GOVERNMENT SAYS IT DOESN’T LISTEN IN ON AMERICANS WITHOUT COURT ORDER

The following incidents say it does –

1) 1960’s and 1970’s - NSA eavesdropping on Americans, MLK and Anti-war types, as well as Senator Frank Church himself
2) Mark Klein, AT&T, and NSA Eavesdropping
3) David Murphee Faulk and Adrienne Kinne (Fort Gordon)
4) FBI Dir Mueller in testimony to the Senate on 30 Mar 2011.
5) Thomas Tamm – U.S. Dept. of Justice
6) Tim Clemente (ex FBI) on CNN
7) Russell Tice
8) LOVEINT
9) 60 Minutes – phone numbers reveal indexing
10) Bart Gellman article re FBI reading content supplied by NSA and its own operations
11) Gemalto SIM card manufacturer hacked by GCHQ and NSA
12) Clapper admits to “backdoor” warrantless searches of Americans
13) NSA acknowledges it does not need authorization to listen to phone calls
14) FOIA-ed “Five IGs” report – Page 8 – confirms NSA collected content
15) Michael Morrell confirms content collected in program other than Section 215
16) DHS Reveals Extensive Keyword List for Searching Data
17) Parallel Construction – DEA uses intercept to prosecute Americans (2 articles)
18) Govt sent the lawyers of Al Haramain copies of the classified transcripts of their phone conversations with their law firm members
19) National Security Agency discloses in secret Capitol Hill briefing that thousands of analysts can listen to domestic phone calls.

20) NSA Collects far more non-targeted than targeted entities

---------------------------------------------------

NSA Eavesdropping – Now and in 1960’s and 1970’s

http://www.washingtonpost.com/wpdyn/content/article/2005/12/31/AR2005123100808_pf.html

The Washington Post

NSA Gave Other U.S. Agencies Information From Surveillance

Fruit of Eavesdropping Was Processed and Cross-Checked With Databases

By Walter Pincus
Washington Post Staff Writer
Sunday, January 1, 2006

Information captured by the National Security Agency's secret eavesdropping on communications between the United States and overseas has been passed on to other government agencies, which cross-check the information with tips and information collected in other databases, current and former administration officials said.

The NSA has turned such information over to the Defense Intelligence Agency (DIA) and to other government entities, said three current and former senior administration officials, although it could not be determined which agencies received what types of information. Information from intercepts -- which typically includes records of telephone or e-mail
communications -- would be made available by request to agencies that are allowed to have it, including the FBI, DIA, CIA and Department of Homeland Security, one former official said.

At least one of those organizations, the DIA, has used NSA information as the basis for carrying out surveillance of people in the country suspected of posing a threat, according to two sources. A DIA spokesman said the agency does not conduct such domestic surveillance but would not comment further. Spokesmen for the FBI, the CIA and the director of national intelligence, John D. Negroponte, declined to comment on the use of NSA data.

Since the revelation last month that President Bush had authorized the NSA to intercept communications inside the United States, public concern has focused primarily on the legality of the NSA eavesdropping. Less attention has been paid to, and little is known about, how the NSA's information may have been used by other government agencies to investigate American citizens or to cross-check with other databases. In the 1960s and 1970s, the military used NSA intercepts to maintain files on U.S. peace activists, revelations of which prompted Congress to restrict the NSA from intercepting communications of Americans.

Today's NSA intercepts yield two broad categories of information, said a former administration official familiar with the program: "content," which would include transcripts of a phone call or e-mail, and "non-content," which would be records showing, for example, who in the United States was called by, or was calling, a number in another country thought to have a connection to a terrorist group. At the same time, NSA tries to limit identifying the names of Americans involved.

"NSA can make either type of information available to other [intelligence] agencies where relevant, but with appropriate masking of its origin," meaning that the source of the information and method of getting it would be concealed, the former official said.

Agencies that get the information can use it to conduct "data mining," or looking for patterns or matches with other databases that they maintain, which may or may not be specifically geared toward detecting terrorism threats, he said. "They are seeking to separate the known from the unknown, relationships or associations," he added.
The NSA would sometimes monitor telephones, e-mails or fax communications in cases where individuals in the United States -- and sometimes people they contacted -- were linked to an alleged foreign terrorist group, officials have said. The NSA, officials said, limited its decisions to follow-up with more electronic surveillance on an individual to those cases where there was some apparent link to terrorist sources.

But other agencies, one former official said, have used phone numbers or other records obtained from NSA in combination with wide-ranging databases to look for links and associations. "What data sets are included is a policy decision [made by individual agencies] when they involve other than terrorist links," he said.

DIA personnel stationed inside the United States went further on occasion, conducting physical surveillance of people or vehicles identified as a result of NSA intercepts, said two sources familiar with the operations, although the DIA said it does not conduct such activities.

The military personnel -- some of whose findings were reported to the Northern Command in Colorado -- were employed as part of the Pentagon's growing post-Sept. 11, 2001, domestic intelligence activity based on the need to protect Defense Department facilities and personnel from terrorist attacks, the sources said.

Northcom was set up in October 2002 to conduct operations to deter, prevent and defeat terrorist threats in the United States and its territories. The command runs two fusion centers that receive and analyze intelligence gathered by other government agencies.

Those Northcom centers conduct data mining, where information received from the NSA, the CIA, the FBI, state and local police, and the Pentagon's Talon system are cross-checked to see if patterns develop that could indicate terrorist activities.

Talon is a system that civilian and military personnel use to report suspicious activities around military installations. Information from these reports is fed into a database known as the Joint Protection Enterprise Network, which is managed, as is the Talon system, by the Counterintelligence Field Activity, the newest Defense Department intelligence agency to focus primarily on counterterrorism. The database is shared with intelligence and law enforcement agencies and was found last
month to have contained information about peace activists and others protesting the Iraq war that appeared to have no bearing on terrorism.

Military officials acknowledged that such information should have been purged after 90 days and that the Talon system was being reviewed.

Gen. Michael V. Hayden, deputy director for national intelligence and former head of NSA, told reporters last month that the interception of communications to the United States allegedly connected to terrorists was, in almost every case, of short duration. He also said that when the NSA creates intelligence reports based on information it collects, it minimizes the number of Americans whose identities are disclosed, doing so only when necessary.

"The same minimalizationist standards apply across the board, including for this program," he said of the domestic eavesdropping effort. "To make this very clear -- U.S. identities are minimized in all of NSA's activities, unless, of course, the U.S. identity is essential to understand the inherent intelligence value of the intelligence report." Hayden did not address the question of how long government agencies would archive or handle information from the NSA.

Today's controversy over the domestic NSA intercepts echoes events of more than three decades ago. Beginning in the late 1960s, the NSA was asked initially by the Johnson White House and later by the Army, the Secret Service, and the Bureau of Narcotics and Dangerous Drugs to intercept messages to or from the United States. Members of Congress were not informed of the program, code-named Minaret in one phase.

The initial purpose was to "help determine the existence of foreign influence" on "civil disturbances occurring throughout the nation," threats to the president and other issues, Gen. Lew Allen Jr., then director of NSA, told a Select Senate Committee headed by then-Sen. Frank Church (D-Idaho) in 1975.

Allen, in comments similar to recent Bush administration statements, said collecting communications involving American citizens was approved legally, by two attorneys general. He also said that the Minaret intercepts discovered "a major foreign terrorist act planned in a large city" and prevented "an assassination attempt on a prominent U.S. figure abroad."
Overall, Allen said that 1,200 Americans citizens' calls were intercepted over six years, and that about 1,900 reports were issued in three areas of terrorism. As the Church hearings later showed, the Army expanded the NSA collection and had units around the country gather names and license plates of those attending antiwar rallies and demonstrations. That, in turn, led to creation of files on these individuals within Army intelligence units. At one point a Senate Judiciary subcommittee showed the Army had amassed about 18,000 names. In response, Congress in 1978 passed the Foreign Intelligence Security Act, which limited NSA interception of calls from overseas to U.S. citizens or those involving American citizens traveling abroad.
Lawsuits over government surveillance languish

Associated Press

Mark Klein looks through documents while interviewed at his home in Alameda, Calif., Tuesday, June 11, 2013.


Before there was Edward Snowden and the leak of explosive documents showing widespread government surveillance, there was Mark Klein _ a telecommunications technician who alleged that AT&T was allowing U.S. spies to siphon vast amounts of customer data without warrants.

Klein's allegations and the news reports about them launched dozens of consumer lawsuits in early 2006.
against the government and telecommunications companies. The lawsuits alleged invasion of privacy and targeted the very same provisions of the Foreign Intelligence Surveillance Act that are at the center of the latest public outcry.

That was seven years ago, and the warrantless collection continues, perhaps on an even greater scale, underscoring just how difficult the recently outraged will have in pursuing any new lawsuits, like the one the American Civil Liberties Union filed against the government on Tuesday in New York federal court.

"I warned whoever I could," Klein said in telephone interview from his home in Alameda, a city across the bay from San Francisco. "I was angry then. I'm angrier now."

All the lawsuits prompted by Klein's disclosures were bundled up and shipped to a single San Francisco federal judge to handle. Nearly all the cases were tossed out when Congress in 2008 granted the telecommunications retroactive immunity from legal challenges, a law the U.S. Supreme Court upheld. Congress' action will make it difficult to sue the companies caught up in the latest disclosures.

The only lawsuit left from that bundle is one aimed directly at the government. And that case has been tied up in litigation over the U.S. Justice Department's insistence that airing the case in court would jeopardize national security.

"The United States government under both administrations has been stonewalling us in court," said Lee Tien, an attorney with the Electronic Frontier Foundation, which represents the consumers who filed that lawsuit. EFF has also filed a related lawsuit seeking the Justice Department's legal interpretation of the law that the government is apparently relying on to collect consumers' electronic data without a warrant.

James Clapper, director of national intelligence, personally urged U.S. District Judge Jeffrey White to throw out the remaining lawsuit. Clapper wrote the judge in September that the government risks "exceptionally grave damage to the national security of the United States" if forced to fight the lawsuit.
But on Friday, federal prosecutors asked the judge to delay making any decision until it can report back to the court on July 12 what the latest disclosures may mean to the lawsuit. Tien and other EFF lawyers are also assessing the newest disclosures to determine if they bolster their case.

Snowden, 29, a former CIA employee who most recently worked as a contractor for the National Security Agency, admitted leaking details of two secret government surveillance programs.

He revealed a top-secret court order issued April 25 by the Foreign Intelligence Surveillance Court that granted a three-month renewal for the large-scale collection of American phone records. That program, the same one Klein tried to expose, allows the NSA to gather hundreds of millions of U.S. phone records to search for possible links to terrorists abroad.

Snowden also disclosed another program that allows the government to tap into nine U.S. Internet companies and gather all communications to detect suspicious behavior that begins overseas.

A decade earlier, Klein began to sniff out the contours of the large-scale data collection. In 2002, he let in a visitor to his AT&T office in San Francisco who identified himself as an NSA representative. The NSA official interviewed Klein's colleague, who said he was given top-secret government clearance soon after the encounter.

A year later, Klein was touring another AT&T office in San Francisco where he saw the colleague installing a special room. By coincidence, Klein was transferred to that location a few months later and quickly discovered the colleague with the government clearance was the only person with access to the special room.

When the colleague retired in 2004, he gave Klein several documents, including highly technical wiring diagrams. The diagrams showed AT&T's electronic communications flowed through a "splitter," which created identical copies of the digital material. One copy continued on to its intended destination of consumer email in-boxes, phones and the like. The other copy flowed into the secret room.

"That's when I knew," Klein said.
Other documents showed similar setups at other communication companies, including Internet service providers and other telecommunications companies.

Those documents are now part of the lawsuit EFF is pursuing against the government.

Klein said he decided to publicize his concerns after President Bush in 2005, responding to a New York Times story about domestic eavesdropping, defended the program as limited to only foreign-based communications.

"It was clear that the NSA was looking at everything," Klein said. "It wasn't limited to foreign communications."

On Tuesday, Klein said that for a number of reasons, Snowden's disclosures sparked more public outrage than his own revelations did more than seven years ago.

For one thing, Klein said, Snowden had direct access to a secret court order and details of the program, while Klein pieced together the government's surveillance through internal AT&T documents and in discussions with colleagues who worked on the project.

"The government painted me as a nobody, a technician who was merely speculating," said Klein, who made his disclosures after he accepted a buyout and retired from AT&T in 2004. "Now we have an actual copy of a FISA court order. There it is in black and white. It's undisputable. They can't deny that."

Klein also said the allegations that the government was accessing social media sites such as Facebook may have gotten the attention of more younger people who weren't bothered by his initial disclosures.

"Now, the government is intruding in places they go," said Klein, 68. "That probably got their attention."
MUELLER TESTIMONY VIDEO

http://www.c-spanvideo.org/program/298757-1  See 43:47 – 44:12 minute marks

DAVID MURPHEE FAULK AND ADRIENNE KINNE

http://abcnews.go.com/Blotter/exclusive-inside-account-us-eavesdropping-americans/story?id=5987804&singlePage=true#.UcDfuPm0eSo

Exclusive: Inside Account of U.S. Eavesdropping on Americans
Despite pledges by President George W. Bush and American intelligence officials to the contrary, hundreds of US citizens overseas have been eavesdropped on as they called friends and family back home, according to two former military intercept operators who worked at the giant National Security Agency (NSA) center in Fort Gordon, Georgia.

The chairman of the Senate Intelligence Committee, Jay Rockefeller (D-WV), called the allegations "extremely disturbing" and said the committee has begun its own examination.

"We have requested all relevant information from the Bush Administration," Rockefeller said Thursday. "The Committee will take whatever action is necessary."

 watches the Nightline story

"These were just really every-day, average, ordinary Americans who happened to be in the Middle East, in our area of intercept and happened to be making these phone calls on satellite phones," said Adrienne Kinne, a 31-year old US Army Reserves Arab linguist assigned to a special military program at the NSA's Back Hall at Fort Gordon from November 2001 to 2003.

Kinne described the contents of the calls as "personal, private things with Americans who are not in any way, shape or form associated with anything to do with terrorism."

 watches Kinne discuss why it was 'awkward' listening to her fellow Americans.

She said US military officers, American journalists and American aid workers were routinely intercepted and "collected on" as they called their offices or homes in the United States.
Watch "World News Tonight with Charles Gibson" and "Nightline" for more of Brian Ross' exclusive report.

Another intercept operator, former Navy Arab linguist, David Murfee Faulk, 39, said he and his fellow intercept operators listened into hundreds of Americans picked up using phones in Baghdad's Green Zone from late 2003 to November 2007.

"Calling home to the United States, talking to their spouses, sometimes their girlfriends, sometimes one phone call following another," said Faulk.

**WATCH Faulk discuss what a day on the job was like listening to Americans.**

The accounts of the two former intercept operators, who have never met and did not know of the other's allegations, provide the first inside look at the day to day operations of the huge and controversial US terrorist surveillance program.

"There is a constant check to make sure that our civil liberties of our citizens are treated with respect," said President Bush at a news conference this past February.

But the accounts of the two whistleblowers, which could not be independently corroborated, raise serious questions about how much respect is accorded those Americans whose conversations are intercepted in the name of fighting terrorism.

**US Soldier's 'Phone Sex' Intercepted, Shared**

Faulk says he and others in his section of the NSA facility at Fort Gordon routinely shared salacious or tantalizing phone calls that had been intercepted, alerting office mates to certain time codes of "cuts" that were available on each operator's computer.

"Hey, check this out," Faulk says he would be told, "there's good phone sex or there's some pillow talk, pull up this call, it's really funny, go check it out. It would be some colonel making pillow talk and we would say, 'Wow, this was crazy'," Faulk told ABC News.
Faulk said he joined in to listen, and talk about it during breaks in Back Hall's "smoke pit," but ended up feeling badly about his actions.

"I feel that it was something that the people should not have done. Including me," he said.

**WATCH Faulke describe how U.S. officers' calls, including 'phone sex,' were intercepted, recorded & shared at NSA listening post.**

In testimony before Congress, then-NSA director Gen. Michael Hayden, now director of the CIA, said private conversations of Americans are not intercepted.

"It’s not for the heck of it. We are narrowly focused and drilled on protecting the nation against al Qaeda and those organizations who are affiliated with it," Gen. Hayden testified.

He was asked by Senator Orrin Hatch (R-UT), "Are you just doing this because you just want to pry into people's lives?"

"No, sir," General Hayden replied.

Asked for comment about the ABC News report and accounts of intimate and private phone calls of military officers being passed around, a US intelligence official said "all employees of the US government" should expect that their telephone conversations could be monitored as part of an effort to safeguard security and "information assurance."

"They certainly didn't consent to having interceptions of their telephone sex conversations being passed around like some type of fraternity game," said Jonathon Turley, a constitutional law professor at George Washington University who has testified before Congress on the country's warrantless surveillance program.

"This story is to surveillance law what Abu Ghraib was to prison law," Turley said.

**Listening to Aid Workers**

NSA awarded Adrienne Kinne a NSA Joint Service Achievement Medal in 2003 at the same time she says she was listening to hundreds of private
conversations between Americans, including many from the International Red Cross and Doctors without Borders.

"We knew they were working for these aid organizations," Kinne told ABC News. "They were identified in our systems as 'belongs to the International Red Cross' and all these other organizations. And yet, instead of blocking these phone numbers we continued to collect on them," she told ABC News.

**WATCH Kinne describe how listening to aid workers was part of the job.**

A spokesman for Doctors Without Borders, Michael Goldfarb, said: "The abuse of humanitarian action through intelligence gathering for military or political objectives, threatens the ability to assist populations and undermines the safety of humanitarian aid workers."

Both Kinne and Faulk said their military commanders rebuffed questions about listening in to the private conversations of Americans talking to Americans.

"It was just always, that, you know, your job is not to question. Your job is to collect and pass on the information," Kinne said.

Some times, Kinne and Faulk said, the intercepts helped identify possible terror planning in Iraq and saved American lives.

"IED's were disarmed before they exploded, that people who were intending to harm US forces were captured ahead of time," Faulk said.

NSA job evaluation forms show he regularly received high marks for job performance. Faulk left his job as a newspaper reporter in Pittsburgh to join the Navy after 9/11.

Kinne says the success stories underscored for her the waste of time spent listening to innocent Americans, instead of looking for the terrorist needle in the haystack.

"By casting the net so wide and continuing to collect on Americans and aid organizations, it's almost like they're making the haystack bigger and it's harder to find that piece of information that might actually be useful to
somebody," she said. "You're actually hurting our ability to effectively protect our national security."

The NSA: "The Shadow Factory"

Both former intercept operators came forward at first to speak with investigative journalist Jim Bamford for a book on the NSA, "The Shadow Factory," to be published next week.

"It's extremely rare," said Bamford, who has written two previous books on the NSA, including the landmark "Puzzle Palace" which first revealed the existence of the super secret spy agency.

"Both of them felt that what they were doing was illegal and improper, and immoral, and it shouldn't be done, and that's what forces whistleblowers."

