assassinate informants. In 2007, the indictment says, Drake willfully retained top-secret defense documents that he had sworn an oath to protect, sneaking them out of the intelligence agency's headquarters, at Fort Meade, Maryland, and taking them home, for the purpose of "unauthorized disclosure." The aim of this scheme, the indictment says, was to leak government secrets to an unnamed newspaper reporter, who is identifiable as Siobhan Gorman, of the Baltimore *Sun*. Gorman wrote a prize-winning series of articles for the *Sun* about financial waste, bureaucratic dysfunction, and dubious legal practices in N.S.A. counterterrorism programs. Drake is also charged with obstructing justice and lying to federal law-enforcement agents. If he is convicted on all counts, he could receive a prison term of thirty-five years.

The government argues that Drake recklessly endangered the lives of American servicemen.

"This is not an issue of benign documents," William M. Welch II, the senior litigation counsel who is prosecuting the case, argued at a hearing in March, 2010. The N.S.A., he went on, collects "intelligence for the soldier in the field. So when individuals go out and they harm that ability, our intelligence goes dark and our soldier in the field gets harmed."

Top officials at the Justice Department describe such leak prosecutions as almost obligatory. Lanny Breuer, the Assistant Attorney General who supervises the department's criminal division, told me, "You don't get to break the law and disclose classified information just because you want to." He added, "Politics should play no role in it whatsoever."

When President Barack Obama took office, in 2009, he championed the cause of government transparency, and spoke admiringly of whistle-blowers, whom he described as "often the best source of information about waste, fraud, and abuse in government." But the Obama Administration has pursued leak prosecutions with a surprising relentlessness. Including the Drake case, it has been using the Espionage Act to press criminal charges in five alleged instances of national-security leaks—more such prosecutions than have occurred in all previous Administrations combined. The Drake case is one of two that Obama's Justice Department has carried over from the Bush years.

Gabriel Schoenfeld, a conservative political scientist at the Hudson Institute, who, in his book "Necessary Secrets" (2010), argues for more stringent protection of classified information, says, "Ironically, Obama has presided over the most draconian crackdown on leaks in our history—even more so than Nixon."

"Yes, but Mummy and Daddy are on legal drugs."

One afternoon in January, Drake met with me, giving his first public interview about this case. He is tall, with thinning sandy hair framing a domed forehead, and he has the erect bearing of a member of the Air Force, where he served before joining the N.S.A., in 2001. Obsessive, dramatic, and emotional, he has an unwavering belief in his own rectitude. Sitting at a Formica table at the Tastee Diner, in Bethesda, Drake—who is a registered Republican—groaned and thrust his head into his hands. "I actually had hopes for Obama," he said. He had not only expected the President to roll back the prosecutions launched by the Bush Administration; he had thought that Bush Administration officials would be investigated for overstepping the law in the "war on terror."

"But power is incredibly destructive," Drake said. "It's a weird, pathological thing. I also think

the intelligence community coöpted Obama, because he's rather naïve about national security. He's accepted the fear and secrecy. We're in a scary space in this country."

The Justice Department's indictment narrows the frame around Drake's actions, focussing almost exclusively on his handling of what it claims are five classified documents. But Drake sees his story as a larger tale of political reprisal, one that he fears the government will never allow him to air fully in court. "I'm a target," he said. "I've got a bull's-eye on my back." He continued, "I did not tell secrets. I am facing prison for having raised an alarm, period. I went to a reporter with a few key things: fraud, waste, and abuse, and the fact that there were legal alternatives to the Bush Administration's 'dark side' "—in particular, warrantless domestic spying by the N.S.A.

The indictment portrays him not as a hero but as a treacherous man who violated "the government trust." Drake said of the prosecutors, "They can say what they want. But the F.B.I. can find something on anyone."

Steven Aftergood, the director of the Project on Government Secrecy at the Federation of American Scientists, says of the Drake case, "The government wants this to be about unlawfully retained information. The defense, meanwhile, is painting a picture of a public-interested whistle-blower who struggled to bring attention to what he saw as multibillion-dollar mismanagement." Because Drake is not a spy, Aftergood says, the case will "test whether intelligence officers can be convicted of violating the Espionage Act even if their intent is pure." He believes that the trial may also test whether the nation's expanding secret intelligence bureaucracy is beyond meaningful accountability. "It's a much larger debate than whether a piece of paper was at a certain place at a certain time," he says.

Jack Balkin, a liberal law professor at Yale, agrees that the increase in leak prosecutions is part of a larger transformation. "We are witnessing the bipartisan normalization and legitimization of a national-surveillance state," he says. In his view, zealous leak prosecutions are consonant with other political shifts since 9/11: the emergence of a vast new security bureaucracy, in which at least two and a half million people hold confidential, secret, or top-secret clearances; huge expenditures on electronic monitoring, along with a reinterpretation of the law in order to sanction it; and corporate partnerships with the government that have transformed the counterterrorism industry into a powerful lobbying force. Obama, Balkin says, has "systematically adopted policies consistent with the second term of the Bush Administration."

On March 28th, Obama held a meeting in the White House with five advocates for greater transparency in government. During the discussion, the President drew a sharp distinction between whistle-blowers who exclusively reveal wrongdoing and those who jeopardize national security. The importance of maintaining secrecy about the impending raid on Osama bin Laden's compound was likely on Obama's mind. The White House has been particularly bedevilled by the ongoing release of classified documents by WikiLeaks, the group led by Julian Assange. Last year, WikiLeaks began releasing a vast trove of sensitive government documents allegedly leaked by a

U.S. soldier, Bradley Manning; the documents included references to a courier for bin Laden who had moved his family to Abbottabad—the town where bin Laden was hiding out. Manning has been charged with "aiding the enemy."