WATCH Bamford describe how the NSA missed signals leading up to 9/11.

A spokesman for General Hayden, Mark Mansfield, said: "At NSA, the law was followed assiduously. The notion that General Hayden sanctioned or tolerated illegalities of any sort is ridiculous on its face."

The director of the NSA, Lt. General Keith B. Alexander, declined to directly answer any of the allegations made by the whistleblowers.

In a written statement, Gen. Alexander said: "We have been entrusted to protect and defend the nation with integrity, accountability, and respect for the law. As Americans, we take this obligation seriously. Our employees work tirelessly for the good of the nation, and serve this country proudly."

__________________________________
The Fed Who Blew the Whistle

Is he a hero or a criminal?

Michael Isikoff

NEWSWEEK

From the magazine issue dated Dec 22, 2008

Thomas M. Tamm was entrusted with some of the government's most important secrets. He had a Sensitive Compartmented Information security clearance, a level above Top Secret. Government agents had probed Tamm's background, his friends and associates, and determined him trustworthy.

It's easy to see why: he comes from a family of high-ranking FBI officials. During his childhood, he played under the desk of J. Edgar Hoover, and as an adult, he enjoyed a long and successful career as a prosecutor. Now gray-haired, 56 and fighting a paunch, Tamm prides himself on his personal rectitude. He has what his 23-year-old son, Terry, calls a "passion for justice." For that reason, there was one secret he says he felt duty-bound to reveal.

In the spring of 2004, Tamm had just finished a yearlong stint at a Justice Department unit handling wiretaps of suspected terrorists and spies-a unit so sensitive that employees are required to put their hands through a biometric scanner to check their fingerprints upon entering. While there, Tamm stumbled upon the existence of a highly classified National Security Agency program that seemed to be eavesdropping on U.S. citizens. The unit had special rules that appeared to be hiding the NSA activities from a panel of federal judges who are required to approve such surveillance. When Tamm started asking questions, his supervisors told him to drop the subject. He says one volunteered that "the program" (as it was commonly called within the office) was "probably illegal."
Tamm agonized over what to do. He tried to raise the issue with a former colleague working for the Senate Judiciary Committee. But the friend, wary of discussing what sounded like government secrets, shut down their conversation. For weeks, Tamm couldn't sleep. The idea of lawlessness at the Justice Department angered him. Finally, one day during his lunch hour, Tamm ducked into a subway station near the U.S. District Courthouse on Pennsylvania Avenue. He headed for a pair of adjoining pay phones partially concealed by large, illuminated Metro maps. Tamm had been eyeing the phone booths on his way to work in the morning. Now, as he slipped through the parade of midday subway riders, his heart was pounding, his body trembling. Tamm felt like a spy. After looking around to make sure nobody was watching, he picked up a phone and called The New York Times.

That one call began a series of events that would engulf Washington—and upend Tamm's life. Eighteen months after he first disclosed what he knew, the Times reported that President George W. Bush had secretly authorized the NSA to intercept phone calls and e-mails of individuals inside the United States without judicial warrants. The drama followed a quiet, separate rebellion within the highest ranks of the Justice Department concerning the same program. (James Comey, then the deputy attorney general, together with FBI head Robert Mueller and several other senior Justice officials, threatened to resign.) President Bush condemned the leak to the Times as a "shameful act." Federal agents launched a criminal investigation to determine the identity of the culprit.

The story of Tamm's phone call is an untold chapter in the history of the secret wars inside the Bush administration. The New York Times won a Pulitzer Prize for its story. The two reporters who worked on it each published books. Congress, after extensive debate, last summer passed a major new law to govern the way such surveillance is conducted. But Tamm—who was not the Times's only source, but played the key role in tipping off the paper—has not fared so well. The FBI has pursued him relentlessly for the past two and a half years. Agents have raided his house, hauled away personal possessions and grilled his wife, a teenage daughter and a grown son. More recently, they've been questioning Tamm's friends and associates about nearly every aspect of his life. Tamm has resisted pressure to plead to a felony for divulging classified information. But he is living under a pall, never sure if or when federal agents might arrest him.

Exhausted by the uncertainty clouding his life, Tamm now is telling his story publicly for the first time. "I thought this [secret program] was something the other branches of the government—and the public—ought to know about. So they could decide: do they want this massive spying program to be taking place?" Tamm told NEWSWEEK, in one of a series of recent interviews that he granted against the advice of his lawyers. "If somebody were to say, who am I to do that? I would say, 'I had taken an oath to uphold
the Constitution. It's stunning that somebody higher up the chain of command didn't speak up."

Tamm concedes he was also motivated in part by his anger at other Bush-administration policies at the Justice Department, including its aggressive pursuit of death-penalty cases and the legal justifications for "enhanced" interrogation techniques that many believe are tantamount to torture. But, he insists, he divulged no "sources and methods" that might compromise national security when he spoke to the Times. He told reporters Eric Lichtblau and James Risen nothing about the operational details of the NSA program because he didn't know them, he says. He had never been "read into," or briefed, on the details of the program. All he knew was that a domestic surveillance program existed, and it "didn't smell right."

(Justice spokesman Dean Boyd said the department had no comment on any aspect of this story. Lichtblau said, "I don't discuss the identities of confidential sources ... Nearly a dozen people whom we interviewed agreed to speak with us on the condition of anonymity because of serious concerns about the legality and oversight of the secret program." Risen had no comment.)

Still, Tamm is haunted by the consequences of what he did—and what could yet happen to him. He is no longer employed at Justice and has been struggling to make a living practicing law. He does occasional work for a local public defender's office, handles a few wills and estates—and is more than $30,000 in debt. (To cover legal costs, he recently set up a defense fund.) He says he has suffered from depression. He also realizes he made what he calls "stupid" mistakes along the way, including sending out a seemingly innocuous but fateful e-mail from his Justice Department computer that may have first put the FBI on his scent. Soft-spoken and self-effacing, Tamm has an impish smile and a wry sense of humor. "I guess I'm not a very good criminal," he jokes.

At times during his interviews with NEWSWEEK, Tamm would stare into space for minutes, silently wrestling with how to answer questions. One of the most difficult concerned the personal ramifications of his choice. "I didn't think through what this could do to my family," he says.

Tamm's story is in part a cautionary tale about the perils that can face all whistleblowers, especially those involved in national-security programs. Some Americans will view him as a hero who (like Daniel Ellsberg and perhaps Mark Felt, the FBI official since identified as Deep Throat) risked his career and livelihood to expose wrongdoing at the highest levels of government. Others—including some of his former colleagues—will deride Tamm as a renegade who took the law into his own hands and violated solemn obligations to protect the nation's secrets. "You can't have runoffs deciding they're going to be the white knight and running to the press," says Frances
Fragos Townsend, who once headed the unit where Tamm worked and later served as President Bush's chief counterterrorism adviser. Townsend made clear that she had no knowledge of Tamm's particular case, but added:

"There are legal processes in place [for whistle-blowers' complaints]. This is one where I'm a hawk. It offends me, and I find it incredibly dangerous."

Tamm understands that some will see his conduct as "treasonous." But still, he says he has few regrets. If he hadn't made his phone call to the Times, he believes, it's possible the public would never have learned about the Bush administration's secret wiretapping program. "I don't really need anybody to feel sorry for me," he wrote in a recent e-mail to NEWSWEEK. "I chose what I did. I believed in what I did."

If the government were drawing up a profile of a national-security leaker, Tamm would seem one of the least likely suspects. He grew up in the shadow of J. Edgar Hoover's FBI. Tamm's uncle, Edward Tamm, was an important figure in the bureau's history. He was once a top aide to Hoover and regularly briefed President Franklin Roosevelt on domestic intelligence matters. He's credited in some bureau histories with inventing (in 1935) not only the bureau's name, but its official motto: Fidelity, Bravery, Integrity. Tamm's father, Quinn Tamm, was also a high-ranking bureau official. He too was an assistant FBI director under Hoover, and at one time he headed up the bureau's crime lab. Tamm's mother, Ora Belle Tamm, was a secretary at the FBI's identification division.

When Thomas Tamm was a toddler, he crawled around Hoover's desk during FBI ceremonies. (He still remembers his mother fretting that his father might get in trouble for it.) As an 8-year-old, Tamm and his family watched John F. Kennedy's Inaugural parade down Pennsylvania Avenue from the balcony of Hoover's office, then located at the Justice Department.

Tamm's brother also served for years as an FBI agent and later worked as an investigator for the 9/11 Commission. (He now works for a private consulting firm.) Tamm himself, after graduating from Brown University in 1974 and Georgetown Law three years later, chose a different path in law enforcement. He joined the state's attorney's office in Montgomery County, Md. (He was also, for a while, the chairman of the county chapter of the Young Republicans.) Tamm eventually became a senior trial attorney responsible for prosecuting murder, kidnapping and sexual-assault cases. Andrew Sonner, the Democratic state's attorney at the time, says that Tamm was an unusually gifted prosecutor who knew how to connect with juries, in part by "telling tales" that explained his case in a way that ordinary people could understand. "He was about as good before a jury as anybody that ever worked for me," says Sonner, who later served as an appellate judge in Maryland.
In 1998, Tamm landed a job at the Justice Department’s Capital Case Unit, a new outfit
within the criminal division that handled prosecutions that could bring the federal death
penalty. A big part of his job was to review cases forwarded by local U.S. Attorneys’
Offices and make recommendations about whether the government should seek
execution. Tamm would regularly attend meetings with Attorney General Janet Reno,
who was known for asking tough questions about the evidence in such cases—a rigorous
approach that Tamm admired. In July 2000, at a gala Justice Department ceremony,
Reno awarded Tamm and seven colleagues in his unit the John Marshall Award, one of
the department’s highest honors.

After John Ashcroft took over as President Bush’s attorney general the next year, Tamm
became disaffected. The Justice Department began to encourage U.S. attorneys to
seek the death penalty in as many cases as possible. Instead of Reno’s skepticism
about recommendations to seek death, the capital-case committee under Ashcroft
approved them with little, if any, challenge. “It became a rubber stamp,” Tamm says.
This bothered him, though there was nothing underhanded about it. Bush had
campaigned as a champion of the death penalty. Ashcroft and the new Republican
leadership of the Justice Department advocated its use as a matter of policy.

Tamm’s alienation grew in 2002 when he was assigned to assist on one especially high-
profile capital case—the prosecution of Zacarias Moussaoui, a Qaeda terrorist arrested in
Minnesota who officials initially (and wrongly) believed might have been the “20th
hijacker”

in the September 11 plot. Tamm’s role was to review classified CIA cables about the
9/11 plot to see if there was any exculpatory information that needed to be relinquished
to Moussaoui’s lawyers.

While reviewing the cables, Tamm says, he first spotted reports that referred to the
rendition of terror suspects to countries like Egypt and Morocco, where aggressive
interrogation practices banned by American law were used. It appeared to Tamm that
CIA officers knew “what was going to happen to [the suspects]”—that the government
was indirectly participating in abusive interrogations that would be banned under U.S.
law.

But still, Tamm says he was fully committed to the prosecution of the war on terror and
wanted to play a bigger role in it. So in early 2003, he applied and was accepted for
transfer to the Office of Intelligence Policy and Review (OIPR), probably the most
sensitive unit within the Justice Department. It is the job of OIPR lawyers to request
permission for national-security wiretaps. These requests are made at secret hearings
of the Foreign Intelligence Surveillance Court, a body composed of 11 rotating federal
judges.
Congress created the FISA court in 1978 because of well-publicized abuses by the intelligence community. It was designed to protect the civil liberties of Americans who might come under suspicion. The court’s role was to review domestic national-security wiretaps to make sure there was "probable cause" that the targets were "agents of a foreign power"—either spies or operatives of a foreign terrorist organization. The law creating the court, called the Foreign Intelligence Surveillance Act, made it a federal crime-punishable by up to five years in prison—for any official to engage in such surveillance without following strict rules, including court approval.

But after arriving at OIPR, Tamm learned about an unusual arrangement by which some wiretap requests were handled under special procedures. These requests, which could be signed only by the attorney general, went directly to the chief judge and none other. It was unclear to Tamm what was being hidden from the other 10 judges on the court (as well as the deputy attorney general, who could sign all other FISA warrants). All that Tamm knew was that the "A.G.-only" wiretap requests involved intelligence gleaned from something that was obliquely referred to within OIPR as "the program."

The program was in fact a wide range of covert surveillance activities authorized by President Bush in the aftermath of 9/11. At that time, White House officials, led by Vice President Dick Cheney, had become convinced that FISA court procedures were too cumbersome and time-consuming to permit U.S. intelligence and law-enforcement agencies to quickly identify possible Qaeda terrorists inside the country. (Cheney's chief counsel, David Addington, referred to the FISA court in one meeting as that "obnoxious court," according to former assistant attorney general Jack Goldsmith.) Under a series of secret orders, Bush authorized the NSA for the first time to eavesdrop on phone calls and e-mails between the United States and a foreign country without any court review. The code name for the NSA collection activities—unknown to all but a tiny number of officials at the White House and in the U.S. intelligence community—was "Stellar Wind."

The NSA identified domestic targets based on leads that were often derived from the seizure of Qaeda computers and cell phones overseas. If, for example, a Qaeda cell phone seized in Pakistan had dialed a phone number in the United States, the NSA would target the U.S. phone number—which would then lead agents to look at other numbers in the United States and abroad called by the targeted phone. Other parts of the program were far more sweeping. The NSA, with the secret cooperation of U.S. telecommunications companies, had begun collecting vast amounts of information about the phone and e-mail records of American citizens. Separately, the NSA was also able to access, for the first time, massive volumes of personal financial records—such as credit-card transactions, wire transfers and bank withdrawals—that were being
reported to the Treasury Department by financial institutions. These included millions of "suspicious-activity reports," or SARS, according to two former Treasury officials who declined to be identified talking about sensitive programs. (It was one such report that tipped FBI agents to former New York governor Eliot Spitzer's use of prostitutes.) These records were fed into NSA supercomputers for the purpose of "data mining"-looking for links or patterns that might (or might not) suggest terrorist activity.

But all this created a huge legal quandary. Intelligence gathered by the extralegal phone eavesdropping could never be used in a criminal court. So after the NSA would identify potential targets inside the United States, counterterrorism officials would in some instances try to figure out ways to use that information to get legitimate FISA warrants-giving the cases a judicial stamp of approval.

It's unclear to what extent Tamm's office was aware of the origins of some of the information it was getting. But Tamm was puzzled by the unusual procedures-which sidestepped the normal FISA process-for requesting wiretaps on cases that involved program intelligence. He began pushing his supervisors to explain what was going on. Tamm says he found the whole thing especially curious since there was nothing in the special "program" wiretap requests that seemed any different from all the others. They looked and read the same. It seemed to Tamm there was a reason for this: the intelligence that came from the program was being disguised. He didn't understand why. But whenever Tamm would ask questions about this within OIPR, "nobody wanted to talk about it."

At one point, Tamm says, he approached Lisa Farabee, a senior counsel in OIPR who reviewed his work, and asked her directly, "Do you know what the program is?" According to Tamm, she replied: "Don't even go there," and then added, "I assume what they are doing is illegal." Tamm says his immediate thought was, "I'm a law-enforcement officer and I'm participating in something that is illegal?" A few weeks later Tamm bumped into Mark Bradley, the deputy OIPR counsel, who told him the office had run into trouble with Colleen Kollar-Kotelly, the chief judge on the FISA court. Bradley seemed nervous, Tamm says. Kollar-Kotelly had raised objections to the special program wiretaps, and "the A.G.-only cases are being shut down," Bradley told Tamm. He then added, "This may be [a time] the attorney general gets indicted," according to Tamm. (Told of Tamm's account, Justice spokesman Boyd said that Farabee and Bradley "have no comment for your story.")

One official who was aware of Kollar-Kotelly's objections was U.S. Judge Royce C. Lamberth, a former chief of the FISA court. Lamberth tells NEWSWEEK that when the NSA program began in October 2001, he was not informed. But the then chief of OIPR, James Baker, discovered later that year that program intelligence was being used in FISA warrants-and he raised concerns. At that point, Lamberth was called in for a
briefing by Ashcroft and Gen. Michael Hayden, the NSA chief at the time. Lamberth made clear to Ashcroft that NSA program intelligence should no longer be allowed in any FISA warrant applications without his knowledge. If it did appear, Lamberth warned, he would be forced to rule on the legality of what the administration was doing, potentially setting off a constitutional clash about the secret program.

Lamberth stepped down as chief FISA judge when his term ended in May 2002, but Kollar-Kotelly asked him to continue as an adviser about matters relating to the program. In early 2004, Kollar-Kotelly thought something was amiss. According to Lamberth, she had concerns that the intelligence community, after collecting information on U.S. citizens without warrants, was again attempting to launder that intelligence through her court-without her knowledge. She "had begun to suspect that they were back-dooring information from the program into" FISA applications, Lamberth tells NEWSWEEK. Kollar-Kotelly drew the line and wouldn't permit it. "She was as tough as I was," says Lamberth, who had once barred a top FBI agent from his court when he concluded the bureau hadn't been honest about FISA applications. "She was going to know what she was signing off on before she signed off … I was proud of her." (Kollar-Kotelly declined to speak with NEWSWEEK.)

Unbeknownst to Tamm, something else was going on at the Justice Department during this period. A new assistant attorney general, a law professor named Jack Goldsmith, had challenged secret legal opinions justifying the NSA surveillance program. (The controversial opinions, written by a young and very conservative legal scholar named John Yoo, had concluded that President Bush had broad executive authority during wartime to override laws passed by Congress and order the surveillance of U.S. citizens.) James Comey, the deputy attorney general, had agreed with Goldsmith and refused to sign off on a renewal of the domestic NSA program in March 2004. Attorney General Ashcroft was in the hospital at the time. The White House first tried to get an extremely ill Ashcroft, drugged and woozy, to overrule Comey, and then, after he refused, President Bush ordered the program to continue anyway. Comey, in turn, drafted a resignation letter. He described the situation he was confronting as "apocalyptic" and then added, "I and the Justice Department have been asked to be part of something that is fundamentally wrong," according to a copy of the letter quoted in "Angler," a book by Washington Post reporter Barton Gellman.

Tamm—who had no knowledge of the separate rebellion within the ranks of the Justice Department—decided independently to get in touch with Sandra Wilkinson, a former colleague of his on the Capital Case Unit who had been detailed to work on the Senate Judiciary Committee. He met with Wilkinson for coffee in the Senate cafeteria, where he laid out his concerns about the program and the unusual procedures within OIPR. "Look, the government is doing something weird here," he recalls saying. "Can you talk to somebody on the intelligence committee and see if they know about this?"
Some weeks passed, and Tamm didn’t hear back. So he e-mailed Wilkinson from his OIPR computer (not a smart move, he would later concede) and asked if they could get together again for coffee. This time, when they got together, Wilkinson was cool, Tamm says. What had she learned about the program? “I can’t say,” she replied and urged him to drop the subject. “Well, you know, then,” he says he replied, “I think my only option is to go to the press.” (Wilkinson would not respond to phone calls from NEWSWEEK, and her lawyer says she has nothing to say about the matter.)