Danielle Brian, the executive director of the Project on Government Oversight, attended the meeting, and said that Obama's tone was generally supportive of transparency. But when the subject of national-security leaks came up, Brian said, "the President shifted in his seat and leaned forward. He said this may be where we have some differences. He said he doesn't want to protect the people who leak to the media war plans that could impact the troops." Though Brian was impressed with Obama's over-all stance on transparency, she felt that he might be misinformed about some of the current leak cases. She warned Obama that prosecuting whistle-blowers would undermine his legacy. Brian had been told by the White House to avoid any "ask"s on specific issues, but she told the President that, according to his own logic, Drake was exactly the kind of whistle-blower who deserved protection.

As Drake tells it, his problems began on September 11, 2001. "The next seven weeks were crucial," he said. "It's foundational to why I am a criminal defendant today."

The morning that Al Qaeda attacked the U.S. was, coincidentally, Drake's first full day of work as a civilian employee at the N.S.A.—an agency that James Bamford, the author of "The Shadow Factory" (2008), calls "the largest, most costly, and most technologically sophisticated spy organization the world has ever known." Drake, a linguist and a computer expert with a background in military crypto-electronics, had worked for twelve years as an outside contractor at the N.S.A. Under a program code-named Jackpot, he focussed on finding and fixing weaknesses in the agency's software programs. But, after going through interviews and background checks, he began working full time for Maureen Baginski, the chief of the Signals Intelligence Directorate at the N.S.A., and the agency's third-highest-ranking official.

Even in an age in which computerized feats are commonplace, the N.S.A.'s capabilities are breathtaking. The agency reportedly has the capacity to intercept and download, every six hours, electronic communications equivalent to the contents of the Library of Congress. Three times the size of the C.I.A., and with a third of the U.S.'s entire intelligence budget, the N.S.A. has a five-thousand-acre campus at Fort Meade protected by iris scanners and facial-recognition devices. The electric bill there is said to surpass seventy million dollars a year.

Nevertheless, when Drake took up his post the agency was undergoing an identity crisis. With the Cold War over, the agency's mission was no longer clear. As Drake puts it, "Without the Soviet Union, it didn't know what to do." Moreover, its technology had failed to keep pace with the shift in communications to cellular phones, fibre-optic cable, and the Internet. Two assessments commissioned by General Michael Hayden, who took over the agency in 1999, had drawn devastating conclusions. One described the N.S.A. as "an agency mired in bureaucratic conflict"

and "suffering from poor leadership." In January, 2000, the agency's computer system crashed for three and a half days, causing a virtual intelligence blackout.

Agency leaders decided to "stir up the gene pool," Drake says. Although his hiring was meant to signal fresh thinking, he was given a clumsy bureaucratic title: Senior Change Leader/Chief, Change Leadership & Communications Office, Signals Intelligence Directorate.

The 9/11 attacks caught the U.S.'s national-security apparatus by surprise. N.S.A. officials were humiliated to learn that the Al Qaeda hijackers had spent their final days, undetected, in a motel in Laurel, Maryland—a few miles outside the N.S.A.'s fortified gates. They had bought a folding knife at a Target on Fort Meade Road. Only after the attacks did agency officials notice that, on September 10th, their surveillance systems had intercepted conversations in Afghanistan and Saudi Arabia warning that "the match begins tomorrow" and "tomorrow is Zero Hour."

Drake, hoping to help fight back against Al Qaeda, immediately thought of a tantalizing secret project he had come across while working on Jackpot. Code-named ThinThread, it had been developed by technological wizards in a kind of Skunk Works on the N.S.A. campus. Formally, the project was supervised by the agency's Signals Intelligence Automation Research Center, or SARC.

While most of the N.S.A. was reeling on September 11th, inside SARC the horror unfolded "almost like an 'I-told-you-so' moment," according to J. Kirk Wiebe, an intelligence analyst who worked there. "We knew we weren't keeping up." SARC was led by a crypto-mathematician named Bill Binney, whom Wiebe describes as "one of the best analysts in history." Binney and a team of some twenty others believed that they had pinpointed the N.S.A.'s biggest problem—data overload—and then solved it. But the agency's management hadn't agreed.

Binney, who is six feet three, is a bespectacled sixty-seven-year-old man with wisps of dark hair; he has the quiet, tense air of a preoccupied intellectual. Now retired and suffering gravely from diabetes, which has already claimed his left leg, he agreed recently to speak publicly for the first time about the Drake case. When we met, at a restaurant near N.S.A. headquarters, he leaned crutches against an extra chair. "This is too serious not to talk about," he said.

Binney expressed terrible remorse over the way some of his algorithms were used after 9/11. ThinThread, the "little program" that he invented to track enemies outside the U.S., "got twisted," and was used for both foreign and domestic spying: "I should apologize to the American people. It's violated everyone's rights. It can be used to eavesdrop on the whole world." According to Binney, Drake took his side against the N.S.A.'s management and, as a result, became a political target within the agency.

Binney spent most of his career at the agency. In 1997, he became the technical director of the World Geopolitical and Military Analysis Reporting Group, a division of six thousand employees which focusses on analyzing signals intelligence. By the late nineties, the N.S.A. had become overwhelmed by the amount of digital data it was collecting. Binney and his team began

developing codes aimed at streamlining the process, allowing the agency to isolate useful intelligence. This was the beginning of ThinThread.

In the late nineties, Binney estimated that there were some two and a half billion phones in the world and one and a half billion I.P. addresses. Approximately twenty terabytes of unique information passed around the world every minute. Binney started assembling a system that could trap and map all of it. "I wanted to graph the world," Binney said. "People said, 'You can't do this—the possibilities are infinite.' " But he argued that "at any given point in time the number of atoms in the universe is big, but it's finite."