He next few weeks were excruciating. Tamm says he consulted with an old law-school friend, Gene Karpinski, then the executive director of a public-interest lobbying group. He asked about reporters who might be willing to pursue a story that involved wrongdoing in a national-security program, but didn't tell him any details. (Karpinski, who has been questioned by the FBI and has hired a lawyer, declined to comment.)

Tamm says he initially considered contacting Seymour Hersh, the investigative reporter for The New Yorker, but didn’t know where to reach him. He’d also noticed some strong stories by Eric Lichtblau, the New York Times reporter who covered the Justice Department—and with a few Google searches tracked down his phone number.

Tamm at this point had transferred out of OIPR at his own initiative, and moved into a new job at the U.S. Attorney’s Office. He says he "hated" the desk work at OIPR and was eager to get back into the courtroom prosecuting cases. His new offices were just above Washington’s Judiciary Square Metro stop. When he went to make the call to the Times, Tamm said, "My whole body was shaking." Tamm described himself to Lichtblau as a "former" Justice employee and called himself "Mark," his middle name. He said he had some information that was best discussed in person. He and Lichtblau arranged to meet for coffee at Olsson’s, a now shuttered bookstore near the Justice Department.

After Tamm hung up the phone, he was struck by the consequences of what he had just done. "Oh, my God," he thought. "I can't talk to anybody about this." An even more terrifying question ran through his mind. He thought back to his days at the capital-case squad and wondered if disclosing information about a classified program could earn him the death penalty.

In his book, "Bush’s Law: The Remaking of American Justice," Lichtblau writes that he first got a whiff of the NSA surveillance program during the spring of 2004 when he got a cold call from a "walk-in" source who was "agitated about something going on in the intelligence community." Lichtblau wrote that his source was wary at first. The source did not know precisely what was going on—he was, in fact, maddeningly vague, the reporter wrote. But after they got together for a few meetings ("usually at a bookstore or coffee shops in the shadows of Washington's power corridors") his source's "credibility and his bona fides became clear and his angst appeared sincere." The source told him
of turmoil within the Justice Department concerning counterterrorism operations and the FISA court. "Whatever is going on, there's even talk Ashcroft could be indicted," the source told Lichtblau, according to his book.

Tamm grew frustrated when the story did not immediately appear. He was hoping, he says, that Lichtblau and his partner Risen (with whom he also met) would figure out on their own what the program was really all about and break it before the 2004 election. He was, by this time, "pissed off" at the Bush administration, he says. He contributed $300 to the Democratic National Committee in September 2004, according to campaign finance records.

It wasn't until more than a year later that the paper's executive editor, Bill Keller, rejecting a personal appeal and warning by President Bush, gave the story a green light. (Bush had warned "there'll be blood on your hands" if another attack were to occur.)

BUSH LETS U.S. SPY ON CALLERS WITHOUT COURTS, read the headline in the paper's Dec. 16, 2005, edition. The story—which the Times said relied on "nearly a dozen current and former officials"—had immediate repercussions. Democrats, including the then Sen. Barack Obama, denounced the Bush administration for violating the FISA law and demanded hearings. James Robertson, one of the judges on the FISA court, resigned. And on Dec. 30, the Justice Department announced that it was launching a criminal investigation to determine who had leaked to the Times.

Not long afterward, Tamm says, he started getting phone calls at his office from Jason Lawless, the hard-charging FBI agent in charge of the case. The calls at first seemed routine. Lawless was simply calling everybody who had worked at OIPR to find out what they knew.

But Tamm ducked the calls; he knew that the surest way to get in trouble in such situations was to lie to an FBI agent. Still, he grew increasingly nervous. The calls continued. Finally, one day, Lawless got him on the phone. "This will just take a few minutes," Lawless said, according to Tamm's account. But Tamm told the agent that he didn't want to be interviewed—and he later hired a lawyer. (The FBI said that Lawless would have no comment.)

In the months that followed, Tamm learned he was in even more trouble. He suspected the FBI had accessed his former computer at OIPR and recovered the e-mail he had sent to Wilkinson. The agents tracked her down and questioned her about her conversations with Tamm. By this time, Tamm was in the depths of depression. He says he had trouble concentrating on his work at the U.S. Attorney's Office and ignored some e-mails from one of his supervisors. He was accused of botching a drug case. By mutual agreement, he resigned in late 2006. He was out of a job and squarely in the
sights of the FBI. Nevertheless, he began blogging about the Justice Department for liberal Web sites.

Early on the morning of Aug. 1, 2007, 18 FBI agents-some of them wearing black flak jackets and carrying guns - showed up unannounced at Tamm's redbrick colonial home in Potomac, Md., with a search warrant.

While his wife, wearing her pajamas, watched in horror, the agents marched into the house, seized Tamm’s desktop computer, his children’s laptops, his private papers, some of his books (including one about Deep Throat) and his family Christmas-card list. Terry Tamm, the lawyer's college-age son, was asleep at the time and awoke to find FBI agents entering his bedroom. He was escorted downstairs, where, he says, the agents arranged him, his younger sister and his mother around the kitchen table and questioned them about their father. (Thomas Tamm had left earlier that morning to drive his younger son to summer school and to see a doctor about a shoulder problem.) "They asked me questions like 'Are there any secret rooms or compartments in the house'?” recalls Terry. "Or did we have a safe? They asked us if any New York Times reporters had been to the house. We had no idea why any of this was happening." Tamm says he had never told his wife and family about what he had done.

After the raid, Justice Department prosecutors encouraged Tamm to plead guilty to a felony for disclosing classified information-an offer he refused. More recently, Agent Lawless, a former prosecutor from Tennessee, has been methodically tracking down Tamm's friends and former colleagues. The agent and a partner have asked questions about Tamm's associates and political meetings he might have attended, apparently looking for clues about his motivations for going to the press, according to three of those interviewed.

In the meantime, Tamm lives in a perpetual state of limbo, uncertain whether he's going to be arrested at any moment. He could be charged with violating two laws, one concerning the disclosure of information harmful to "the national defense," the other involving "communications intelligence." Both carry penalties of up to 10 years in prison. "This has been devastating to him," says Jeffrey Taylor, an old law-school friend of Tamm’s. "It's just been hanging over his head for such a long time … Sometimes Tom will just zone out. It's like he goes off in a special place. He's sort of consumed with this because he doesn't know where it's going."

Taylor got a few clues into what the case was about last September when Agent Lawless and a partner visited him. The FBI agents sat in his office for more than an hour, asking what he knew about Tamm. The agents even asked about Tamm's participation in a political lunch group headed by his former boss, Andrew Sonner, that
takes place once a month at a Rockville, Md., restaurant. "What does that have to do with anything?" Taylor asked.

Agent Lawless explained. "This kind of activity"-leaking to the news media-"can be motivated by somebody who is a do-gooder who thinks that something wrong occurred," Lawless said, according to Taylor. "Or it could be politically motivated by somebody who wants to cause harm."

If it was the former - if Tamm was a "do-gooder"-the government could face a problem if it tried to bring a case to trial. The jurors might sympathize with Tamm and "you'd face jury nullification," said Lawless, according to Taylor, referring to a situation in which a jury refuses to convict a defendant regardless of the law.

Just this month, Lawless and another agent questioned Sonner, the retired judge who had served as a mentor to Tamm. The agents wanted to know if Tamm had ever confided in Sonner about leaking to the Times. Sonner said he hadn't, but he told the agents what he thought of their probe. "I told them I thought operating outside of the FISA law was one of the biggest injustices of the Bush administration," says Sonner. If Tamm helped blow the whistle, "I'd be proud of him for doing that."

Paul Kemp, one of Tamm's lawyers, says he was recently told by the Justice Department prosecutor in charge of Tamm's case that there will be no decision about whether to prosecute until next year-after the Obama administration takes office. The case could present a dilemma for the new leadership at Justice. During the presidential campaign, Obama condemned the warrantless-wiretapping program. So did Eric Holder, Obama's choice to become attorney general. In a tough speech last June, Holder said that Bush had acted "in direct defiance of federal law" by authorizing the NSA program.

Tamm's lawyers say his case should be judged in that light. "When I looked at this, I was convinced that the action he took was based on his view of a higher responsibility," says Asa Hutchinson, the former U.S. attorney in Little Rock and under secretary of the Department of Homeland Security who is assisting in Tamm's defense. "It reflected a lawyer's responsibility to protect the rule of law." Hutchinson also challenged the idea-argued forcefully by other Bush administration officials at the time-that The New York Times story undermined the war on terror by tipping off Qaeda terrorists to surveillance. "Anybody who looks at the overall result of what happened wouldn't conclude there was any harm to the United States," he says. After reviewing all the circumstances, Hutchinson says he hopes the Justice Department would use its "discretion" and drop the investigation. In judging Tamm's actions-his decision to reveal what little he knew about a secret domestic spying program that still isn't completely known-it can be hard
to decipher right from wrong. Sometimes the thinnest of lines separates the criminal from the hero.
Former FBI Counterterrorism Agent Tim Clemente: 'No Digital Communication Is Secure'

The Huffington Post | By Alexis Kleinman Posted: 05/07/2013 2:49 pm EDT | Updated: 05/07/2013 2:57 pm EDT

Even a former FBI agent doesn't seem comfortable with the level of surveillance his former employer exercises over Americans.

In an interview with CNN on Wednesday, former FBI counterterrorism agent Tim Clemente said that the FBI could listen to phone calls between Tamerlan Tsarnaev and his wife. "Welcome to America," he said. "All of that stuff is being captured as we speak whether we know it or like it or not."

The next day, Clemente returned to CNN, saying that "there's a way to look at digital communications in the past" and that "no digital communication is secure." Clemente specified that this type of surveillance can't be used in a criminal investigation but is used in "major terrorism investigations or counterintelligence investigations."

Watch the CNN interview below:

In an email to the Huffington Post, Christopher M. Allen from FBI Office of Public Affairs said that while he would not comment on Clemente's remarks, he did provide us with a link to congressional testimony from the bureau's former general counsel from 2011. "I can verify that the information from the testimony remains accurate," Allen said.
The testimony refers to the Communications Assistance for Law Enforcement Act (CALEA) of 1994. According to FBI counsel Valerie Caproni, the law "requires 'telecommunications carriers' to develop and deploy intercept solutions in their networks to ensure that the government is able to intercept electronic communications when lawfully authorized."

While the law covers phone networks, "CALEA does not cover popular Internet-based communications modalities such as webmail, social networking sites, or peer-to-peer services," Caproni wrote. But at a March luncheon, another FBI lawyer, Andrew Weissman, said that updating the law to let authorities monitor web activities in real time is a "top priority" of the bureau in 2013.

Surveillance has been at the top of everyone's mind since cameras were used to help find the Boston bombing suspects. Americans are having a difficult time deciding at what point their privacy is being violated more than their safety is being protected.

This essentially means that all digital communication is recorded and stored by the government, Guardian columnist Glenn Greenwald suggests. "[T]his revelation, made in passing on CNN, that every single telephone call made by and among Americans is recorded and stored is something which most people undoubtedly do not know, even if the small group of people who focus on surveillance issues believed it to be true," Greenwald wrote.

If there were a conversation somewhere out there that could make a huge difference in a terrorism case, how long would it take the FBI to find it? And at what cost?


ORIGINAL NSA WHISTLEBLOWER: I Saw The Order To Wiretap Barack Obama In 2004

MICHAEL B KELLEY JUN. 22, 2013, 10:31 AM
Russ Tice worked as an offensive National Security Agency (NSA) analyst from 2002 to 2005, before becoming a source for this Pulitzer Prize-winning New York Times article exposing NSA domestic spying.

This week he appeared on the Boiling Frogs Show and detailed how he had his hands "in the nitty-gritty, the nuts and bolts" during his 20 years as a U.S. intelligence analyst.

Tice claimed that he held NSA wiretap orders targeting numerous members of the U.S. government, including one for a young senator from Illinois named Barack Obama.

"In the summer of 2004, one of the papers that I held in my hand was to wiretap a bunch of numbers associated with a forty-some-year-old senator from Illinois. You wouldn't happen to know where that guy lives now would you? It's a big White House in Washington D.C. That's who the NSA went after. That's the President of the United States now."

Tice added that he also saw orders to spy on Hillary Clinton, Senators John McCain and Diane Feinstein, then-Secretary of State Colin Powell, Gen. David Petraeus, and a current Supreme Court Justice.

That sounds like a lot of abuse of the rules that govern NSA domestic spying. And that's exactly what Tice is claiming.
"The abuse is rampant and everyone is pretending that it's never happened, and it couldn't happen. ... I know [there was abuse] because I had my hands on the papers for these sorts of things: They went after high-ranking military officers; they went after members of congress — Senate and the House — especially on the intelligence committees and the armed services committees, lawyers, law firms, judges, State Department officials, part of the White House, multinational companies, financial firms, NGOs, civil rights groups ..."

Tice told Sibel Edmonds' radio show that back in 2005 the NSA didn't have the processing power, infrastructure, and storage to collect everything, but a source inside the NSA today confirmed to him that increased capabilities allow the spy agency to copy "every domestic communication in this country, word for word, content, every phone conversation, every email — they are collecting everything in bulk and putting it in databases."

That's an astonishing claim. And here's the kicker, according to Tice:

"Outrageous abuses ... have happened, and it's all being kept hush hush."


LOVEINT: When NSA officers use their spying power on love interests

By Andrea Peterson August 24, 2013
The National Security Agency admitted in a statement Friday that there have been “very rare” instances of willful violations of agency protocols by agency officers. The Wall Street Journal reports that some of those willful violations involved officials turning their private eyes on love interests:

The practice isn’t frequent — one official estimated a handful of cases in the last decade — but it’s common enough to garner its own spycraft label: LOVEINT.

Spy agencies often refer to their various types of intelligence collection with the suffix of “INT,” such as “SIGINT” for collecting signals intelligence, or communications; and “HUMINT” for human intelligence, or spying.

The “LOVEINT” examples constitute most episodes of willful misconduct by NSA employees, officials said.
While troubling, this type of snooping is by no means unprecedented. There are plenty of cases in which local law enforcement officials have been accused of abusing their access to databases to acquire information about potential romantic interests.

Most of the NSA violations were self-reported, and each instance resulted in administrative action of termination. The LOVEINT violations involved overseas communications, according to officials who spoke to the Journal.

That's consistent with what program defenders have said so far. Sen. Dianne Feinstein (D-Calif.), chair of the Senate of Intelligence Committee, told the Journal that violations didn't involve an American's personal information “in most instances” and that she’s seen no evidence that any of the violations involved the NSA’s domestic surveillance infrastructure.

Similarly, NSA Director Keith B. Alexander told a crowd of hackers and security experts at a Black Hat conference in July that Congress's review of domestic surveillance programs "found no one at NSA had ever gone outside the boundaries."

An NSA audit dated May 2012 that was obtained by The Post last week counted "2,776 incidents in the preceding 12 months of unauthorized collection, storage, access to or distribution of legally protected communications" -- most of them unintended.

---------------------------------------------

60 Minutes program about NSA on 15 Dec 2013 showed that they had a reverse lookup of the US phone book (the list of US number they show gives not just state but also city. You cannot get city unless you index every nr in the book.

http://www.cbsnews.com/videos/inside-the-nsa/
Cover Story: Is the FBI Up to the Job 10 Years After 9/11?

By Barton Gellman

FBI Director Bob Mueller glanced at the black chronograph he wears Marine-style, the face inside his wrist. It was 7:38 a.m. Not quite time. He reviewed his inbox. Drummed a four-fingered staccato on the desk. Consulted his wrist again: 7:39.

Mueller had already slashed through the red leather briefing book that headquarters dispatched to his Georgetown home before dawn. The title embossed on the cover was simply "Director," above the words "Top Secret/Contains Codeword Material." Yellow highlights flagged the points Mueller wanted to probe.

An al-Qaeda affiliate was evading surveillance with a new covert channel of communication. Cyberintruders had breached a defense contractor's firewall. The Tucson, Ariz., shooting of Representative Gabrielle Giffords had become a grotesque recruiting tool for antigovernment extremists. Turmoil in Bahrain had left FBI agents unable to serve a fugitive warrant. Egypt's meltdown was causing trouble for a valuable counterintelligence source. One of three deputy U.S. marshals shot in West Virginia had succumbed to his wounds. Two more federal officers, from Immigration and Customs Enforcement, had been ambushed in northern Mexico, one
fatally. Mexican authorities wanted access to FBI files, and Mueller had to decide how much to share.

Something more pressing was on Mueller's mind on Feb. 17, when TIME shadowed him through much of his day. The director had locked his sights on Lubbock, Texas, and Spokane, Wash., where his agents were closing in on a pair of unrelated terrorist plots. Mueller stood up abruptly at 7:40, five minutes ahead of schedule, and swept into conference room 7074. His division chiefs had learned by now, some of them the hard way, to assemble early. More analysts beamed in from the National Counterterrorism Center in suburban Virginia, linked by secure video to 61-in. plasma displays on three walls. Said Mueller: "We'll spend 15, 20 minutes going through what happened overnight."

As he nears the end of a 10-year term, Mueller, 66, is easily the longest-serving of his peers atop the national-security establishment. His anonymity in the role is almost a parlor trick. He remade the bureau in his image, pushed out the old guard and hired more than half its present cohort. Behind the scenes, he fought historic battles with the White House, twice compelling George W. Bush to change course under threat that Mueller would resign. Yet he is so careful to dodge the spotlight, so rigorously bland when caught onstage, that he could drink unrecognized at any bar in America.

It is a revelation to see Mueller in his own domain. There, he is a charismatic figure, level-voiced and seldom profane, who keeps his staff off balance with deadpan remarks that may or may not be jokes. He played ice hockey long past college, until his knees gave out, and he runs operations briefs as a contact sport. "I tend to be impatient," Mueller says. "Sometimes that's good. Sometimes that is not good. A certain degree of impatience is necessary to get decisions made and implemented and to move a group of individuals in a certain way."

Mueller inherited 56 field offices, each a distant fiefdom run by a special agent in charge. Old-school SACs (pronounced S-A-C, never sack) measured progress by arrests, kept their files to themselves and lived by the motto "Real agents don't type." They were accountable to no one but the director, and even those chains were loose.
Then came the searing failure of Sept. 11, 2001, seven days after Mueller's swearing-in. It was the worst hour in the FBI's 93-year history. "You talk about a learning curve," recalls Art Cummings, who worked alongside him. "He's barely been on the job, hasn't met many of his senior executives" and suddenly is faced with "the 'oh, crap' moments." Field offices in Phoenix and Minneapolis had important clues to the plot long before the attacks. Neither knew what the other knew, and no one put the pieces together. Critics began to say the FBI was irreparably broken, ill equipped to collect intelligence and disinclined to share it anyway. The labor force — heavily white and male, with a blue collar culture that prized physical courage over book smarts — lacked the language and technical skills to adapt. Other agencies took their lumps after 9/11, not least the CIA, but the FBI was on the chopping block when Congress began carving up government agencies.

To avoid dismemberment, Mueller made bold promises to cure what ailed the FBI from within — rebuilding it into a modern, intelligence-driven enterprise. His departure in September will mark the end of an era and another big change to an Obama team that will soon see Leon Panetta heading to the Pentagon and General David Petraeus succeeding him at the CIA.

Mueller put his money where his mouth was, doubling the agent force on national security and tripling the number of analysts. The FBI built a trip-wire system of early warnings that pre-empted some serious plots. But even a decade's reform has not changed J. Edgar Hoover's gangbusters into a 21st century counterterrorist force. The FBI lumps together in one superagency domestic law-enforcement tasks (such as fighting kidnapping, bank fraud and organized crime) with domestic intelligence roles (such as countering terror and espionage plots). But nearly every U.S. ally — the U.K., for instance, with Scotland Yard and MI5 — keeps them separate. It is far from clear that any agency can do a good job at both. "The problem with the FBI is that it has a fundamental institutional culture that does not mesh well with the needs of intelligence," says Judge Richard Posner of the Seventh Circuit Court of Appeals. Police do their work in a world of known crimes and criminals, while an intelligence service must devote years to "looking assiduously and competently for something that may not exist."
Tearing down old folkways in an FBI grown sclerotic with tradition called for a shift of power from autonomous field offices to the big blue chair in the director's conference room. That suited Mueller fine. He was an outstanding Marine officer candidate in 1966, author Garrett Graff reports in *The Threat Matrix*, but he earned a D for delegation. He is not a man who suffers attempts to chauffeur him around a briefing. "He's a perpetual-motion machine," says Thomas J. Harrington, who holds the FBI's third highest post, associate deputy director. "He likes to drive the thing the whole time." Among Mueller's disconcerting habits is a gesture with a cupped right hand that beckons a briefer to quit talking and slide over his notes. Mueller scans them and skips to cross-examination.

Two men, 1,300 miles apart, had Mueller's attention when he convened his operations brief on Feb. 17. Khalid Ali-M Aldawsari, a 20-year-old Saudi national, studied chemical engineering at Texas Tech University. Kevin William Harpham, 36, an unemployed Army veteran and avowed white supremacist, lived in a small town near Spokane. On this day the FBI's interest was a closely guarded secret, but indictments to come would allege that the two men were behind separate plots to set off powerful homemade bombs. Until recently, the FBI had not heard of either man.

The Spokane attack struck without warning on Jan. 17. Shortly before the start of Spokane's Martin Luther King Jr. Day parade, city workers found an abandoned backpack along the route. Inside was an explosive core laced with rat poison — an anticoagulant — and surrounded by lead fishing weights. A remote car starter and cell-phone parts were mated in a detonation circuit. The FBI lab in Quantico, Va., recovered DNA, but there was no suspect to test for a match.

Good luck and shoe leather led the FBI to Aldawsari, the Saudi student. One of the trip-wire programs rolled out after 9/11 invited vendors of hazardous goods to report unusual purchases to the feds. Aldawsari went undetected at first as he acquired the ingredients of TNP, an explosive used in World War I artillery shells. Amazon.com filled an order for 3 gal. of concentrated sulfuric acid, and the Georgia-based QualiChem Technologies shipped 10 boxes of nitric acid to a FedEx mail drop. Neither reported the buys. Aldawsari also dodged a student-visa review after flunking out of Texas Tech. Only on Feb. 1, when he ordered phenol, his last ingredient, did Aldawsari trip an alarm. Carolina Biological Supply tipped the FBI's Charlotte, N.C., field office, and Con-Way Freight, where
Aldawsari planned to take delivery, sent word to the Dallas field office by way of the Lubbock police.

In Mueller's FBI 2.0, Dallas and Charlotte alerted headquarters, which put the leads together and took command.

Mueller had every reason to believe his term as director would end long before this day. He had written his resignation letter on March 12, 2004, and fully expected to deliver it. At issue was a highly classified surveillance program, called Stellar Wind, that President Bush approved after 9/11. For the first time since Congress forbade the practice in 1978, the National Security Agency was spying on domestic communications traffic without a warrant. In the second week of March 2004, Attorney General John Ashcroft's Justice Department ruled that Stellar Wind was illegal. The next day, Ashcroft fell gravely ill with acute pancreatitis. Bush sent two top aides to George Washington University Hospital, where the Attorney General lay in critical condition. White House counsel Alberto Gonzales and chief of staff Andrew Card Jr. asked the semiconscious Ashcroft to sign a document reversing the Justice Department's ruling. Mueller arrived at the hospital just after Card and Gonzales retreated in defeat. His notes described Ashcroft as "feeble, barely articulate."

A close associate says Mueller saw the visit as a "cowardly and outrageous" attempt to take advantage of a sick man. The next afternoon, Mueller learned that Bush had reauthorized Stellar Wind over formal Justice Department objections. That night, he shut down the FBI's part in it and stayed up until 1:30 a.m. composing a letter: "Should the President order the continuation of the FBI's participation in the program, and in the absence of further legal advice from the AG, I would be constrained to resign as Director of the FBI."

Mueller knew the stakes. Acting Attorney General James Comey, together with nearly the whole top cadre at Justice, was also preparing to leave — a meltdown that would have dwarfed Richard Nixon's Saturday Night Massacre.

"I remember it all very well," says Valerie Caproni, then and now the FBI general counsel. "From my perspective, there was a very real likelihood of a collapse of government."
Early on Friday, March 12, Mueller stood with Comey in a foyer outside the Oval Office. "We knew this was our last morning," Comey recalls. "We both were just staring out, looking at the Rose Garden, thinking, This is the last time I'll ever see this." Mueller, Comey says, "wasn't rattled, but I could tell he was just very sad."

In the private dining room abutting the Oval Office, Mueller told Bush one-on-one that he would not carry out the President's order. He offered his resignation. Bush pulled back from the brink, submitting to the Justice Department's legal ruling.

Mueller will not speak of the episode, but when asked, he offers an indirect reply. "There are days that go by, but not many, that you're not balancing national security against civil liberties when you're addressing terrorism," he says. "So they are not easy decisions."

"But there's a place where you draw a black-and-white line and say, 'I can't do that'?" I ask.

"Yes," Mueller replies.

"If I'm ordered to do that, I can't'?"

"Yes. Yes."

The Stellar Wind confrontation was a rare moment in presidential history, an act of defiance that turned the Commander in Chief in his tracks. "You can only do that once, threaten to resign," says Frances Fragos Townsend, who was then Bush's counterterrorism adviser. "The second time you do it, you're going to be told, 'Accepted.'"

That was not how it turned out for Mueller. He did it again two years later, with much the same result.

On May 18, 2006, with Justice Department backing, Mueller obtained a search warrant for the legislative office of Representative William Jefferson. The seizure of documents there, in a corruption probe, touched off a furious protest on Capitol Hill, where members of both parties accused the Bush Administration of crossing a constitutional line. Separation of powers, Jefferson's lawyers argued, forbade executive intrusion into the protected spaces of the House.
In tense negotiations, aides to Bush instructed the FBI to return Jefferson's papers. Mueller — again joined by top Justice Department officials — passed word that he would leave before handing back evidence obtained by a lawful court order. A standoff ensued. Finally, Bush withdrew the instruction. He asked the FBI to seal Jefferson's papers temporarily while the Congressman made a constitutional challenge. Mueller agreed, the search warrant was upheld, and Jefferson was convicted of bribery, racketeering and money laundering. He remains free pending appeal.

Mueller has never spoken publicly of this episode either. I ask him what issue of principle was at stake.

"I think you've perhaps hit on a —" Mueller says, then stops. "I'm just going to stay away from it. I was close, but I've just got to stay away from it."

When Mueller convened his executive team on Feb. 17, Aldawsari had been under a microscope for two weeks. Four shifts of agents watched the Saudi engineering student 24 hours a day. Vehicles equipped with StingRay transceivers followed him around greater Dallas, recording his cell-phone calls. Agents had slipped secretly into Aldawsari's apartment, armed with a warrant from the Foreign Intelligence Surveillance Court. They inventoried his chemicals, cloned his computer drive and copied a journal handwritten in Arabic.

Hours before that morning's briefing, Aldawsari had published a blog post alluding to a special celebration of his upcoming 21st birthday. One of his handwritten journal entries, according to a hasty FBI translation, said, "And now, after mastering the English language, learning how to build explosives and continuous planning to target the infidel Americans, it is time for jihad."

Meanwhile, in the Spokane operation, investigators had caught a break. Harpham, a former member of the neo-Nazi National Alliance, was already a suspect, but until now he could not be linked forensically to the bomb plot. Hundreds of agents, canvassing retail purchases that matched bomb components, finally found a debit-card transaction in Harpham's name. The card had been used to buy a quantity of fishing weights at Walmart, the same brand and batch used as shrapnel in the backpack bomb.

As criminal cases, Lubbock and Spokane were well in hand. By now, the FBI of old would have placed the suspects under arrest. Waiting raised the risk that they might slip surveillance and flee or launch an unexpected
attack. But Mueller has changed this way of thinking. Moving in too soon would tip the FBI's hand, risking the loss of valuable intelligence. Harpham and Aldawsari looked like classic lone wolves, but investigators could not yet rule out accomplices. Were there opportunities to trace a network of support — financial, operational or ideological — that might lead to plotters of otherwise unrelated attacks?

This new way of thinking "is wickedly important to him," says Tracy Reinhold, the FBI's assistant director for intelligence. "You want to make sure that you gather all the intelligence you can possibly get before you decide to disrupt."

Mueller dug in, detail by granular detail. Did Harpham have offline contacts with his online correspondents in the Vanguard News Network, where he posted messages calling for race war? Had his Army service at Fort Lewis, Wash., overlapped with soldiers there who provoked a scandal with white-supremacist tattoos? What was holding up delivery of Harpham's Army DNA records?

In Lubbock, the team that searched Aldawsari's apartment had been interrupted and did not have time to learn whether he had unpacked his chemicals or whether he had the makings for a high explosive that required no phenol. The hasty retreat also left a gap in electronic surveillance, which nowadays has to include not only phone taps and pinhole cameras but voice-over-Internet, social-network messaging and online-gaming consoles. The Texas plot was unfolding across three e-mail addresses, which sent one another lists of "targets" and "nice targets" and directions for handling TNP. Was it one man? Two? Three?

The search team had to get back in. Mueller had no patience for explanations that agents were doing "pattern-of-life analysis" to find an opening. "You're not getting it done," Mueller said. "What are you going to do about it?" Later that day, the sneak-and-peek squad got it done. Then the investigators solved the mystery of the three e-mail addresses: Aldawsari was using all of them, they concluded, to send notes to himself.

One week later, on Feb. 24, agents placed Aldawsari under arrest. On March 9 the FBI's elite tactical force, the Hostage Rescue Team, moved in on Harpham. Both men were charged with attempted use of a weapon of mass destruction, which the law defines broadly enough to cover any kind
of bomb. Both have pleaded not guilty, and their lawyers note they are entitled to a presumption of innocence.

Harpham's plot, if the allegations prove true, turned out to be the more advanced. He had built a powerful bomb and placed it, for maximum carnage, atop a metal bench with a brick wall behind it to focus the blast. The half-complete work of Aldawsari, an Arab whose jihadi aims fit the popular image of a terrorist, received far more public attention. More than a year ago, Mueller raised some eyebrows when he testified that "homegrown and lone-wolf extremists pose an equally serious threat." But that message did not take root in the body politic or even in the national-security establishment. As the FBI chased the twin terrorist plots all through February, President Obama's team heard daily reports about Aldawsari's case but not Harpham's. Some of Mueller's lieutenants marveled at the contrast.

Domestic plots are not routinely included in the President's daily briefing or the interagency threat matrix, an FBI official says, even though "the degree of harm is often greater" than in jihadi terrorist plots.

"Any questions? We've got a couple of minutes," Mueller says to me between meetings, eyes drifting to his wrist. "Actually, about one minute."

Well, sure. Any tough decisions lately? But Mueller is already trotting down the hall and two flights of stairs to the FBI headquarters' innermost sanctum. Minutes later, at 8:30, Attorney General Eric Holder Jr. arrives for his own daily briefing. The two of them disappear into an area labeled "Restricted Access" and "Authorized Personnel Only."

Unlike the White House Situation Room and other pale shadows of a Hollywood command post, the FBI's Strategic Intelligence Operations Center has the flash to live up to its name. It covers just under an acre in a profusion of sealed rooms and internal corridors. An elevated communications pod, walled in glass, overlooks doors with signs like "Ops H" and "Intel Watch 24/7." Large maps compete for wall space with expanses of flat-screen monitors and a bank of clocks labeled with the four U.S. time zones, Greenwich Mean Time and local times in Afghanistan and Iraq.

The SIOC filled to capacity on 9/11 and remained that way through PENTTBOM, the FBI cryptonym for "Pentagon," "Twin Towers" and
"Bombing." From a standing start, Mueller ran the largest criminal investigation in FBI history and an equally massive intelligence effort to ward off the next catastrophe. FBI agents swarmed dive shops on a scuba-bomb tip and rural airfields on a crop-duster tip. They traced every long-haul truck that crossed one Canadian border post, some of which had since traveled thousands of miles, when the Energy Department reported a nuclear-weapon signature on a sensor it had started testing that day.

Only in retrospect, says a former Mueller lieutenant, did anyone treat as humorous another hunt that began with a source who overheard talk in a restroom in Ukraine of a stolen warhead. The resulting operation — which came to be known as Ukrainian Urinal — took on added urgency when then governor Tom Ridge called the White House and said, "I've just heard a report about a nuclear device in Pennsylvania." It turned out to be nothing. Ten years later, says Vahid Majidi, who runs the FBI's WMD directorate, the terrorist nuclear scenario is "very exciting, always good to see in a movie setting ... but we haven't seen a credible approach."

On average, since 9/11, the FBI reckons that just over 100,000 terrorism leads each year have come over the transom. Analysts and agents designate them as immediate, priority or routine, but the bureau says every one is covered. Leads from the Stellar Wind program were so vague and voluminous that field agents called them "Pizza Hut cases" — ostensibly suspicious calls that turned out to be takeout food orders. "In a year, we'll do, I don't know, 500 white powders, but you don't know which of those white powders in envelopes may contain something that kills somebody," Mueller said. "And so, yes, is it time-consuming? Absolutely. Do 99% of them wash out? Yes, but it's that other 1% that we've got to be concerned about."

By 2:30 p.m., Mueller was back in the big blue chair at the helm of his conference room. Four big-city special agents in charge, linked in from their offices, faced the director on his wall-size plasma screens.

For the next two hours, Mueller interrogated the SACs in Baltimore, Newark, N.J., Boston and Philadelphia about their records. TIME sat in on the first half hour, before the talk turned classified.

Mueller has made strikingly public events of these reviews: not only could each man see and hear the others, but each was surrounded by
subordinates. Few SACs emerge unscathed from the ritual, which is intended to spread Mueller's message quickly through the ranks. Nobody missed the point last year when the SAC in Albany, N.Y. — whose convictions produced half the FBI's average prison term — retired early. Mueller concluded he had been choosing easy targets.

In 2008, when Mueller unveiled the new reviews, he rated only 1 in 7 SACs as "good." Another 20% earned a "fair," and the rest were deemed deficient.

Before the Feb. 17 session, each SAC reported his assessment of top threats and accomplishments in counterterrorism, counterintelligence, cyber- and criminal operations. Baltimore ranked "al-Qaeda/Sunni" extremists as its most lethal threat, while Newark put down "homegrown Sunni extremists" and Boston the "self-radicalized, globally inspired." Philadelphia foresaw emerging threats from foreign spies looking to steal nanotechnology research. Mueller hammers on his SACs to justify these assessments and share the evidence with other agencies. If a field office has been stingy with intelligence-information reports (IIRs), which circulate around the government, former assistant FBI director John Miller says, the SAC will face relentless questioning. Mueller, he says, asks: "Is it that your sources don't have much information ... or is it that you're getting good information and your agents aren't bothering to write up IIRs?"

At that, Miller says, "you see that SAC sit there uncomfortably and try to decide what he wants to admit."

Mueller says later, poker-faced, that "it's probably been a growth experience for some SACs."

That afternoon Mueller directed an opening shot at Philadelphia "because I don't like the Phillies' pitching rotation." A Red Sox fan, Mueller has been known to consult Major League Baseball's At Bat app on his iPad during lunch.

Harrington, the FBI's No. 3, says softly, "Get ready." Mueller had spent hours reviewing line graphs and pie charts of results against resources for each field office. His jokes were often a barometer of mood.
SAC George Venizelos described a gang-control initiative in Camden, N.J., across the Delaware River from Philadelphia. Already there had been 58 arrests. Mueller's left eyebrow climbed.

"How are you measuring positive community impact?" he asked. Venizelos kicked the question to John Cosenza, his No. 2. "Initially, when you go in and make arrests, you can create more crime — territorial, people coming in and trying to take over," Cosenza said. "Hopefully, some of the crime statistics will get lower."

Hopefully. Mueller turned away. Boston (gang violence) and Baltimore (armed robbery) sounded much the same.

Michael Ward in Newark had results. He had come to the aid of local police when carjackings spiked 2,000% in Newark and Trenton, N.J., and his measure of impact was "a reduction in the carjacking rate." He threw 30 to 40 agents at the problem and brought the numbers back down.

Mueller's fingers drummed. He shifted in his seat. Carjackings? Weeks later, Ward says he doesn't know "how it registered at headquarters," but he defends his work as a model of "how you're supposed to deal with emerging threats." Mueller, looking back, says, "I learned a lot that day in terms of what was happening in Trenton." It is good to lend a hand to local police, but carjacking "is not one of the top priorities." Mueller says he is still "trying to drive out ... the usual metric of arrests, indictments and convictions by numbers."

In the moment, there was nothing Mueller wanted to say to Ward with a reporter in the room. Shortly afterward, Mueller looked at his watch, looked at me and looked pointedly at the door.

"O.K.," he said. "We're going to turn to national security in 15 seconds."

Mueller's interrogation of SACs, according to David Schlendorf, the FBI's assistant director for resource planning, arose from a frustrated question: "How do I, as one person, pull the levers so that 35,000 people do what I want them to do?" Schlendorf embodies a startling invasion of private-sector managers into Mueller's FBI. He arrived as a special assistant in 2003 with a Harvard MBA and was amazed to discover that he had to walk down the hall to find the Internet. Within five years, he had leapfrogged a generation of agents to the FBI's top executive ranks.
Mueller wants more like him and makes regular recruiting trips to business schools. Their graduates have brought modern office tools to an FBI that still cannot buy a box of pencils without filling out Form FD 369 in quintuplicate — using carbon paper. They also brought exotic business jargon and a four-color FBI strategy map of arrows chasing ovals. Outsiders displaced agents with badges and guns as assistant directors in charge of finance, human resources, information technology and the directorate of weapons of mass destruction.