As Binney imagined it, ThinThread would correlate data from financial transactions, travel records, Web searches, G.P.S. equipment, and any other "attributes" that an analyst might find useful in pinpointing "the bad guys." By 2000, Binney, using fibre optics, had set up a computer network that could chart relationships among people in real time. It also turned the N.S.A.'s data-collection paradigm upside down. Instead of vacuuming up information around the world and then sending it all back to headquarters for analysis, ThinThread processed information as it was collected—discarding useless information on the spot and avoiding the overload problem that plagued centralized systems. Binney says, "The beauty of it is that it was open-ended, so it could keep expanding."

Pilot tests of ThinThread proved almost too successful, according to a former intelligence expert who analyzed it. "It was nearly perfect," the official says. "But it processed such a large amount of data that it picked up more Americans than the other systems." Though ThinThread was intended to intercept foreign communications, it continued documenting signals when a trail crossed into the U.S. This was a big problem: federal law forbade the monitoring of domestic communications without a court warrant. And a warrant couldn't be issued without probable cause and a known suspect. In order to comply with the law, Binney installed privacy controls and added an "anonymizing feature," so that all American communications would be encrypted until a warrant was issued. The system would indicate when a pattern looked suspicious enough to justify a warrant.

But this was before 9/11, and the N.S.A.'s lawyers deemed ThinThread too invasive of Americans' privacy. In addition, concerns were raised about whether the system would function on a huge scale, although preliminary tests had suggested that it would. In the fall of 2000, Hayden decided not to use ThinThread, largely because of his legal advisers' concerns. Instead, he funded a rival approach, called Trailblazer, and he turned to private defense contractors to build it. Matthew Aid, the author of a heralded 2009 history of the agency, "The Secret Sentry," says, "The resistance to ThinThread was just standard bureaucratic politics. ThinThread was small, cost-effective, easy to understand, and protected the identity of Americans. But it wasn't what the higher-ups wanted. They wanted a big machine that could make Martinis, too."

The N.S.A.'s failure to stop the 9/11 plot infuriated Binney: he believed that ThinThread had

been ready to deploy nine months earlier. Working with N.S.A. counterterrorism experts, he had planned to set up his system at sites where foreign terrorism was prevalent, including Afghanistan and Pakistan. "Those bits of conversations they found too late?" Binney said. "That would have never happened. I had it managed in a way that would send out automatic alerts. It would have been, Bang!"

Meanwhile, there was nothing to show for Trailblazer, other than mounting bills. As the system stalled at the level of schematic drawings, top executives kept shuttling between jobs at the agency and jobs with the high-paying contractors. For a time, both Hayden's deputy director and his chief of signals-intelligence programs worked at SAIC, a company that won several hundred million dollars in Trailblazer contracts. In 2006, Trailblazer was abandoned as a $1.2-billion flop.

Soon after 9/11, Drake says, he prepared a short, classified summary explaining how ThinThread "could be put into the fight," and gave it to Baginski, his boss. But he says that she "wouldn't respond electronically. She just wrote in a black felt marker, 'They've found a different solution.' " When he asked her what it was, she responded, "I can't tell you." Baginski, who now works for a private defense contractor, recalls her interactions with Drake differently, but she declined to comment specifically.

In the weeks after the attacks, rumors began circulating inside the N.S.A. that the agency, with the approval of the Bush White House, was violating the Foreign Intelligence Surveillance Act—the 1978 law, known as FISA, that bars domestic surveillance without a warrant. Years later, the rumors were proved correct. In nearly total secrecy, and under pressure from the White House, Hayden sanctioned warrantless domestic surveillance. The new policy, which lawyers in the Justice Department justified by citing President Bush's executive authority as Commander-in-Chief, contravened a century of constitutional case law. Yet, on October 4, 2001, Bush authorized the policy, and it became operational by October 6th. Bamford, in "The Shadow Factory," suggests that Hayden, having been overcautious about privacy before 9/11, swung to the opposite extreme after the attacks. Hayden, who now works for a security-consulting firm, declined to respond to detailed questions about the surveillance program.

When Binney heard the rumors, he was convinced that the new domestic-surveillance program employed components of ThinThread: a bastardized version, stripped of privacy controls. "It was my brainchild," he said. "But they removed the protections, the anonymization process. When you remove that, you can target anyone." He said that although he was not "read in" to the new secret surveillance program, "my people were brought in, and they told me, 'Can you believe they're doing this? They're getting billing records on U.S. citizens! They're putting pen registers' "—logs of dialled phone numbers—" 'on everyone in the country!' "

Drake recalled that, after the October 4th directive, "strange things were happening. Equipment was being moved. People were coming to me and saying, 'We're now targeting our own country!'

" Drake says that N.S.A. officials who helped the agency obtain FISA warrants were suddenly reassigned, a tipoff that the conventional process was being circumvented. He added, "I was concerned that it was illegal, and none of it was necessary." In his view, domestic data mining "could have been done legally" if the N.S.A. had maintained privacy protections. "But they didn't want an accountable system."

Aid, the author of the N.S.A. history, suggests that ThinThread's privacy protections interfered with top officials' secret objective—to pick American targets by name. "They wanted selection, not just collection," he says.

A former N.S.A. official expressed skepticism that Drake cared deeply about the constitutional privacy issues raised by the agency's surveillance policies. The official characterizes him as a bureaucrat driven by resentment of a rival project—Trailblazer—and calls his story "revisionist history." But Drake says that, in the fall of 2001, he told Baginski he feared that the agency was breaking the law. He says that to some extent she shared his views, and later told him she feared that the agency would be "haunted" by the surveillance program. In 2003, she left the agency for the F.B.I., in part because of her discomfort with the surveillance program. Drake says that, at one point, Baginski told him that if he had concerns he should talk to the N.S.A.'s general counsel. Drake claims that he did, and that the agency's top lawyer, Vito Potenza, told him, "Don't worry about it. We're the executive agent for the White House. It's all been scrubbed. It's legal." When he pressed further, Potenza told him, "It's none of your business." (Potenza, who is now retired, declined to comment.)

Drake says, "I feared for the future. If Pandora's box was opened, what would the government become?" He was not about to drop the matter. Matthew Aid, who describes Drake as "brilliant," says that "he has sort of a Jesus complex—only he can see the way things are. Everyone else is mentally deficient, or in someone's pocket." Drake's history of whistle-blowing stretches back to high school, in Manchester, Vermont, where his father, a retired Air Force officer, taught. When drugs infested the school, Drake became a police informant. And Watergate, which occurred while he was a student, taught him "that no one is above the law."

Drake says that in the Air Force, where he learned to capture electronic signals, the FISA law "was drilled into us." He recalls, "If you accidentally intercepted U.S. persons, there were special procedures to expunge it." The procedures had been devised to prevent the recurrence of past abuses, such as Nixon's use of the N.S.A. to spy on his political enemies.

Drake didn't know the precise details, but he sensed that domestic spying "was now being done on a vast level." He was dismayed to hear from N.S.A. colleagues that "arrangements" were being made with telecom and credit-card companies. He added, "The mantra was 'Get the data!' " The transformation of the N.S.A., he says, was so radical that "it wasn't just that the brakes came off after 9/11—we were in a whole different vehicle."

Few people have a precise knowledge of the size or scope of the N.S.A.'s domestic-surveillance powers. An agency spokesman declined to comment on how the agency "performs its mission," but said that its activities are constitutional and subject to "comprehensive and rigorous" oversight. But Susan Landau, a former engineer at Sun Microsystems, and the author of a new book, "Surveillance or Security?," notes that, in 2003, the government placed equipment capable of copying electronic communications at locations across America. These installations were made, she says, at "switching offices" that not only connect foreign and domestic communications but also handle purely domestic traffic. As a result, she surmises, the U.S. now has the capability to monitor domestic traffic on a huge scale. "Why was it done this way?" she asks. "One can come up with all sorts of nefarious reasons, but one doesn't want to think that way about our government."

Binney, for his part, believes that the agency now stores copies of all e-mails transmitted in America, in case the government wants to retrieve the details later. In the past few years, the N.S.A. has built enormous electronic-storage facilities in Texas and Utah. Binney says that an N.S.A. e-mail database can be searched with "dictionary selection," in the manner of Google. After 9/11, he says, "General Hayden reassured everyone that the N.S.A. didn't put out dragnets, and that was true. It had no need—it was getting every fish in the sea."

Binney considers himself a conservative, and, as an opponent of big government, he worries that the N.S.A.'s data-mining program is so extensive that it could help "create an Orwellian state." Whereas wiretap surveillance requires trained human operators, data mining is automated, meaning that the entire country can be watched. Conceivably, U.S. officials could "monitor the Tea Party, or reporters, whatever group or organization you want to target," he says. "It's exactly what the Founding Fathers never wanted."

On October 31, 2001, soon after Binney concluded that the N.S.A. was headed in an unethical direction, he retired. He had served for thirty-six years. His wife worked there, too. Wiebe, the analyst, and Ed Loomis, a computer scientist at SARC, also left. Binney said of his decision, "I couldn't be an accessory to subverting the Constitution."

Not long after Binney quit the N.S.A., he says, he confided his concerns about the secret surveillance program to Diane Roark, a staff member on the House Permanent Select Committee on Intelligence, which oversees the agency. Roark, who has flowing gray hair and large, wide-set eyes, looks like a waifish poet. But in her intelligence-committee job, which she held for seventeen years, she modelled herself on Machiavelli's maxim that it is better to be feared than loved. Within the N.S.A.'s upper ranks she was widely resented. A former top N.S.A. official says of her, "In meetings, she would just say, 'You're lying.' "

Roark agrees that she distrusted the N.S.A.'s managers. "I asked very tough questions, because they were trying to hide stuff," she says. "For instance, I wasn't supposed to know about the warrantless surveillance. They were all determined that no one else was going to tell them what to

do."

Like Drake and Binney, Roark was a registered Republican, skeptical about bureaucracy but strong on national defense. She had a knack for recruiting sources at the N.S.A. One of them was Drake, who introduced himself to her in 2000, after she visited N.S.A. headquarters and gave a stinging talk on the agency's failings; she also established relationships with Binney and Wiebe. Hayden was furious about this back channel. After learning that Binney had attended a meeting with Roark at which N.S.A. employees complained about Trailblazer, Hayden dressed down the critics. He then sent out an agency-wide memo, in which he warned that several "individuals, in a session with our congressional overseers, took a position in direct opposition to one that we had corporately decided to follow. . . . Actions contrary to our decisions will have a serious adverse effect on our efforts to transform N.S.A., and I cannot tolerate them." Roark says of the memo, "Hayden brooked no opposition to his favorite people and programs."

Roark, who had substantial influence over N.S.A. budget appropriations, was an early champion of Binney's ThinThread project. She was dismayed, she says, to hear that it had evolved into a means of domestic surveillance, and felt personally responsible. Her oversight committee had been created after Watergate specifically to curb such abuses. "It was my duty to oppose it," she told me. "That is why oversight existed, so that these things didn't happen again. I'm not an attorney, but I thought that there was no way it was constitutional." Roark recalls thinking that, if N.S.A. officials were breaking the law, she was "going to fry them."

She soon learned that she was practically alone in her outrage. Very few congressional leaders had been briefed on the program, and some were apparently going along with it, even if they had reservations. Starting in February, 2002, Roark says, she wrote a series of memos warning of potential illegalities and privacy breaches and handed them to the staffers for Porter Goss, the chairman of her committee, and Nancy Pelosi, its ranking Democrat. But nothing changed. (Pelosi's spokesman denied that she received such memos, and pointed out that a year earlier Pelosi had written to Hayden and expressed grave concerns about the N.S.A.'s electronic surveillance.)