Mueller spurred the change of guard with an up-or-out rule for field supervisors. Hundreds retired, quit or were removed from their posts, an enormous loss of collective memory. "These were people who knew their craft very well," says Konrad Motyka, president of the FBI Agents Association. "There are certain things the field knows and certain things headquarters knows, and sometimes they don't exactly mesh." The old guard calls Mueller's rising stars the "blue flamers," which is not a compliment. Schlendorf was equally undiplomatic. "To use a loaded term, the legacy employees — sometimes we've had an issue where they might be threatened by the younger, newer generation, more tech-savvy," he says. "So that's been a challenge. But we need to be competing with Google, with GE, for the best talent."

And then there is Mueller himself. Years ago, when he ran the Justice Department's criminal division, subordinates dubbed him Bobby Three Sticks. The Mob-style sobriquet made sport of his Brahmin demeanor and fancy Philadelphia name, Robert Swan Mueller III. Only one old friend, Associate Deputy Attorney General David Margolis, "has ever used that name to my face," Mueller says. In the FBI, it is not pronounced with affection. Michael Mason, who retired in 2007, says Mueller's Princeton diploma and prep-school pedigree gave agents an excuse to oppose reforms: "People tend to look for 'How are you not like me? Why is it O.K. for me to not like this?'"

Mueller's occasional efforts to show a softer side tend to be awkward. One legendary example, recounted fondly by former counsel Chuck Rosenberg, began with a phone call before 6 a.m. at the office.

"Yes, sir," Rosenberg said.

"How are you?" Mueller asked.
"Fine."

"Everything O.K.?"

"Yes, sir. Everything's fine. Do you need anything?"

"Nope," Mueller said.

The line went dead, and the phone rang next door. A moment later, Mueller's special assistant told Rosenberg, "I just got the strangest call from the director."

After 9/11, Bush summoned Mueller and Ashcroft to brief him daily in the Oval Office. He scaled back eventually to twice a week. Obama convenes a weekly Terror Tuesday to review threats and operations with a large cast of Cabinet and agency chiefs. Mueller likes to use visual aids. When he met President-elect Obama in Chicago, he and Michael Leiter, director of the National Counterterrorism Center, brought an al-Qaeda map so large they call it the "horse blanket." But Mueller drew the line at showing Obama a staff-produced model of the underwear bomb — explosives stuffed into the crotch — that Umar Farouk Abdulmutallab wore aboard a flight to Detroit in the failed Christmas bombing attempt of 2009. "Not a good idea," he said. Instead he showed a video clip of the basketball-size hole blown through the fuselage of a test aircraft when FBI technicians set off a replica of Abdulmutallab's bomb. Says Holder of Mueller: "The President relies on him, has faith in him, is anxious to hear from him."

Under Obama as under Bush, many of the tough calls fall to Mueller. One of the toughest began on Sept. 9, 2009, when a shuttle-bus driver named Najibullah Zazi set out from Denver to New York City. A multiagency intelligence effort had identified him as an al-Qaeda operative on his way to a suicide bombing, but crucial details were unknown. He was thought to be carrying detonators and the explosive TATP. The case, Holder says, "literally developed as Zazi was driving across the country. How far are you going to let him go? If the concern is that he's bringing explosive material in the car, how do you deal with that?" Surveillance, hampered by weather, could not be guaranteed.

As Zazi neared the Hudson River, Leiter says, the question was, "Do we let him go into New York City? You're approaching the Sept. 11 anniversary."
You know he's talking to al-Qaeda. You don't know who he's going to meet, what he's going to do."

The stakes were high for New York, and for Mueller, if Zazi decided to set off his charges on the George Washington Bridge. Arresting him would prevent a disaster like that, but Mueller held back, intent on identifying confederates. He arranged for ruses to search Zazi's rental car at a fake drug-screening checkpoint and then an impoundment lot, where traffic police towed it on a trumped-up infraction. Only when New York City detectives spooked Zazi did Mueller's agents move in.

By then, the FBI and National Security Agency had enough in hand to unravel the plot. Zazi and two high school friends, all trained in Pakistan, planned to detonate backpack bombs simultaneously aboard subway trains in Times Square and Grand Central Station. Threats to prosecute his parents for immigration fraud induced Zazi to give up the details. He pleaded guilty to conspiracy to use a weapon of mass destruction and two other charges. Sentencing is expected in June.

The threat stream since 9/11 has brought perhaps a dozen plots as grave and near at hand as Zazi's. It is no small victory that all of them failed, even if a balky shoe-bomb fuse and other gifts of fortune played their roles. But the FBI has expended great effort too against less obvious threats, using controversial undercover tools. In case after case, agents or informants have fanned loose talk of violence by angry Muslims into FBI-led plots — recruiting participants, selecting targets, teaching tradecraft, providing cash or matériel and then swooping in with arrests. The Liberty City Seven in Miami were said to be conspiring to destroy the Willis (then Sears) Tower, but the consensus among trial observers was that they "probably couldn't have found their way to Chicago," as Posner puts it with only mild hyperbole. Six men aroused suspicion when they tried to copy a video about jihad. An informant, recruited under threat of deportation, offered weapons and drove them on surveillance routes, culminating in charges that they planned an attack on New Jersey's Fort Dix. Thus far, prosecutors have fought off entrapment defenses, but theMutt and Jeff—style cases raise doubts about the FBI's priorities. "If we don't, someone else may very well help them," says David Kris, who oversaw national-security cases at Justice. "We can't afford to ignore them."
The director's unmarked Gulfstream jet rolled into a fast descent, corkscrewing to avoid potential ground fire. The U.S. embassy in Yemen had come under mortar attack three days earlier, on April 6, 2008, and the threat stream in Sana'a was surging. Mueller turned to Ed McCormack, chief of his security detail, shortly after landing. "Got a spare set of handcuffs?" he asked. McCormack obliged with a well-scuffed pair that had seen hard use on bank robbers in his street-agent days. Mueller stuffed them under his belt and set off for the presidential palace.

Some hours later, Mueller's meeting with President Ali Abdullah Saleh was ending badly. The FBI chief pressed for the extradition of convicted al-Qaeda terrorist Jamal al-Badawi, who kept making unlikely escapes from Yemeni prison. Saleh dodged. He would need an act of parliament. He had personally obtained al-Badawi's promise to give up terrorism.

Mueller was unmoved. Saleh turned to bluster. "He flared his arms, raised his voice, made it clear this was his country," recalls Carlos Fernandez, then the FBI's legal attaché in Yemen. The President stood and escorted his visitors to the door, past a gold-plated Kalashnikov rifle sent by Saddam Hussein. Mueller stopped and reached for the small of his back. He pulled out the 10-oz. Peerless cuffs and plunked them into Saleh's hand. "Next time I'm here, I'd like to see these on Mr. Badawi," Mueller said. Saleh's eyes widened as the translator caught up. Then Mueller cracked a smile and clapped the smaller man on the shoulder. Saleh threw back his head and laughed.

The encounter highlighted a remarkable expansion of the FBI's global role. The bureau has more legal attachés — 60 full-time overseas posts in countries ranging from Saudi Arabia to Sierra Leone — than domestic field offices. Mueller has traveled to 40 countries in 110 visits overseas.

To admirers, the Yemen trip showed off Mueller as an effective diplomat. "Saleh is very much a man's man in his own mind," says former U.S. ambassador Stephen Seche, who witnessed the stunt. "Mueller's strategy was to play to this element of his character." Saleh stood firm on extradition, but he gave Mueller a quiet guarantee "that Badawi was going to stay behind bars forever," Fernandez says.

But the episode could equally be said to show the limits of Mueller's reach. This was his ninth unsuccessful attempt to persuade Saleh to extradite a
man on the FBI's most-wanted-terrorists list. Two months ago, Saleh released several dozen al-Qaeda fighters from jail. The FBI will not say whether it knows al-Badawi's whereabouts. Meanwhile, Saleh himself is fighting for survival in Yemen and may soon be heading out the door.

Mueller has had his share of failures, including missteps in the lead-up to the Fort Hood, Texas, shooting, disregarded warnings about the abuse of national-security letters and an epochal investigation of the 2001 anthrax letters that concentrated for years on the wrong man. Not least of the black marks is the serially disastrous effort to build a modern information system for the FBI. Mueller struggled throughout his term to replace what the Government Accountability Office called an "antiquated, paper-based, legacy system" for managing intelligence and case files. The first attempt, Virtual Case File, spent $104 million over three years on a project so badly broken that it had to be discarded altogether. He has promised delivery of the replacement project, called Sentinel, nearly every year since 2006. Mueller's most recent projection calls for "full operability" in September, the month he steps down.

Yet even Glenn Fine, who dogged the FBI for 10 years as the Justice Department inspector general, gave a watchdog's grudging endorsement. "They haven't done everything perfectly. They've made mistakes," he says. "By and large, he has moved the FBI in the right direction."

Mueller's goal of an agile, intelligence-driven service may spill the banks of plausible ambition, but there is not much doubt that important change is under way. "Our organization historically has been criticized for collecting a lot and either not doing anything with it or not sharing it," says Shawn Henry, who oversees the criminal and cyber divisions. When he sees valuable intelligence shared with other agencies, "it astounds me because I still expect some reluctance," but field agents increasingly accept that "if I can't action this, somebody else might be able to action it. If it's sitting in my drawer, or worse, sitting in my head, shame on me."

Mueller maintains that the FBI's police role complements intelligence gathering. "Because of the cooperation we get in just about every case, because of plea bargains, we get a substantial amount of intelligence," he says. The hardened terrorists of myth, he says, "are like everybody else. There are very few that have not in some way cooperated for some period of time."
Most people inside the bureau believe that the blown opportunities to head off 9/11 would not recur today. Even among the FBI's doubters, few disagree that the bureau has come a long way. Comey, whom Mueller has described privately as his preferred successor, says it will take another generation to reach the goals that Mueller set. "I think he has started the turning of the cultural battleship," Comey says. "I don't know if it's a quarter-turn or a half-turn, but the job of the next director is to keep pushing."


Edward Snowden reveals that NSA and GCHQ hacked SIM card manufacturer

BY ALEJANDRO ALBA

NEW YORK DAILY NEWS

Thursday, February 19, 2015, 4:12 PM
The NSA and the Government Communications Headquarters targeted Gemalto, a multinational firm in the Netherlands that makes mobile phone SIM cards, to monitor mobile communications on respective SIMs without permission from telephone companies.

British and American spies stole the encryption keys from the largest SIM card manufacturer in the world, according to a government document handed to The Intercept by National Security Agency whistleblower Edward Snowden.

The NSA and its British counterpart Government Communications Headquarters targeted Gemalto, a multinational firm in the Netherlands that makes mobile phone SIM cards, to monitor mobile communications without permission from telephone companies.

Gemalto currently creates SIM cards for AT&T, T-Mobile, Verizon, Sprint and 450 other wireless network providers around the world. Gemalto produces around 2 billion SIM cards every year.

The breach, detailed in a 2010 GCHQ document, also gave the NSA and GCHQ the ability to monitor phone activity without leaving a trace that wireless providers could track. The intelligence agencies were also allowed to decrypt communications that they previously couldn't decode.

Gemalto said that it was unaware of the hack until The Intercept reached out to them for comment. The SIM manufacturer said it launched an investigation on its system Wednesday, but it wasn't able to find any trace of the security breach.

"I'm disturbed, quite concerned that this happened," Paul Beverly, Gemalto executive vice president, told The Intercept. "The most important thing for me is to understand exactly how this was done, so we can take every measure to ensure that it doesn't happen again."

The top-secret GCHQ document also revealed that the intelligence agencies cyberstalked Gemalto's employees in an effort to secretly obtain information that could give them access to millions of encryption keys.
It's still unclear as to whether or not other Gemalto security products and
data were compromised. It's also unclear how many wireless network
providers and customers have been affected in the breach.

T-Mobile, Verizon, Sprint and AT&T were asked by the Daily News to
comment on the issue, but a response was not immediately returned.

The NSA and GCHQ have declined to comment on the document leak.

aalba@nydailynews.com

http://www.theguardian.com/world/2014/apr/01/nsa-surveillance-loophole-americans-data

**NSA performed warrantless searches on Americans' calls and emails – Clapper**

NSA used 'back door' to search Americans' communications
Director of national intelligence confirms use of new legal rule
Data collected under 'Prism' and 'Upstream' programs

**Spencer Ackerman** in Washington and **James Ball** in New York

The Guardian, Tuesday 1 April 2014 16.17 EDT

Clapper said: 'These queries were performed pursuant to minimization
procedures and consistent with the statute and the fourth amendment.'

Photo: Shawn Thew/EPA
US intelligence chiefs have confirmed that the National Security Agency has used a "back door" in surveillance law to perform warrantless searches on Americans’ communications.

The NSA’s collection programs are ostensibly targeted at foreigners, but in August the Guardian revealed a secret rule change allowing NSA analysts to search for Americans’ details within the databases. Now, in a letter to Senator Ron Wyden, an Oregon Democrat on the intelligence committee, the director of national intelligence, James Clapper, has confirmed the use of this legal authority to search for data related to “US persons”.

“There have been queries, using US person identifiers, of communications lawfully acquired to obtain foreign intelligence targeting non-US persons reasonably believed to be located outside the United States,” Clapper wrote in the letter, which has been obtained by the Guardian.

“These queries were performed pursuant to minimization procedures approved by the Fisa court and consistent with the statute and the fourth amendment.”

The legal authority to perform the searches, revealed in top-secret NSA documents provided to the Guardian by Edward Snowden, was denounced by Wyden as a “backdoor search loophole.”

Many of the NSA’s most controversial programs collect information under the law affected by the so-called loophole. These include Prism, which allows the agency to collect data from Google, Apple, Facebook, Yahoo and other tech companies, and the agency’s Upstream program – a huge network of internet cable taps.

Clapper did not say how many warrantless searches had been performed by the NSA. It was not the first time the searches had been confirmed: after the Snowden leaks, the office of the director of national intelligence declassified documents that discussed the rule change. But Clapper’s letter drew greater attention to the issue.

Confirmation that the NSA has searched for Americans’ communications in its phone call and email databases complicates President Barack Obama’s initial defenses of the broad surveillance in June.
“When it comes to telephone calls, nobody is listening to your telephone calls. That’s not what this program’s about,” Obama said. “As was indicated, what the intelligence community is doing is looking at phone numbers and durations of calls. They are not looking at people’s names, and they’re not looking at content.”

Obama was referring specifically to the bulk collection of US phone records, but his answer misleadingly suggested that the NSA could not examine Americans’ phone calls and emails.

At a recent hearing of the Privacy and Civil Liberties Oversight Board, administration lawyers defended their latitude to perform such searches. The board is scheduled to deliver a report on the legal authority under which the communications are collected, Section 702 of the Foreign Intelligence Surveillance Act (Fisa), passed in 2008.

Wyden and Colorado Democrat Mark Udall failed in 2012 to persuade their fellow Senate intelligence committee members to prevent such warrantless searches during the re-authorisation of the 2008 Fisa Amendments Act, which wrote Section 702 into law.

Dianne Feinstein, the California Democrat who chairs the committee, defended the practice, and argued that it did not violate the act’s “reverse targeting” prohibition on using NSA’s vast powers to collect content on Americans.

“With respect to analysing the information lawfully collected under Section 702, however, the intelligence community provided several examples in which it might have a legitimate foreign intelligence need to conduct queries in order to analyze data already in its possession,” Feinstein said in June 2012.

“The Department of Justice and the intelligence community reaffirmed that any queries made of Section 702 data will be conducted in strict compliance with applicable guidelines and procedures, and do not provide a means to circumvent the general requirement to obtain a court order before targeting a US person under Fisa.”

Clapper referred to that debate in his letter to Wyden, which came in response to the senator’s request in January for a public answer on whether the NSA had in fact conducted such searches.
“As you know, when Congress reauthorized Section 702, the proposal to restrict such queries was specifically raised and ultimately not adopted,” Clapper wrote.

Much of the NSA’s bulk data collection is covered by section 702 of the Fisa Amendments Act. This allows for the collection of communications – content and metadata alike – without individual warrants, so long as there is a reasonable belief the communications are both foreign and overseas.

The communications of Americans in direct contact with foreign targets can also be collected without a warrant, and the intelligence agencies acknowledge that purely domestic communications can also be inadvertently swept into its databases. That process is known as "incidental collection".

Initially, NSA rules on such data prevented the databases being searched for any details relating to "US persons" – that is, citizens or residents of the US. However, in October 2011 the Fisa court approved new procedures which allowed the agency to search for US person data, a revelation contained in documents revealed by Snowden.

The ruling appears to give the agency free access to search for information relating to US people within its vast databases, though not to specifically collect information against US citizens in the first place. However, until the DNI’s disclosure to Wyden, it was not clear whether the NSA had ever actually used these powers.

On Tuesday, Wyden and Udall said the NSA’s warrantless searches of Americans’ emails and phone calls “should be concerning to all.”

“This is unacceptable. It raises serious constitutional questions, and poses a real threat to the privacy rights of law-abiding Americans. If a government agency thinks that a particular American is engaged in terrorism or espionage, the fourth amendment requires that the government secure a warrant or emergency authorisation before monitoring his or her communications. This fact should be beyond dispute,” the two senators said in a joint statement.

They continued: “Today’s admission by the Director of National Intelligence is further proof that meaningful surveillance reform must include closing the back-door searches loophole and requiring the intelligence community to
show probable cause before deliberately searching through data collected under section 702 to find the communications of individual Americans."

This article was amended on 1 April to correct the month in 2012 when the 2008 Fisa Amendments Act was reauthorsied. It was further amended on 2 April to make it clear that in August 2013, the US government declassified documents that first confirmed the searches of US persons' data under Section 702 of Fisa.


**NSA spying flap extends to contents of U.S. phone calls**

National Security Agency discloses in secret Capitol Hill briefing that thousands of analysts can listen to domestic phone calls. That authorization appears to extend to e-mail and text messages too.

by Declan McCullagh

June 15, 2013 4:39 PM PDT
NSA Director Keith Alexander says his agency's analysts, which until recently included Edward Snowden among their ranks, take protecting "civil liberties and privacy and the security of this nation to their heart every day."

The National Security Agency has acknowledged in a new classified briefing that it does not need court authorization to listen to domestic phone calls, a participant said.

Rep. Jerrold Nadler, a New York Democrat, disclosed on Thursday that during a secret briefing to members of Congress, he was told that the contents of a phone call could be accessed "simply based on an analyst deciding that."

If the NSA wants "to listen to the phone," an analyst's decision is sufficient, without any other legal authorization required, Nadler said he learned. "I was rather startled," said Nadler, an attorney and congressman who serves on the House Judiciary committee.
Not only does this disclosure shed more light on how the NSA's formidable eavesdropping apparatus works domestically, it also suggests the Justice Department has secretly interpreted federal surveillance law to permit thousands of low-ranking analysts to eavesdrop on phone calls.