Roark, feeling powerless, retired. Before leaving Washington, though, she learned that Hayden, who knew of her strong opposition to the surveillance program, wanted to talk to her. They met at N.S.A. headquarters on July 15, 2002. According to notes that she made after the meeting, Hayden pleaded with her to stop agitating against the program. He conceded that the policy would leak at some point, and told her that when it did she could "yell and scream" as much as she wished. Meanwhile, he wanted to give the program more time. She asked Hayden why the N.S.A. had chosen not to include privacy protections for Americans. She says that he "kept not answering. Finally, he mumbled, and looked down, and said, 'We didn't need them. We had the power.' He didn't even look me in the eye. I was flabbergasted." She asked him directly if the government was getting warrants for domestic surveillance, and he admitted that it was not.

In an e-mail, Hayden confirmed that the meeting took place, but said that he recalled only its

"broad outlines." He noted that Roark was not "cleared to know about the expanded surveillance program, so I did not go into great detail." He added, "I assured her that I firmly believed that what N.S.A. was doing was effective, appropriate, and lawful. I also reminded her that the program's success depended on it remaining secret, that it was appropriately classified, and that any public discussion of it would have to await a later day."

During the meeting, Roark says, she warned Hayden that no court would uphold the program. Curiously, Hayden responded that he had already been assured by unspecified individuals that he could count on a majority of "the nine votes"—an apparent reference to the Supreme Court. According to Roark's notes, Hayden told her that such a vote might even be 7–2 in his favor.

Roark couldn't believe that the Supreme Court had been adequately informed of the N.S.A.'s transgressions, and she decided to alert Chief Justice William H. Rehnquist, sending a message through a family friend. Once again, there was no response. She also tried to contact a judge on the FISA court, in Washington, which adjudicates requests for warrants sanctioning domestic surveillance of suspected foreign agents. But the judge had her assistant refer the call to the Department of Justice, which had approved the secret program in the first place. Roark says that she even tried to reach David Addington, the legal counsel to Vice-President Dick Cheney, who had once been her congressional colleague. He never called back, and Addington was eventually revealed to be one of the prime advocates for the surveillance program.

"This was such a Catch-22," Roark says. "There was no one to go to." In October, 2003, feeling "profoundly depressed," she left Washington and moved to a small town in Oregon.

Drake was still working at the N.S.A., but he was secretly informing on the agency to Congress. In addition to briefing Roark, he had become an anonymous source for the congressional committees investigating intelligence failures related to 9/11. He provided Congress with top-secret documents chronicling the N.S.A.'s shortcomings. Drake believed that the agency had failed to feed other intelligence agencies critical information that it had collected before the attacks. Congressional investigators corroborated these criticisms, though they found greater lapses at the C.I.A. and the F.B.I.

Around this time, Drake recalls, Baginski warned him, "Be careful, Tom—they're looking for leakers." He found this extraordinary, and asked himself, "Telling the truth to congressional oversight committees is leaking?" But the N.S.A. has a rule requiring employees to clear any contact with Congress, and in the spring of 2002 Baginski told Drake, "It's time for you to find another job." He soon switched to a less sensitive post at the agency, the first of several.

As for Binney, he remained frustrated even in retirement about what he considered the misuse of ThinThread. In September, 2002, he, Wiebe, Loomis, and Roark filed what they thought was a confidential complaint with the Pentagon's Inspector General, extolling the virtues of the original ThinThread project and accusing the N.S.A. of wasting money on Trailblazer. Drake did not put his

name on the complaint, because he was still an N.S.A. employee. But he soon became involved in helping the others, who had become friends. He obtained documents aimed at proving waste, fraud, and abuse in the Trailblazer program.

The Inspector General's report, which was completed in 2005, was classified as secret, so only a few insiders could read what Drake describes as a scathing document. Possibly the only impact of the probe was to hasten the end of Trailblazer, whose budget overruns had become indisputably staggering. Though Hayden acknowledged to a Senate committee that the costs of the Trailblazer project "were greater than anticipated, to the tune of, I would say, hundreds of millions," most of the scandal's details remained hidden from the public.

In December, 2005, the N.S.A.'s culture of secrecy was breached by a stunning leak. The *Times* reporters James Risen and Eric Lichtblau revealed that the N.S.A. was running a warrantless wiretapping program inside the United States. The paper's editors had held onto the scoop for more than a year, weighing the propriety of publishing it. According to Bill Keller, the executive editor of the *Times,* President Bush pleaded with the paper's editors to not publish the story; Keller told *New York* that "the basic message was: You'll have blood on your hands." After the paper defied the Administration, Bush called the leak "a shameful act." At his command, federal agents launched a criminal investigation to identify the paper's source.

The *Times* story shocked the country. Democrats, including then Senator Obama, denounced the program as illegal and demanded congressional hearings. A FISA court judge resigned in protest. In March, 2006, Mark Klein, a retired A.T. & T. employee, gave a sworn statement to the Electronic Frontier Foundation, which was filing a lawsuit against the company, describing a secret room in San Francisco where powerful Narus computers appeared to be sorting and copying all of the telecom's Internet traffic—both foreign and domestic. A high-capacity fibre-optic cable seemed to be forwarding this data to a centralized location, which, Klein surmised, was N.S.A. headquarters. Soon, *USA Today* reported that A.T. & T., Verizon, and BellSouth had secretly opened their electronic records to the government, in violation of communications laws. Legal experts said that each instance of spying without a warrant was a serious crime, and that there appeared to be hundreds of thousands of infractions.

President Bush and Administration officials assured the American public that the surveillance program was legal, although new legislation was eventually required to bring it more in line with the law. They insisted that the traditional method of getting warrants was too slow for the urgent threats posed by international terrorism. And they implied that the only domestic surveillance taking place involved tapping phone calls in which one speaker was outside the U.S.

Drake says of Bush Administration officials, "They were lying through their teeth. They had chosen to go an illegal route, and it wasn't because they had no other choice." He also believed that the Administration was covering up the full extent of the program. "The phone calls were the tip of

the iceberg. The really sensitive stuff was the data mining." He says, "I was faced with a crisis of conscience. What do I do—remain silent, and complicit, or go to the press?"

Drake has a wife and five sons, the youngest of whom has serious health problems, and so he agonized over the decision. He researched the relevant legal statutes and concluded that if he spoke to a reporter about unclassified matters the only risk he ran was losing his job. N.S.A. policy forbids initiating contact with the press. "I get that it's grounds for 'We have to let you go,' " he says. But he decided that he was willing to lose his job. "This was a violation of everything I knew and believed as an American. We were making the Nixon Administration look like pikers."

Drake got in touch with Gorman, who covered the N.S.A. for the Baltimore *Sun*. He had admired an article of hers and knew that Roark had spoken to her previously, though not about anything classified. He got Gorman's contact information from Roark, who warned him to be careful. She knew that in the past the N.S.A. had dealt harshly with people who embarrassed it.

Drake set up a secure Hushmail e-mail account and began sending Gorman anonymous tips. Half in jest, he chose the pseudonym The Shadow Knows. He says that he insisted on three ground rules with Gorman: neither he nor she would reveal his identity; he wouldn't be the sole source for any story; he would not supply her with classified information. But a year into the arrangement, in February, 2007, Drake decided to blow his cover, surprising Gorman by showing up at the newspaper and introducing himself as The Shadow Knows. He ended up meeting with Gorman half a dozen times. But, he says, "I never gave her anything classified." Gorman has not been charged with wrongdoing, and declined, through her lawyer, Laura Handman, to comment, citing the pending trial.

Starting on January 29, 2006, Gorman, who now works at the *Wall Street Journal*, published a series of articles about problems at the N.S.A., including a story describing Trailblazer as an expensive fiasco. On May 18, 2006, the day that Hayden faced Senate confirmation hearings for a new post—the head of the C.I.A.—the *Sun* published Gorman's exposé on ThinThread, which accused the N.S.A. of rejecting an approach that protected Americans' privacy. Hayden, evidently peeved, testified that intelligence officers deserved "not to have every action analyzed, second-guessed, and criticized on the front pages of the newspapers."

At the time, the government did not complain that the *Sun* had crossed a legal line. It did not contact the paper's editors or try to restrain the paper from publishing Gorman's work. A former N.S.A. colleague of Drake's says he believes that the *Sun* stories revealed government secrets. Others disagree. Steven Aftergood, the secrecy expert, says that the articles "did not damage national security."

Matthew Aid argues that the material Drake provided to the *Sun* should not have been highly classified—if it was—and in any case only highlighted that "the N.S.A. was a management nightmare, which wasn't a secret in Washington." In his view, Drake "was just saying, 'We're not doing our job, and it's having a deleterious effect on mission performance.' He was right, by the

way." The *Sun* series, Aid says, was "embarrassing to N.S.A. management, but embarrassment to the U.S. government is not a criminal offense in this country." (Aid has a stake in this debate. In 1984, when he was in the Air Force, he spent several months in the stockade for having stored classified documents in a private locker. The experience, he says, sensitized him to issues of government secrecy.)

While the *Sun* was publishing its series, twenty-five federal agents and five prosecutors were struggling to identify the *Times'* source. The team had targeted some two hundred possible suspects, but had found no culprits. The *Sun* series attracted the attention of the investigators, who theorized that its source might also have talked to the *Times*. This turned out not to be true. Nevertheless, the investigators quickly homed in on the Trailblazer critics. "It's sad," an intelligence expert says. "I think they were aiming at the *Times* leak and found this instead."

Roark was an obvious suspect for the *Times* leak. Everyone from Hayden on down knew that she had opposed the surveillance program. After the article appeared, she says, "I was waiting for the shoe to drop." The F.B.I. eventually contacted her, and in February, 2007, she and her attorney met with the prosecutor then in charge, Steven Tyrrell, who was the head of the fraud section at the Justice Department. Roark signed an affidavit saying that she was not a source for the *Times* story or for "State of War," a related book that James Risen wrote. She also swore that she had no idea who the source was. She says of the experience, "It was an interrogation, not an interview. They treated me like a target."

Roark recalls that the F.B.I. agents tried to force her to divulge the identity of her old N.S.A. informants. They already seemed to know about Drake, Binney, and Wiebe—perhaps from the Inspector General's report. She refused to coöperate, arguing that it was improper for agents of the executive branch to threaten a congressional overseer about her sources. "I had the sense that N.S.A. was egging the F.B.I. on," she says. "I'd gotten the N.S.A. so many times—they were going to get me. The N.S.A. hated me." (The N.S.A. and the Justice Department declined to comment on the investigations.)

In the months that followed, Roark heard nothing. Finally, her lawyer placed the case in her "dead file."

On July 26, 2007, at 9 A.M. Eastern Standard Time, armed federal agents simultaneously raided the houses of Binney, Wiebe, and Roark. (At Roark's house, in Oregon, it was six o'clock.) Binney was in the shower when agents arrived, and recalls, "They went right upstairs to the bathroom and held guns on me and my wife, right between the eyes." The agents took computer equipment, a copy of the Inspector General complaint and a copy of a commercial pitch that Binney had written with Wiebe, Loomis, and Roark. In 2001, the N.S.A. indicated to Binney that he could pursue commercial projects based on ThinThread. He and the others thought that aspects of the software could be used to help detect Medicare fraud.