James Owens, a spokesman for Nadler, provided a statement on Sunday morning, a day after this article was published, saying: "I am pleased that the administration has reiterated that, as I have always believed, the NSA cannot listen to the content of Americans' phone calls without a specific warrant." Owens said he couldn't comment on what assurances from the Obama administration Nadler was referring to, and said Nadler was unavailable for an interview. (CNET had contacted Nadler for comment on Friday.)

Because the same legal standards that apply to phone calls also apply to e-mail messages, text messages, and instant messages, being able to listen to phone calls would mean the NSA analysts could also access the contents of Internet communications without going before a court and seeking approval.

Nadler's initial statement appears to confirm some of the allegations made by Edward Snowden, a former NSA infrastructure analyst who leaked classified documents to the Guardian. Snowden said in a video interview that, while not all NSA analysts had this ability, he could from Hawaii "wiretap anyone from you or your accountant to a federal judge to even the president."

There are serious "constitutional problems" with this approach, said Kurt Opsahl, a senior staff attorney at the Electronic Frontier Foundation who has litigated warrantless wiretapping cases. "It epitomizes the problem of secret laws."

The NSA declined to comment to CNET. (This is unrelated to the disclosure that the NSA is currently collecting records of the metadata of all domestic Verizon calls, but not the actual contents of the conversations.)

Rep. Mike Rogers (R-Mich.), the head of the House Intelligence committee, told CNN on Sunday that the NSA "is not listening to Americans' phone calls" or monitoring their e-mails, and any statements to the contrary are "misinformation." It would be "illegal" for the NSA to do that, Rogers said.
The Washington Post disclosed Saturday that the existence of a top-secret NSA program called NUCLEON, which "intercepts telephone calls and routes the spoken words" to a database. Top intelligence officials in the Obama administration, the Post said, "have resolutely refused to offer an estimate of the number of Americans whose calls or e-mails have thus made their way into content databases such as NUCLEON."

(Credit: Getty Images)

A portion of the NSA's mammoth data center in Bluffdale, Utah, scheduled to open this fall.

Earlier reports have indicated that the NSA has the ability to record nearly all domestic and international phone calls -- in case an analyst needed to access the recordings in the future. A Wired magazine article last year disclosed that the NSA has established "listening posts" that allow the agency to collect and sift through billions of phone calls through a massive new data center in Utah, "whether they originate within the country or overseas." That includes not just metadata, but also the contents of the communications.

William Binney, a former NSA technical director who helped to modernize the agency's worldwide eavesdropping network, told the Daily Caller this week that the NSA records the phone calls of 500,000 to 1 million people
who are on its so-called target list, and perhaps even more. "They look through these phone numbers and they target those and that's what they record," Binney said.

Brewster Kahle, a computer engineer who founded the Internet Archive, has vast experience storing large amounts of data. He created a spreadsheet this week estimating that the cost to store all domestic phone calls a year in cloud storage for data-mining purposes would be about $27 million per year, not counting the cost of extra security for a top-secret program and security clearances for the people involved.

NSA's annual budget is classified but is estimated to be around $10 billion.

Documents that came to light in an EFF lawsuit provide some insight into how the spy agency vacuums up data from telecommunications companies. Mark Klein, who worked as an AT&T technician for over 22 years, disclosed in 2006 (PDF) that he witnessed domestic voice and Internet traffic being surreptitiously "diverted" through a "splitter cabinet" to secure room 641A in one of the company's San Francisco facilities. The room was accessible only to NSA-cleared technicians.

AT&T and other telecommunications companies that allow the NSA to tap into their fiber links receive absolute immunity from civil liability or criminal prosecution, thanks to a law that Congress enacted in 2008 and renewed in 2012. It's a series of amendments to the Foreign Intelligence Surveillance Act, also known as the FISA Amendments Act.

That law says surveillance may be authorized by the attorney general and director of national intelligence without prior approval by the secret Foreign Intelligence Surveillance Court, as long as minimization requirements and general procedures blessed by the court are followed.

A requirement of the 2008 law is that the NSA "may not intentionally target any person known at the time of acquisition to be located in the United States." A possible interpretation of that language, some legal experts said, is that the agency may vacuum up everything it can domestically -- on the theory that indiscriminate data acquisition was not intended to "target" a specific American citizen.
Rep. Jerrold Nadler, an attorney and member of the House Judiciary committee, who said he was "startled" to learn that NSA analysts could eavesdrop on domestic calls without court authorization.

(Credit: Getty Images)

Rep. Nadler's statement that NSA analysts can listen to calls without court orders came during a House Judiciary hearing on June 13 that included FBI director Robert Mueller as a witness.

Mueller initially sought to downplay concerns about NSA surveillance by claiming that, to listen to a phone call, the government would need to seek "a special, a particularized order from the FISA court directed at that particular phone of that particular individual."

Is information about that procedure "classified in any way?" Nadler asked.

"I don't think so," Mueller replied.

"Then I can say the following," Nadler said. "We heard precisely the opposite at the briefing the other day. We heard precisely that you could
get the specific information from that telephone simply based on an analyst deciding that...In other words, what you just said is incorrect. So there's a conflict.

Sen. Dianne Feinstein (D-Calif.), the head of the Senate Intelligence committee, separately acknowledged that the agency's analysts have the ability to access the "content of a call."

Sen. Dianne Feinstein, chair of the Senate Intelligence committee, acknowledged this week that NSA analysts have the ability to access the "content of a call."

(Credit: Getty Images)

Director of National Intelligence Michael McConnell indicated during a House Intelligence hearing in 2007 that the NSA's surveillance process involves "billions" of bulk communications being intercepted, analyzed, and incorporated into a database.
They can be accessed by an analyst who's part of the NSA's "workforce of thousands of people" who are "trained" annually in minimization procedures, he said. (McConnell, who had previously worked as the director of the NSA, is now vice chairman at Booz Allen Hamilton, Snowden's former employer.)

If it were "a U.S. person inside the United States, now that would stimulate the system to get a warrant," McConnell told the committee. "And that is how the process would work. Now, if you have foreign intelligence data, you publish it [inside the federal government]. Because it has foreign intelligence value."

McConnell said during a separate congressional appearance around the same time that he believed the president had the constitutional authority, no matter what the law actually says, to order domestic spying without warrants.

Former FBI counterterrorism agent Tim Clemente told CNN last month that, in national security investigations, the bureau can access records of a previously made telephone call. "All of that stuff is being captured as we speak whether we know it or like it or not," he said. Clemente added in an appearance the next day that, thanks to the "intelligence community" -- an apparent reference to the NSA -- "there's a way to look at digital communications in the past."

NSA Director Keith Alexander said on June 12 that his agency's analysts abide by the law: "They do this lawfully. They take compliance oversight, protecting civil liberties and privacy and the security of this nation to their heart every day."

But that's not always the case. A New York Times article in 2009 revealed the NSA engaged in significant and systemic "overcollection" of Americans' domestic communications that alarmed intelligence officials. The Justice Department said in a statement at the time that it "took comprehensive steps to correct the situation and bring the program into compliance" with the law.

Jameel Jaffer, director of the ACLU's Center for Democracy, says he was surprised to see the 2008 FISA Amendments Act be used to vacuum up information on American citizens. "Everyone who voted for the statute thought it was about international communications," he said.
Updated 6/16 at 11:15 a.m. PT The original headline when the story was published on Saturday was "NSA admits listening to U.S. phone calls without warrants," which was changed to "NSA spying flap extends to contents of U.S. phone calls," to better match the story. The first paragraph was changed to add attribution to Rep. Nadler. Also added was an additional statement that the congressman's aide sent this morning, an excerpt from a Washington Post story on NSA phone call content surveillance that appeared Saturday, and remarks that Rep. Rogers made on CNN this morning.]

Declassified Report Shows Doubts About Value of N.S.A.’s Warrantless Spying - NYTimes.com

See declassified report here (see top Page 8 for confirmation of collection of content):

Declassified Report Shows Doubts About Value of N.S.A.’s Warrantless Spying

By CHARLIE SAVAGE
APRIL 24, 2015

WASHINGTON — The secrecy surrounding the National Security Agency’s post-9/11 warrantless surveillance and bulk data collection program hampered its effectiveness, and many members of the intelligence community later struggled to identify any specific terrorist attacks it thwarted, a newly declassified document shows.

The document is a lengthy report on a once secret N.S.A. program code-named Stellarwind. The report was a joint project in 2009 by
inspectors general for five intelligence and law enforcement agencies, and it was withheld from the public at the time, although a short, unclassified version was made public. The government released a redacted version of the full report to The New York Times on Friday evening in response to a Freedom of Information Act lawsuit.

Shortly after the terrorist attacks on Sept. 11, 2001, President George W. Bush secretly told the N.S.A. that it could wiretap Americans’ international phone calls and collect bulk data about their phone calls and emails without obeying the Foreign Intelligence Surveillance Act. Over time, Stellarwind’s legal basis evolved, and pieces of it emerged into public view, starting with an article in The Times about warrantless wiretapping in 2005.

The report amounts to a detailed history of the program. While significant parts remain classified, it includes some new information. For example, it explains how the Bush administration came to tell the chief judge of the Foreign Intelligence Surveillance Court at the time of the Sept. 11 attacks, Royce C. Lamberth, about the program’s existence in early 2002.

James A. Baker, then the Justice Department’s top intelligence lawyer, had not been told about the program. But he came across “strange, unattributed” language in an application for an ordinary surveillance warrant and figured it out, then insisted on telling Judge Lamberth. Mr. Baker is now the general counsel to the F.B.I.

It also says that Mr. Baker developed procedures to make sure that warrant applications using information from Stellarwind went only to the judges who knew about the program: first Judge Lamberth and then his successor, Judge Colleen Kollar-Kotelly.

The White House would not let Judge Kollar-Kotelly keep a copy of a letter written by a Justice Department lawyer, John C. Yoo, explaining the claimed legal basis of the program, and it rejected a request by Attorney General John Ashcroft to tell his deputy, Larry Thompson, about the program.
The report said that the secrecy surrounding the program made it less useful. Very few working-level C.I.A. analysts were told about it. After the warrantless wiretapping part became public, Congress legalized it in 2007; the report said this should have happened earlier to remove “the substantial restrictions placed on F.B.I. agents’ and analysts’ access to and use of program-derived information due to the highly classified status” of Stellarwind.

In 2003, after Mr. Yoo left the government, other Justice Department officials read his secret memo approving the program — most of which has not been made public — and concluded that it was flawed.

Among other things, the report said, Mr. Yoo’s reasoning was premised on the assumption that the surveillance act, which requires warrants for national security wiretaps, did not expressly apply to wartime situations. His memo did not mention that a provision of that law explains how it applies in war: The warrant rule is suspended for the first 15 days of a war.

The report has new details about a dramatic episode in March 2004, when several Justice Department officials confronted Alberto R. Gonzales, the White House counsel at the time, in the hospital room of Mr. Ashcroft over the legality of the program. The officials included Mr. Thompson’s successor as deputy attorney general, James B. Comey, who is now the F.B.I. director, and the new head of the office where Mr. Yoo had worked, Jack Goldsmith.

The showdown prompted Mr. Bush to make two or three changes to Stellarwind, the report said. But while the report gives a blow-by-blow account of the bureaucratic fight, it censors an explanation of the substance of the legal dispute and Mr. Bush’s changes.

Last year, the Obama administration released a redacted version of a memo that Mr. Goldsmith later wrote about Stellarwind and similarly censored important details.

Nevertheless, it is public knowledge, because of documents leaked by the former intelligence contractor Edward J. Snowden, that one part of
the dispute concerned the legality of the component of Stellarwind that collected bulk records about Americans’ emails.

Mr. Snowden’s disclosures included a working draft version of the N.S.A. inspector general’s contribution to this report, roughly 50 pages long. The final document — with many passages redacted as still classified — was part of Friday’s release.

Another part of the newly disclosed report provides an explanation for a change in F.B.I. rules during the Bush administration. Previously, F.B.I. agents had only two types of cases: “preliminary” and “full” investigations. But the Bush administration created a third, lower-level type called an “assessment.”

This development, it turns out, was a result of Stellarwind. F.B.I. agents were asked to scrutinize phone numbers deemed suspicious because of information from the program. But the agents were not told why the numbers had been deemed suspicious, only “not to use the information in legal or judicial proceedings.”

That made some agents uncomfortable, and it was not clear how such mysterious leads fit into their rules for investigations. The Justice Department created the new type of investigation, initially called a “threat assessment,” which could be opened with lower-grade tips. Agents now use them tens of thousands of times a year.

But little came of the Stellarwind tips. In 2004, the F.B.I. looked at a sampling of all the tips to see how many had made a “significant contribution” to identifying a terrorist, deporting a terrorism suspect, or developing a confidential informant about terrorists.

Just 1.2 percent of the tips from 2001 to 2004 had made such a contribution. Two years later, the F.B.I. reviewed all the leads from the warrantless wiretapping part of Stellarwind between August 2004 and January 2006. None had proved useful.

Still, the report includes several redacted paragraphs describing “success” cases.
The NSA's bulk collection program may soon end, but they may not care

PRI's The World
May 14, 2015 · 6:00 PM EDT

By Joyce Hackel (follow) and Shirin Jaafari (follow)

A view of sensor arrays at a former NSA monitoring base in Bad Aibling in Bavaria, Germany.

Credit: Michaela Rehle/Reuters

Congress is about to decide the future of surveillance, and the US government's bulk data collection program is on the line.

The House of Representatives has approved a bill that would end the National Security Agency's mass data collection, which is currently allowed under Section 215 of the Patriot Act. Rather than allowing the government to simply hold such
records on its own, the bill would have them request needed information from private phone companies like AT&T, Verizon and Sprint. The bill still needs to be approved by the Senate.

Michael Morrell, the CIA’s acting director from 2012 to 2013, said in an interview that the shift is an important check against potential abuse. (Questions and answers have been lightly edited for clarity and space.)

**Michael Morrell:** The government should be required to get a court order every time they want to query the data. That's what I think is the good compromise here. There haven't been any privacy or civil liberty abuses by the NSA in this program, but the government holding this data holds the potential for abuse, and there's been plenty of times in our history when the government has abused its power. So that's what led us to say let's keep the program going but let's take the data out of the hands of the government and force a little bit more oversight in terms of allowing the government to query the data.

**Marco Werman:** There's the case in San Francisco where plaintiffs sued the Justice Department for taking their metadata from AT&T — not to mention people who check in on former girlfriends. So isn't that abuse?

**MM:** Yes, that happened on a couple of occasions at NSA, but that was not this program. One of the problems, Marco, is that when Edward Snowden disclosed this program, the media took this to the scariest corner of the room. You know, the media implied in what it reported — and I remember watching this on CNN — the media reported that the NSA was listening to your phone calls and NSA was reading your emails. I remember listening that first day to CNN say over and over again, "If you call your grandmother in Arkansas, NSA is gonna know." And that's just not true.

**MW:** But NSA can know and does know. You can construct several different pieces of metadata and find out a lot more.

**MM:** Sure, absolutely. And that's why the potential for abuse is there. So if you have — I'm making this up, right? — if you have my phone number and you have what numbers my phone called, right, you can do a Google search, you can find out that my number is me, Michael Morell, and you can do a Google search and you can find
out that I've called a psychiatrist, that I've called a dating service, that I've done all of these things that would be rather embarrassing to me. So yes, you can find that out and that's why there's potential for abuse here. And that's why the review group that I was on unanimously said the government shouldn't hold this data, and you should have a court order every time

MW: There were representatives of the American people in Congress asking Keith Alexander, the former head of the NSA, was there or is there not a bulk data collection program. He said there was not. Was he lying under oath?

MM: Some of the questions were unfairly put, in my view, to representatives of the intelligence community in public, specifically trying to put them on the spot, to make it difficult for them to answer.

MW: But isn't that what a House committee is supposed to do?

MM: Behind the scenes, right. That's where that work gets done. That's why those intelligence committees were created in the first place. That's how they operate, behind the scenes, in secret. I'm not disagreeing with you that there's more room to talk to the American people about this, but there also has to be an understanding that there is a line you can't cross in terms of making things public, because that will advantage our adversaries, number one. And number two, there can't be sole individuals who decide that they're going to leak stuff whenever they think because then there would be leaks every single day of the week.

In a separate interview, David Sanger of the New York Times offered another reason why the NSA might be happy to give up its bulk collection program.

David Sanger: The dirty little secret is that the NSA doesn't really care about this program that much any more. Even before the Snowden revelations, there was a movement within the NSA to say 'Hey, look, we've got a limited amount of money ... for our programs. This one has not yielded very many tips and help in locating terror groups, so would we be better spending our money on some other kind of monitoring program?'

It wasn't that they necessarily objected on any moral or legal ground to Section 215 bulk collection, they just didn't think it was necessarily worth the cash they were
laying out for it. You'll notice you’re not hearing any screaming from the NSA or the Director of the National Intelligence about this House bill. Why is it? Because they have already moved on. They’re thinking about other ways they could spend that money.

**MW:** Do you know how else they could spend that money? Is it something we should be concerned about? How is this going to affect that massive multi-billion dollar complex out in Utah where they’re going to store all this data?

**DS:** Well, the good thing about storing data is there’s lots of other data to store. If you’re the NSA, espionage of the traditional way — listening in to phone calls, all that kind of stuff — is fine. But to some degree it can sort of be left to the summer interns. The high art at the NSA these days is all in the cyber side of things. That’s where the money, the energy and the talent is going.

---


**Revealed: Hundreds of words to avoid using online if you don't want the government spying on you (and they include 'pork', 'cloud' and 'Mexico')**

- Department of Homeland Security forced to release list following freedom of information request
- Agency insists it only looks for evidence of genuine threats to the U.S. and not for signs of general dissent
Revealing: A list of keywords used by government analysts to scour the internet for evidence of threats to the U.S. was released under the Freedom of Information Act.

The Department of Homeland Security has been forced to release a list of keywords and phrases it uses to monitor social networking sites and online media for signs of terrorist or other threats against the U.S.

The intriguing list includes obvious choices such as 'attack', 'Al Qaeda', 'terrorism' and 'dirty bomb' alongside dozens of seemingly innocent words like 'pork', 'cloud', 'team' and 'Mexico'.

Released under a freedom of information request, the information sheds new light on how government analysts are instructed to patrol the internet searching for domestic and external threats.

The words are included in the department's 2011 'Analyst's Desktop Binder' used by workers at their National Operations Center which instructs...
workers to identify 'media reports that reflect adversely on DHS and response activities'.

Department chiefs were forced to release the manual following a House hearing over documents obtained through a Freedom of Information Act lawsuit which revealed how analysts monitor social networks and media organisations for comments that 'reflect adversely' on the government.