Binney professed his innocence, and he says that the agents told him, "We think you're lying. You need to implicate someone. " He believed that they were trying to get him to name Roark as the *Times'* source. He suggested that if they were looking for criminal conspirators they should focus on Bush and Hayden for allowing warrantless surveillance. Binney recalls an agent responding that such brazen spying didn't happen in America. Looking over the rims of his owlish glasses, Binney replied, "Oh, really?"

Roark was sleeping when the agents arrived, and didn't hear them until "it sounded as if they were going to pull the house down, they were rattling it so badly." They took computers and a copy of the same commercial pitch. Her son had been interested in collaborating on the venture, and he, too, became a potential target. "They believed everybody was conspiring," Roark says. "For years, I couldn't talk to my own son without worrying that they'd say I was trying to influence his testimony." Although she has been fighting cancer, she has spoken with him only sparingly since the raid.

The agents seemed to think that the commercial pitch contained classified information. Roark was shaken: she and the others thought they had edited it scrupulously to insure that it did not. Agents also informed her that a few scattered papers in her old office files were classified. After the raid, she called her lawyer and asked, "If there's a disagreement on classification, does intent mean anything?" The question goes to the heart of the Drake case.

Roark, who always considered herself "a law-and-order person," said of the raid, "This changed my faith." Eventually, the prosecution offered her a plea bargain, under which she would plead guilty to perjury, for ostensibly lying to the F.B.I. about press leaks. The prosecutors also wanted her to testify against Drake. Roark refused. "I'm not going to plead guilty to deliberately doing anything wrong," she told them. "And I can't testify against Tom because I don't know that he did anything wrong. Whatever Tom revealed, I am sure that he did not think it was classified." She says, "I didn't think the system was perfect, but I thought they'd play fair with me. They didn't. I felt it was retribution."

Wiebe, the retired analyst, was the most surprised by the raid—he had not yet been contacted in connection with the investigation. He recalls that agents locked his two Pembroke Welsh corgis in a bathroom and commanded his daughter and his mother-in-law, who was in her bathrobe, to stay on a couch while they searched his house. He says, "I feel I'm living in the very country I worked for years to defeat: the Soviet Union. We're turning into a police state." Like Roark, he says of the raid, "It was retribution for our filing the Inspector General complaint."

Under the law, such complaints are confidential, and employees who file them are supposed to be protected from retaliation. It's unclear if the Trailblazer complaint tipped off authorities, but all four people who signed it became targets. Jesselyn Radack, of the Government Accountability Project, a whistle-blower advocacy group that has provided legal support to Drake, says of his case, "It's the most severe form of whistle-blower retaliation I have ever seen."

A few days after the raid, Drake met Binney and Wiebe for lunch, at a tavern in Glenelg, Maryland. "I had a pretty good idea I was next," Drake says. But it wasn't until the morning of November 28, 2007, that he saw armed agents streaming across his lawn. Though Drake was informed of his right to remain silent, he viewed the raid as a fresh opportunity to blow the whistle. He spent the day at his kitchen table, without a lawyer, talking. He brought up Trailblazer, but found that the investigators weren't interested in the details of a defunct computer system, or in cost overruns, or in the constitutional conflicts posed by warrantless surveillance. Their focus was on the *Times* leak. He assured them that he wasn't the source, but he confirmed his contact with the *Sun*, insisting that he had not relayed any classified information. He also disclosed his computer password. The agents bagged documents, computers, and books, and removed eight or ten boxes of office files from his basement. "I felt incredibly violated," he says.

For four months, Drake continued coöperating. He admitted that he had given Gorman information that he had cut and pasted from secret documents, but stressed that he had not included anything classified. He acknowledged sending Gorman hundreds of e-mails. Then, in April, 2008, the F.B.I. told him that someone important wanted to meet with him, at a secure building in Calverton, Maryland. Drake agreed to the appointment. Soon after he showed up, he says, Steven Tyrrell, the prosecutor, walked in and told him, "You're screwed, Mr. Drake. We have enough evidence to put you away for most of the rest of your natural life."

Prosecutors informed Drake that they had found classified documents in the boxes in his basement—the indictment cites three—and discovered two more in his e-mail archive. They also accused him of shredding other documents, and of deleting e-mails in the months before he was raided, in an attempt to obstruct justice. Further, they said that he had lied when he told federal agents that he hadn't given Gorman classified information.

"They had made me into an enemy of the state just by saying I was," Drake says. The boxes in his basement contained copies of some of the less sensitive material that he had procured for the Inspector General's Trailblazer investigation. The Inspector General's Web site directs complainants to keep copies. Drake says that if the boxes did, in fact, contain classified documents he didn't realize it. (The indictment emphasizes that he "willfully" retained documents.) The two documents that the government says it extracted from his e-mail archive were even less sensitive, Drake says. Both pertained to a successor to Trailblazer, code-named Turbulence. One document listed a schedule of meetings about Turbulence. It was marked "unclassified/for official use only" and posted on the N.S.A.'s internal Web site. The government has since argued that the schedule should have been classified, and that Drake should have known this. The other document, which touted the success of Turbulence, was officially declassified in July, 2010, three months after Drake was indicted. "After charging him with having this ostensibly serious classified document, the government waved a wand and decided it wasn't so classified after all," Radack says.

Clearly, the intelligence community hopes that the Drake case will send a message about the gravity of exposing government secrets. But Drake's lawyer, a federal public defender named James Wyda, argued in court last spring that "there have never been two documents so benign that are the subject of this kind of prosecution against a client whose motives are as salutary as Tom's."