However they insisted the practice was aimed not at policing the internet for disparaging remarks about the government and signs of general dissent, but to provide awareness of any potential threats.

As well as terrorism, analysts are instructed to search for evidence of unfolding natural disasters, public health threats and serious crimes such as mall/school shootings, major drug busts, illegal immigrant busts.

The list has been posted online by the Electronic Privacy Information Center - a privacy watchdog group who filed a request under the Freedom of Information Act before suing to obtain the release of the documents.

In a letter to the House Homeland Security Subcommittee on Counter-terrorism and Intelligence, the centre described the choice of words as 'broad, vague and ambiguous'. 
Threat detection: Released under a freedom of information request, the information sheds new light on how government analysts are instructed to patrol the internet searching for domestic and external threats.

They point out that it includes 'vast amounts of First Amendment protected speech that is entirely unrelated to the Department of Homeland Security mission to protect the public against terrorism and disasters.'
A senior Homeland Security official told the Huffington Post that the manual 'is a starting point, not the endgame' in maintaining situational awareness of natural and man-made threats and denied that the government was monitoring signs of dissent.

However the agency admitted that the language used was vague and in need of updating.

Spokesman Matthew Chandler told website: 'To ensure clarity, as part of ... routine compliance review, DHS will review the language contained in all materials to clearly and accurately convey the parameters and intention of the program.'
MIND YOUR LANGUAGE: THE LIST OF KEYWORDS IN FULL
<table>
<thead>
<tr>
<th>Domestic Security</th>
<th>Emergency management</th>
<th>Gangs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assassination</td>
<td>Emergency response</td>
<td>National security</td>
</tr>
<tr>
<td>Attack</td>
<td>First responder</td>
<td>State of emergency</td>
</tr>
<tr>
<td>Domestic security</td>
<td>Homeland security</td>
<td>Security</td>
</tr>
<tr>
<td>Drill</td>
<td>Maritime domain awareness (MDA)</td>
<td>Breach</td>
</tr>
<tr>
<td>Exercise</td>
<td>National preparedness initiative</td>
<td>Threat</td>
</tr>
<tr>
<td>Cops</td>
<td>Militia</td>
<td>Standoff</td>
</tr>
<tr>
<td>Law enforcement</td>
<td>Shooting</td>
<td>SWAT</td>
</tr>
<tr>
<td>Authorities</td>
<td>Shots fired</td>
<td>Screening</td>
</tr>
<tr>
<td>Disaster assistance</td>
<td>Evacuation</td>
<td>Lockdown</td>
</tr>
<tr>
<td>Disaster management</td>
<td>Deaths</td>
<td>Bomb (squad or threat)</td>
</tr>
<tr>
<td>DNDO (Domestic Nuclear Detection Office)</td>
<td>Hostage</td>
<td>Crash</td>
</tr>
<tr>
<td>National preparedness</td>
<td>Explosion (explosive)</td>
<td>Looting</td>
</tr>
<tr>
<td>Mitigation</td>
<td>Police</td>
<td>Riot</td>
</tr>
<tr>
<td>Prevention</td>
<td>Disaster medical assistance team (DMAT)</td>
<td>Emergency Landing</td>
</tr>
<tr>
<td>Response</td>
<td>Organized crime</td>
<td>Pipe bomb</td>
</tr>
<tr>
<td>Recovery</td>
<td></td>
<td>Incident</td>
</tr>
<tr>
<td>Dirty bomb</td>
<td></td>
<td>Facility</td>
</tr>
<tr>
<td>Domestic nuclear detection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| HAZMAT & Nuclear                        |                       |                           |
| Hazmat                                  |                       |                           |
| Nuclear                                 |                       |                           |
| Chemical spill                          |                       |                           |
| Suspicious package/device               |                       |                           |
| Toxic                                   |                       |                           |
| National laboratory                     |                       |                           |
| Nuclear facility                        |                       |                           |
| Nuclear threat                          |                       |                           |
| Cloud                                   |                       |                           |
| Plume                                   |                       |                           |
| Radiation                               |                       |                           |
| Radioactive                             |                       |                           |
| Leak                                    |                       |                           |
| Biological infection (or event)         |                       |                           |
| Chemical                                |                       |                           |
| Chemical burn                           |                       |                           |
| Biological                              |                       |                           |
| Epidemic                                |                       |                           |
| Hazardous                               |                       |                           |
| Hazardous material incident             |                       |                           |
| Industrial spill                        |                       |                           |
| Infection                               |                       |                           |
| Powder (white)                          |                       |                           |
| Gas                                     |                       |                           |
| Spillover                               |                       |                           |
| Anthrax                                 |                       |                           |
| Blister agent                           |                       |                           |
| Chemical agent                          |                       |                           |
| Exposure                                |                       |                           |
| Burn                                    |                       |                           |
| Nerve agent                             |                       |                           |
| Ricin                                    |                       |                           |
| Sarin                                   |                       |                           |
| North Korea                             |                       |                           |

<p>| Health Concern + H1N1                   |                       |                           |
| Outbreak                                |                       |                           |
| Contamination                           |                       |                           |
| Exposure                                |                       |                           |
| Virus                                   |                       |                           |
| Evacuation                              |                       |                           |
| Bacteria                                |                       |                           |
| Recall                                  |                       |                           |
| Ebola                                   |                       |                           |
| Food Poisoning                          |                       |                           |
| Foot and Mouth (FMD)                    |                       |                           |
| H5N1                                    |                       |                           |
| Avian                                   |                       |                           |
| Flu                                     |                       |                           |
| Salmonella                              |                       |                           |
| Small Pox                               |                       |                           |
| Plague                                  |                       |                           |
| Human to human                          |                       |                           |
| Human to Animal                         |                       |                           |
| Influenza                               |                       |                           |
| Center for Disease Control (CDC)        |                       |                           |
| Drug Administration (FDA)               |                       |                           |
| Public Health                           |                       |                           |
| Toxic                                   |                       |                           |
| Agro Terror                             |                       |                           |
| Tuberculosis (TB)                       |                       |                           |
| Agriculture                             |                       |                           |
| Listeria                                |                       |                           |
| Symptoms                                |                       |                           |
| Mutation                                |                       |                           |
| Resistant                               |                       |                           |
| Antiviral                               |                       |                           |
| Wave                                    |                       |                           |
| Pandemic                                |                       |                           |
| Infection                               |                       |                           |
| Water/air borne                         |                       |                           |
| Sick                                    |                       |                           |
| Swine                                   |                       |                           |
| Pork                                    |                       |                           |</p>
<table>
<thead>
<tr>
<th>Strain</th>
<th>Tamiflu</th>
<th>World Health Organization (WHO) (and components)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine</td>
<td>Norovirus</td>
<td>Viral Hemorrhagic Fever</td>
</tr>
<tr>
<td>H1N1</td>
<td>Epidemic</td>
<td>E. Coli</td>
</tr>
</tbody>
</table>

**Infrastructure Security**

<table>
<thead>
<tr>
<th>Infrastructure security</th>
<th>Airplane (and derivatives)</th>
<th>Chemical fire</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airport</td>
<td>Subway</td>
<td>Electric</td>
</tr>
<tr>
<td>CIKR (Critical Infrastructure &amp; Key Resources)</td>
<td>BART</td>
<td>Failure or outage</td>
</tr>
<tr>
<td>AMTRAK</td>
<td>MARTA</td>
<td>Black out</td>
</tr>
<tr>
<td>Collapse</td>
<td>Port Authority</td>
<td>Brown out</td>
</tr>
<tr>
<td>Computer infrastructure</td>
<td>NBIC (National Biosurveillance Integration Center)</td>
<td>Port</td>
</tr>
<tr>
<td>Communications infrastructure</td>
<td>Transportation security</td>
<td>Dock</td>
</tr>
<tr>
<td>Critical infrastructure</td>
<td>Grid</td>
<td>Bridge</td>
</tr>
<tr>
<td>National infrastructure</td>
<td>Power</td>
<td>Cancelled</td>
</tr>
<tr>
<td>Metro</td>
<td>Smart</td>
<td>Delays</td>
</tr>
<tr>
<td>WMATA</td>
<td>Body scanner</td>
<td>Service disruption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Power lines</td>
</tr>
</tbody>
</table>

**Southwest Border Violence**

<table>
<thead>
<tr>
<th>Drug cartel</th>
<th>Fort Hancock</th>
<th>Gunfight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Violence</td>
<td>San Diego</td>
<td>Trafficking</td>
</tr>
<tr>
<td>Gang</td>
<td>Ciudad Juarez</td>
<td>Kidnap</td>
</tr>
<tr>
<td>Drug</td>
<td>Nogales</td>
<td>Calderon</td>
</tr>
<tr>
<td>Narcotics</td>
<td>Sonora</td>
<td>Reyosa</td>
</tr>
<tr>
<td>Cocaine</td>
<td>Colombia</td>
<td>Bust</td>
</tr>
<tr>
<td>Marijuana</td>
<td>Mara salvatrucha</td>
<td>Tamaulipas</td>
</tr>
<tr>
<td>Heroin</td>
<td>MS13 or MS-13</td>
<td>Meth Lab</td>
</tr>
<tr>
<td>Border</td>
<td>Drug war</td>
<td>Drug trade</td>
</tr>
<tr>
<td>Mexico</td>
<td>Mexican army</td>
<td>Illegal immigrants</td>
</tr>
<tr>
<td>Cartel</td>
<td>Methamphetamine</td>
<td>Smuggling (smugglers)</td>
</tr>
<tr>
<td>Southwest</td>
<td>Cartel de Golfo</td>
<td>Matamoros</td>
</tr>
<tr>
<td>Juarez</td>
<td>Gulf Cartel</td>
<td>Michoacana</td>
</tr>
<tr>
<td>Sinaloa</td>
<td>La Familia</td>
<td>Guzman</td>
</tr>
<tr>
<td>Tijuana</td>
<td>Reynosa</td>
<td>Arellano-Felix</td>
</tr>
<tr>
<td>Torreon</td>
<td>Nuevo Leon</td>
<td>Beltran-Leyva</td>
</tr>
<tr>
<td>Yuma</td>
<td>Narcos</td>
<td>Barrio Azteca</td>
</tr>
<tr>
<td>Tucson</td>
<td>Narco banners (Spanish equivalents)</td>
<td>Artistic Assassins</td>
</tr>
<tr>
<td>Decapitated</td>
<td>Los Zetas</td>
<td>Mexicles</td>
</tr>
<tr>
<td>U.S. Consulate</td>
<td>Shootout</td>
<td>New Federation</td>
</tr>
<tr>
<td>Consular</td>
<td>Execution</td>
<td></td>
</tr>
<tr>
<td>El Paso</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A secretive U.S. Drug Enforcement Administration unit is funneling information from intelligence intercepts, wiretaps, informants and a massive database of telephone records to authorities across the nation to help them launch criminal investigations of Americans.

Although these cases rarely involve national security issues, documents reviewed by Reuters show that law enforcement agents have been directed to conceal how such investigations truly begin - not only from defense lawyers but also sometimes from prosecutors and judges.

The undated documents show that federal agents are trained to "recreate" the investigative trail to effectively cover up where the information originated, a practice that some experts say violates a defendant's Constitutional right to a fair trial. If defendants don't know how an investigation began, they cannot know to ask to review potential sources of exculpatory evidence - information that could reveal entrapment, mistakes or biased witnesses.

"I have never heard of anything like this at all," said Nancy Gertner, a Harvard Law School professor who served as a federal judge from 1994 to 2011. Gertner and other legal experts said the program sounds more
troubling than recent disclosures that the National Security Agency has been collecting domestic phone records. The NSA effort is geared toward stopping terrorists; the DEA program targets common criminals, primarily drug dealers.

"It is one thing to create special rules for national security," Gertner said. "Ordinary crime is entirely different. It sounds like they are phonying up investigations."

THE SPECIAL OPERATIONS DIVISION

The unit of the DEA that distributes the information is called the Special Operations Division, or SOD. Two dozen partner agencies comprise the unit, including the FBI, CIA, NSA, Internal Revenue Service and the Department of Homeland Security. It was created in 1994 to combat Latin American drug cartels and has grown from several dozen employees to several hundred.

Today, much of the SOD's work is classified, and officials asked that its precise location in Virginia not be revealed. The documents reviewed by Reuters are marked "Law Enforcement Sensitive," a government categorization that is meant to keep them confidential.

"Remember that the utilization of SOD cannot be revealed or discussed in any investigative function," a document presented to agents reads. The document specifically directs agents to omit the SOD's involvement from investigative reports, affidavits, discussions with prosecutors and courtroom testimony. Agents are instructed to then use "normal investigative techniques to recreate the information provided by SOD."

A spokesman with the Department of Justice, which oversees the DEA, declined to comment.
But two senior DEA officials defended the program, and said trying to "recreate" an investigative trail is not only legal but a technique that is used almost daily.

A former federal agent in the northeastern United States who received such tips from SOD described the process. "You'd be told only, 'Be at a certain truck stop at a certain time and look for a certain vehicle.' And so we'd alert the state police to find an excuse to stop that vehicle, and then have a drug dog search it," the agent said.

"PARALLEL CONSTRUCTION"

After an arrest was made, agents then pretended that their investigation began with the traffic stop, not with the SOD tip, the former agent said. The training document reviewed by Reuters refers to this process as "parallel construction."

The two senior DEA officials, who spoke on behalf of the agency but only on condition of anonymity, said the process is kept secret to protect sources and investigative methods. "Parallel construction is a law enforcement technique we use every day," one official said. "It's decades old, a bedrock concept."

A dozen current or former federal agents interviewed by Reuters confirmed they had used parallel construction during their careers. Most defended the practice; some said they understood why those outside law enforcement might be concerned.

RELATED COVERAGE

- How DEA program differs from recent NSA revelations

"It's just like laundering money - you work it backwards to make it clean," said Finn Selander, a DEA agent from 1991 to 2008 and now a member of a group called Law Enforcement Against Prohibition, which advocates legalizing and regulating narcotics.
Some defense lawyers and former prosecutors said that using "parallel construction" may be legal to establish probable cause for an arrest. But they said employing the practice as a means of disguising how an investigation began may violate pretrial discovery rules by burying evidence that could prove useful to criminal defendants.

A QUESTION OF CONSTITUTIONALITY

"That's outrageous," said Tampa attorney James Felman, a vice chairman of the criminal justice section of the American Bar Association. "It strikes me as indefensible."

Lawrence Lustberg, a New Jersey defense lawyer, said any systematic government effort to conceal the circumstances under which cases begin "would not only be alarming but pretty blatantly unconstitutional."

Lustberg and others said the government's use of the SOD program skirts established court procedures by which judges privately examine sensitive information, such as an informant's identity or classified evidence, to determine whether the information is relevant to the defense.

"You can't game the system," said former federal prosecutor Henry E. Hockeimer Jr. "You can't create this subterfuge. These are drug crimes, not national security cases. If you don't draw the line here, where do you draw it?"

Some lawyers say there can be legitimate reasons for not revealing sources. Robert Spelke, a former prosecutor who spent seven years as a senior DEA lawyer, said some sources are classified. But he also said there are few reasons why unclassified evidence should be concealed at trial.

"It's a balancing act, and they've doing it this way for years," Spelke said. "Do I think it's a good way to do it? No, because now that I'm a defense lawyer, I see how difficult it is to challenge."
CONCEALING A TIP

One current federal prosecutor learned how agents were using SOD tips after a drug agent misled him, the prosecutor told Reuters. In a Florida drug case he was handling, the prosecutor said, a DEA agent told him the investigation of a U.S. citizen began with a tip from an informant. When the prosecutor pressed for more information, he said, a DEA supervisor intervened and revealed that the tip had actually come through the SOD and from an NSA intercept.

"I was pissed," the prosecutor said. "Lying about where the information came from is a bad start if you're trying to comply with the law because it can lead to all kinds of problems with discovery and candor to the court." The prosecutor never filed charges in the case because he lost confidence in the investigation, he said.

A senior DEA official said he was not aware of the case but said the agent should not have misled the prosecutor. How often such misdirection occurs is unknown, even to the government; the DEA official said the agency does not track what happens with tips after the SOD sends them to agents in the field.

The SOD's role providing information to agents isn't itself a secret. It is briefly mentioned by the DEA in budget documents, albeit without any reference to how that information is used or represented when cases go to court.

The DEA has long publicly touted the SOD's role in multi-jurisdictional and international investigations, connecting agents in separate cities who may be unwittingly investigating the same target and making sure undercover agents don't accidentally try to arrest each other.

SOD'S BIG SUCCESSES
The unit also played a major role in a 2008 DEA sting in Thailand against Russian arms dealer Viktor Bout; he was sentenced in 2011 to 25 years in prison on charges of conspiring to sell weapons to the Colombian rebel group FARC. The SOD also recently coordinated Project Synergy, a crackdown against manufacturers, wholesalers and retailers of synthetic designer drugs that spanned 35 states and resulted in 227 arrests.

Since its inception, the SOD's mandate has expanded to include narco-terrorism, organized crime and gangs. A DEA spokesman declined to comment on the unit's annual budget. A recent LinkedIn posting on the personal page of a senior SOD official estimated it to be $125 million.

Today, the SOD offers at least three services to federal, state and local law enforcement agents: coordinating international investigations such as the Bout case; distributing tips from overseas NSA intercepts, informants, foreign law enforcement partners and domestic wiretaps; and circulating tips from a massive database known as DICE.

The DICE database contains about 1 billion records, the senior DEA officials said. The majority of the records consist of phone log and Internet data gathered legally by the DEA through subpoenas, arrests and search warrants nationwide. Records are kept for about a year and then purged, the DEA officials said.

About 10,000 federal, state and local law enforcement agents have access to the DICE database, records show. They can query it to try to link otherwise disparate clues. Recently, one of the DEA officials said, DICE linked a man who tried to smuggle $100,000 over the U.S. southwest border to a major drug case on the East Coast.

"We use it to connect the dots," the official said.

"AN AMAZING TOOL"
Wiretap tips forwarded by the SOD usually come from foreign governments, U.S. intelligence agencies or court-authorized domestic phone recordings. Because warrantless eavesdropping on Americans is illegal, tips from intelligence agencies are generally not forwarded to the SOD until a caller's citizenship can be verified, according to one senior law enforcement official and one former U.S. military intelligence analyst.

"They do a pretty good job of screening, but it can be a struggle to know for sure whether the person on a wiretap is American," the senior law enforcement official said.

Tips from domestic wiretaps typically occur when agents use information gleaned from a court-ordered wiretap in one case to start a second investigation.

As a practical matter, law enforcement agents said they usually don't worry that SOD's involvement will be exposed in court. That's because most drug-trafficking defendants plead guilty before trial and therefore never request to see the evidence against them. If cases did go to trial, current and former agents said, charges were sometimes dropped to avoid the risk of exposing SOD involvement.

Current and former federal agents said SOD tips aren't always helpful - one estimated their accuracy at 60 percent. But current and former agents said tips have enabled them to catch drug smugglers who might have gotten away.