Drake insists, too, that the only computer files he destroyed were routine trash: "I held then, and I hold now, I had nothing to destroy." Drake, who left the N.S.A. in 2008, and now works at an Apple Store outside Washington, asks, "Why didn't I erase everything on my computer, then? I know how to do it. They found what they found."

Not everyone familiar with Drake's case is moved by his plight. A former federal official knowledgeable about the case says, "To his credit, he tried to raise these issues, and, to an extent, they were dealt with. But who died and left him in charge?"

In May, 2009, Tyrrell proposed a plea bargain: if Drake pleaded guilty to one count of conspiring to violate the Espionage Act and agreed to coöperate against the others, he would get a maximum of five years in prison. "They wanted me to reveal a conspiracy that didn't exist," Drake says. "It was all about the *Times*, but I had no knowledge of the leak." Drake says that he told prosecutors, "I refuse to plea-bargain with the truth."

That June, Drake learned that Tyrrell was leaving the government. Tyrrell was a Republican, and Drake was hopeful that a prosecutor appointed by the Obama Administration would have a different approach. But Drake was dismayed to learn that Tyrrell's replacement, William Welch, had just been transferred from the top spot in the Justice Department's public-integrity section, after an overzealous prosecution of Ted Stevens, the Alaska senator. A judge had thrown out Stevens's conviction, and, at one point, had held Welch in contempt of court. (Welch declined to comment.)

In April, 2010, Welch indicted Drake, shattering his hope for a reprieve from the Obama Administration. But the prosecution's case had shrunk dramatically from the grand conspiracy initially laid out by Tyrrell. (Welch accidentally sent the defense team an early draft of the indictment, revealing how the case had changed.) Drake was no longer charged with leaking classified documents, or with being part of a conspiracy. He is still charged with violating the Espionage Act, but now merely because of unauthorized "willful retention" of the five documents. Drake says that when he learned that, even with the reduced charges, he still faced up to thirty-five years in prison, he "was completely aghast."

Morton Halperin, of the Open Society Institute, says that the reduced charges make the prosecution even more outlandish: "If Drake is convicted, it means the Espionage Law is an Official Secrets Act." Because reporters often retain unauthorized defense documents, Drake's conviction would establish a legal precedent making it possible to prosecute journalists as spies. "It poses a grave threat to the mechanism by which we learn most of what the government does,"

Halperin says.

The Espionage Act has rarely been used to prosecute leakers and whistle-blowers. Drake's case is only the fourth in which the act has been used to indict someone for mishandling classified material. "It was meant to deal with classic espionage, not publication," Stephen Vladeck, a law professor at American University who is an expert on the statute, says.

The first attempt to apply the law to leakers was the aborted prosecution, in 1973, of Daniel Ellsberg, a researcher at the RAND Corporation who was charged with disclosing the Pentagon Papers—a damning secret history of the Vietnam War. But the case was dropped, owing, in large part, to prosecutorial misconduct. The second such effort was the case of Samuel L. Morison, a naval intelligence officer who, in 1985, was convicted for providing U.S. photographs of a Soviet ship to *Jane's Defence Weekly*. Morison was later pardoned by Bill Clinton. The third case was the prosecution, in 2005, of a Defense Department official, Lawrence Franklin, and two lobbyists for the American-Israel Public Affairs Committee. Franklin pleaded guilty to a lesser charge, and the case against the lobbyists collapsed after the presiding judge insisted that prosecutors establish criminal intent. Unable to prove this, the Justice Department abandoned the case, amid criticism that the government had overreached.

Drake's case also raises questions about double standards. In recent years, several top officials accused of similar misdeeds have not faced such serious charges. John Deutch, the former C.I.A. director, and Alberto Gonzales, the former Attorney General, both faced much less stringent punishment after taking classified documents home without authorization. In 2003, Sandy Berger, Clinton's national-security adviser, smuggled classified documents out of a federal building, reportedly by hiding them in his pants. It was treated as a misdemeanor. His defense lawyer was Lanny Breuer—the official overseeing the prosecution of Drake.

Jack Goldsmith, a Harvard law professor who served in the Bush Justice Department, laments the lack of consistency in leak prosecutions. He notes that no investigations have been launched into the sourcing of Bob Woodward's four most recent books, even though "they are filled with classified information that he could only have received from the top of the government." Gabriel Schoenfeld, of the Hudson Institute, says, "The selectivity of the prosecutions here is nightmarish. It's a broken system."

Mark Feldstein, a professor of media and public affairs at George Washington University, warns that, if whistle-blowers and other dissenters are singled out for prosecution, "this has gigantic repercussions. You choke off the information that the public needs to judge policy."

Few people are more disturbed about Drake's prosecution than the others who spoke out against the N.S.A. surveillance program. In 2008, Thomas Tamm, a Justice Department lawyer, revealed that he was one of the people who leaked to the *Times*. He says of Obama, "It's so disappointing from someone who was a constitutional-law professor, and who made all those campaign

promises." The Justice Department recently confirmed that it won't pursue charges against Tamm. Speaking before Congress, Attorney General Holder explained that "there is a balancing that has to be done . . . between what our national-security interests are and what might be gained by prosecuting a particular individual." The decision provoked strong criticism from Republicans, underscoring the political pressures that the Justice Department faces when it backs off such prosecutions. Still, Tamm questions why the Drake case is proceeding, given that Drake never revealed anything as sensitive as what appeared in the *Times*. "The program he talked to the Baltimore *Sun* about was a failure and wasted billions of dollars," Tamm says. "It's embarrassing to the N.S.A., but it's not giving aid and comfort to the enemy."

Mark Klein, the former A.T. & T. employee who exposed the telecom-company wiretaps, is also dismayed by the Drake case. "I think it's outrageous," he says. "The Bush people have been let off. The telecom companies got immunity. The only people Obama has prosecuted are the whistle-blowers." ♦