"It was an amazing tool," said one recently retired federal agent. "Our big fear was that it wouldn't stay secret."

DEA officials said that the SOD process has been reviewed internally. They declined to provide Reuters with a copy of their most recent review.

(Edited by Blake Morrison)
A slide from a presentation about a secretive information-sharing program run by the U.S. Drug Enforcement Administration's Special Operations Division (SOD) is seen in this undated photo.

REUTERS/JOHN SHIFFMAN


DEA agents use NSA intercepts to investigate Americans – report

Published time: August 05, 2013 19:40
Agents of a secretive DEA unit routinely receive tips from US intelligence agencies, including NSA intercepts, a report states. The sources are then concealed with "parallel construction" of evidence – a troubling practice that many call unconstitutional.

A document obtained by Reuters “specifically directs” the agents of the Special Operations Division (SOD) to cover up their information sources from investigative reports, affidavits, discussions with prosecutors and courtroom testimony.

Such sources may include intelligence intercepts, wiretaps, three-letter-agencies' informants and a massive database of telephone records – all of which could reportedly be used to help the authorities launch criminal investigations of Americans.

“Remember that the utilization of SOD cannot be revealed or discussed in any investigative function,” reads the document, which is said to be presented to the agents of this Drug Enforcement Administration (DEA) unit.
SOD is comprised of two dozen partner agencies, which include the FBI, CIA, NSA, Internal Revenue Service and the Department of Homeland Security, and much of the unit’s work is classified.

The unit is said to be offering at least three services to federal, state and local law enforcement agents: coordinating international investigations; distributing tips from overseas NSA intercepts, informants, foreign law enforcement partners and domestic wiretaps; and circulating tips from a massive database known as DICE.

Instead of revealing the agencies’ part in any launch of a criminal case, the agents are instructed to use “normal investigative techniques to recreate the information provided by SOD.”
This in effect means certain “tips” might be given to the agents and the police on condition they never talk about them in court.

A former US federal agent who received such tips from SOD described the process to Reuters. “You’d be told only, ‘Be at a certain truck stop at a certain time and look for a certain vehicle.’ And so we’d alert the state police to find an excuse to stop that vehicle, and then have a drug dog search it.”

Following the arrest, the agents would then pretend the investigation started with the traffic stop, he said.

This process, referred to as “parallel construction,” is a routine practice used by the agents, two senior DEA officials told the news agency, speaking on condition of anonymity.
“Parallel construction is a law enforcement technique we use every day,” one official said, adding that it was “decades old, a bedrock concept” that was used to protect sources and investigative methods.

While most of “a dozen” of other agents interviewed by Reuters were said to have defended the tactics as “legal,” former DEA agent Finn Selander has compared it to a criminal activity.

“It’s just like laundering money – you work it backwards to make it clean,” Selander, who is now a member of the Law Enforcement Against Prohibition group, explained.

‘Blatantly unconstitutional’

Meanwhile, lawyers, prosecutors and legal experts have been outraged by the report, saying that if the so-called “parallel construction” was indeed used for disguising how an investigation began it explicitly violates pretrial discovery rules.

Such practice “would not only be alarming but pretty blatantly unconstitutional,” Lawrence Lustberg, a New Jersey defense lawyer has said.

In particular, it would violate the defendants’ Constitutional right to a fair trial, since if they don’t know how an investigation really began, they cannot ask to review potential sources of exculpatory evidence – information that could reveal entrapment, mistakes or biased witnesses.

By use of the SOD program the US government could also “skirt” the established court procedures, by which judges privately examine sensitive information (informant’s identity, classified evidence etc.) to determine whether the information is relevant to the defense – something which some lawyers find unacceptable.

“You can’t game the system. You can’t create this subterfuge. These are drug crimes, not national security cases. If you don’t draw the line here, where do you draw it?” said former federal prosecutor Henry E. Hockeimer Jr.

The US legal system is very sensitive to the way the evidence is handled, and if the defense or prosecution finds its source inappropriate, the case may be overturned.
An unnamed federal prosecutor said he refused to file charges in a Florida drug case after he learned a DEA agent “lied” to him about where the information came from – it was later revealed he had actually used a SOD tip based on an NSA intercept. The prosecutor said the fact of concealing the information source alone made him lose confidence in the investigation.

Nancy Gertner, a Harvard Law School professor who served as a federal judge for 17 years, said the report sounds more troubling than recent Edward Snowden revelations that the NSA has been indiscriminately collecting domestic phone records.

“It is one thing to create special rules for national security. Ordinary crime is entirely different.”
It sounds like they are phonying up investigations,” Gertner believes.

The Special Operations Division was created in 1994 to initially combat Latin American drug cartels, and has since grown from several dozen employees to several hundred.

Since its inception, the SOD’s mandate has expanded to include narco-terrorism, organized crime and gangs. A recent LinkedIn posting on the personal page of a senior SOD official reportedly estimated the unit’s annual budget to be $125 million.

The unit played a major role in the case against Russian arms dealer Viktor Bout, who was extradited to the US from Thailand and in 2011 sentenced to 25 years in jail on charges of conspiring to sell weapons to the Colombian rebel group FARC.

According to DEA officials, the DICE database they use contains about 1 billion records and largely consists of phone logs and Internet data gathered legally by the DEA through subpoenas, arrests and search warrants nationwide. Those records are said to be kept for
about a year and then purged.

About 10,000 federal, state and local law enforcement agents use the DICE database “to connect the dots,” according to an official cited by Reuters.

But the DEA official insists that tips from intelligence agencies, such as the NSA, are generally not forwarded to the SOD until a caller’s citizenship can be verified, as warrantless eavesdropping on Americans is illegal.

U.S. Government Sends Copies of Transcripts Containing Phone Conversations between Al Haramain and its Lawyers

See Court record here: www.eff.org/files/filenode/att/al-haramain.pdf

The contents of a phone call could be accessed "simply based on an analyst deciding that."


NSA admits listening to U.S. phone calls without warrants

National Security Agency discloses in secret Capitol Hill briefing that thousands of analysts can listen to domestic phone calls. That authorization appears to extend to e-mail and text messages too.
The National Security Agency has acknowledged in a new classified briefing that it does not need court authorization to listen to domestic phone calls.

Rep. Jerrold Nadler, a New York Democrat, disclosed this week that during a secret briefing to members of Congress, he was told that the contents of a phone call could be accessed "simply based on an analyst deciding that."

If the NSA wants "to listen to the phone," an analyst's decision is sufficient, without any other legal authorization required, Nadler said he learned. "I was rather startled," said Nadler, an attorney and congressman who serves on the House Judiciary committee.

Not only does this disclosure shed more light on how the NSA's formidable eavesdropping apparatus works domestically it also suggests the Justice Department has secretly interpreted federal surveillance law to permit thousands of low-ranking analysts to eavesdrop on phone calls.

Because the same legal standards that apply to phone calls also apply to e-mail messages, text messages, and instant messages, Nadler's disclosure indicates the NSA analysts could also access the contents of Internet communications without going before a court and seeking approval.

The disclosure appears to confirm some of the allegations made by Edward Snowden, a former NSA infrastructure analyst who leaked classified documents to the Guardian. Snowden said in a video interview that, while not all NSA analysts had this ability, he could from Hawaii "wiretap anyone from you or your accountant to a federal judge to even the president."
There are serious "constitutional problems" with this approach, said Kurt Opsahl, a senior staff attorney at the Electronic Frontier Foundation who has litigated warrantless wiretapping cases. "It epitomizes the problem of secret laws."

The NSA yesterday declined to comment to CNET. A representative said Nadler was not immediately available. (This is unrelated to last week's disclosure that the NSA is currently collecting records of the metadata of all domestic Verizon calls, but not the actual contents of the conversations.)

Earlier reports have indicated that the NSA has the ability to record nearly all domestic and international phone calls -- in case an analyst needed to access the recordings in the future. A Wired magazine article last year disclosed that the NSA has established "listening posts" that allow the agency to collect and sift through billions of phone calls through a massive new data center in Utah, "whether they originate within the country or overseas." That includes not just metadata, but also the contents of the communications.

William Binney, a former NSA technical director who helped to modernize the agency's worldwide eavesdropping network, told the Daily Caller this week that the NSA records the phone calls of 500,000 to 1 million people who are on its so-called target list, and perhaps even more. "They look through these phone numbers and they target those and that's what they record," Binney said.

Brewster Khale, a computer engineer who founded the Internet Archive, has vast experience storing large amounts of data. He created a spreadsheet this week estimating that the cost to store all domestic phone calls a year in cloud storage for data-mining purposes would be about $27 million per year, not counting the cost of extra security for a top-secret program and security clearances for the people involved.

NSA's annual budget is classified but is estimated to be around $10 billion.

Documents that came to light in an EFF lawsuit provide some insight into how the spy agency vacuums up data from telecommunications companies. Mark Klein, who worked as an AT&T technician for over 22 years, disclosed in 2006 (PDF) that he witnessed domestic voice and Internet traffic being surreptitiously "diverted" through a "splitter cabinet" to
secure room 641A in one of the company's San Francisco facilities. The
room was accessible only to NSA-cleared technicians.

AT&T and other telecommunications companies that allow the NSA to tap
into their fiber links receive absolute immunity from civil liability or criminal
prosecution, thanks to a law that Congress enacted in 2008 and renewed in
2012. It's a series of amendments to the Foreign Intelligence Surveillance Act,
also known as the FISA Amendments Act.

That law says surveillance may be authorized by the attorney general and
director of national intelligence without prior approval by the secret Foreign
Intelligence Surveillance Court, as long as minimization requirements and
general procedures blessed by the court are followed.

A requirement of the 2008 law is that the NSA "may not intentionally target
any person known at the time of acquisition to be located in the United
States." A possible interpretation of that language, some legal experts said,
is that the agency may vacuum up everything it can domestically -- on the
theory that indiscriminate data acquisition was not intended to "target" a
specific American citizen.

Rep. Jerrold Nadler, an attorney and member of the House Judiciary
committee, who said he was "startled" to learn that NSA analysts could
eavesdrop on domestic calls without court authorization.

Rep. Nadler's disclosure that NSA analysts can listen to calls without court
orders came during a House Judiciary hearing on Thursday that included
FBI director Robert Mueller as a witness.

Mueller initially sought to downplay concerns about NSA surveillance by
claiming that, to listen to a phone call, the government would need to seek
"a special, a particularized order from the FISA court directed at that
particular phone of that particular individual."

Is information about that procedure "classified in any way?" Nadler asked.

"I don't think so," Mueller replied.

"Then I can say the following," Nadler said. "We heard precisely the
opposite at the briefing the other day. We heard precisely that you could
get the specific information from that telephone simply based on an analyst deciding that...In other words, what you just said is incorrect. So there's a conflict."

Sen. Dianne Feinstein (D-Calif.), the head of the Senate Intelligence committee, separately acknowledged this week that the agency's analysts have the ability to access the "content of a call."

Director of National Intelligence Michael McConnell indicated during a House Intelligence hearing in 2007 that the NSA's surveillance process involves "billions" of bulk communications being intercepted, analyzed, and incorporated into a database.

They can be accessed by an analyst who's part of the NSA's "workforce of thousands of people" who are "trained" annually in minimization procedures, he said. (McConnell, who had previously worked as the director of the NSA, is now vice chairman at Booz Allen Hamilton, Snowden's former employer.)

If it were "a U.S. person inside the United States, now that would stimulate the system to get a warrant," McConnell told the committee. "And that is how the process would work. Now, if you have foreign intelligence data, you publish it [inside the federal government]. Because it has foreign intelligence value."

McConnell said during a separate congressional appearance around the same time that he believed the president had the constitutional authority, no matter what the law actually says, to order domestic spying without warrants.

Former FBI counterterrorism agent Tim Clemente told CNN last month that, in national security investigations, the bureau can access records of a previously made telephone call. "All of that stuff is being captured as we speak whether we know it or like it or not," he said. Clemente added in an appearance the next day that, thanks to the "intelligence community" -- an apparent reference to the NSA -- "there's a way to look at digital communications in the past."

NSA Director Keith Alexander said this week that his agency's analysts abide by the law: "They do this lawfully. They take compliance oversight,"
protecting civil liberties and privacy and the security of this nation to their heart every day."

But that's not always the case. A New York Times article in 2009 revealed the NSA engaged in significant and systemic "overcollection" of Americans' domestic communications that alarmed intelligence officials. The Justice Department said in a statement at the time that it "took comprehensive steps to correct the situation and bring the program into compliance" with the law.

Jameel Jaffer, director of the ACLU's Center for Democracy, says he was surprised to see the 2008 FISA Amendments Act be used to vacuum up information on American citizens. "Everyone who voted for the statute thought it was about international communications," he said.

Declan McCullagh is the chief political correspondent for CNET. Declan previously was a reporter for Time and the Washington bureau chief for Wired and wrote the Taking Liberties section and Other People's Money column for CBS News' Web site.

In NSA-intercepted data, those not targeted far outnumber the foreigners who are.

Files provided by Snowden show extent to which ordinary Web users are caught in the net.
Ordinary Internet users, American and non-American alike, far outnumber legally targeted foreigners in the communications intercepted by the National Security Agency from U.S. digital networks, according to a four-month investigation by The Washington Post.

Nine of 10 account holders found in a large cache of intercepted conversations, which former NSA contractor Edward Snowden provided in full to The Post, were not the intended surveillance targets but were caught in a net the agency had cast for somebody else.

Many of them were Americans. Nearly half of the surveillance files, a strikingly high proportion, contained names, e-mail addresses or other details that the NSA marked as belonging to U.S. citizens or residents. NSA analysts masked, or “minimized,” more than 65,000 such references to protect Americans’ privacy, but The Post found nearly 900 additional e-mail addresses, unmasked in the files, that could be strongly linked to U.S. citizens or U.S. residents.
The surveillance files highlight a policy dilemma that has been aired only abstractly in public. There are discoveries of considerable intelligence value in the intercepted messages — and collateral harm to privacy on a scale that the Obama administration has not been willing to address.

Among the most valuable contents — which The Post will not describe in detail, to avoid interfering with ongoing operations — are fresh revelations about a secret overseas nuclear project, double-dealing by an ostensible ally, a military calamity that befell an unfriendly power, and the identities of aggressive intruders into U.S. computer networks.

Months of tracking communications across more than 50 alias accounts, the files show, led directly to the 2011 capture in Abbottabad of Muhammad Tahir Shahzad, a Pakistan-based bomb builder, and Umar Patek, a suspect in a 2002 terrorist bombing on the Indonesian island of Bali. At the request of CIA officials, The Post is withholding other examples that officials said would compromise ongoing operations.

Many other files, described as useless by the analysts but nonetheless retained, have a startlingly intimate, even voyeuristic quality. They tell stories of love and heartbreak, illicit sexual liaisons, mental-health crises, political and religious conversions, financial anxieties
and disappointed hopes. The daily lives of more than 10,000 account holders who were not targeted are catalogued and recorded nevertheless.

In order to allow time for analysis and outside reporting, neither Snowden nor The Post has disclosed until now that he obtained and shared the content of intercepted communications. The cache Snowden provided came from domestic NSA operations under the broad authority granted by Congress in 2008 with amendments to the Foreign Intelligence Surveillance Act. FISA content is generally stored in closely controlled data repositories, and for more than a year, senior government officials have depicted it as beyond Snowden’s reach.

The Post reviewed roughly 160,000 intercepted e-mail and instant-message conversations, some of them hundreds of pages long, and 7,900 documents taken from more than 11,000 online accounts.

The material spans President Obama’s first term, from 2009 to 2012, a period of exponential growth for the NSA’s domestic collection.

A composite image of two of the more than 5,000 private photos among data collected by the National Security Agency from online accounts and network links in the United States. The images were included in a large cache of NSA intercepts provided by former agency contractor Edward Snowden. (Images obtained by The Washington Post)
Taken together, the files offer an unprecedented vantage point on the changes wrought by Section 702 of the FISA amendments, which enabled the NSA to make freer use of methods that for 30 years had required probable cause and a warrant from a judge. One program, code-named PRISM, extracts content stored in user accounts at Yahoo, Microsoft, Facebook, Google and five other leading Internet companies. Another, known inside the NSA as Upstream, intercepts data on the move as it crosses the U.S. junctions of global voice and data networks.

No government oversight body, including the Justice Department, the Foreign Intelligence Surveillance Court, intelligence committees in Congress or the president’s Privacy and Civil Liberties Oversight Board, has delved into a comparably large sample of what the NSA actually collects — not only from its targets but also from people who may cross a target’s path.

Among the latter are medical records sent from one family member to another, résumés from job hunters and academic transcripts of schoolchildren. In one photo, a young girl in religious dress beams at a camera outside a mosque.

Scores of pictures show infants and toddlers in bathtubs, on swings, sprawled on their backs and kissed by their mothers. In some photos, men show off their physiques. In others, women model lingerie, leaning suggestively into a webcam or striking risque poses in shorts and bikini tops.

“None of the hits that were received were relevant,” two Navy cryptologic technicians write in one of many summaries of nonproductive surveillance. “No additional information,” writes a civilian analyst. Another makes fun of a suspected kidnapper, newly arrived in Syria before the current civil war, who begs for employment as a janitor and makes wide-eyed observations about the state of undress displayed by women on local beaches.

By law, the NSA may “target” only foreign nationals located overseas unless it obtains a warrant based on probable cause from a special surveillance court. For collection under
PRISM and Upstream rules, analysts must state a reasonable belief that the target has information of value about a foreign government, a terrorist organization or the spread of nonconventional weapons.

Most of the people caught up in those programs are not the targets and would not lawfully qualify as such. “Incidental collection” of third-party communications is inevitable in many forms of surveillance, but in other contexts the U.S. government works harder to limit and discard irrelevant data. In criminal wiretaps, for example, the FBI is supposed to stop listening to a call if a suspect’s wife or child is using the phone.

There are many ways to be swept up incidentally in surveillance aimed at a valid foreign target. Some of those in the Snowden archive were monitored because they interacted directly with a target, but others had more-tenuous links.

If a target entered an online chat room, the NSA collected the words and identities of every person who posted there, regardless of subject, as well as every person who simply “lurked,” reading passively what other people wrote.

“1 target, 38 others on there,” one analyst wrote. She collected data on them all.

In other cases, the NSA designated as its target the Internet protocol, or IP, address of a computer server used by hundreds of people.

The NSA treats all content intercepted incidentally from third parties as permissible to retain, store, search and distribute to its government customers. Raj De, the agency’s general counsel, has testified that the NSA does not generally attempt to remove irrelevant personal content, because it is difficult for one analyst to know what might become relevant to another.

The Obama administration declines to discuss the scale of incidental collection. The NSA, backed by Director of National Intelligence James R. Clapper Jr., has asserted that it is unable to make any estimate, even in classified form, of the number of Americans swept in.
It is not obvious why the NSA could not offer at least a partial count, given that its analysts routinely pick out “U.S. persons” and mask their identities, in most cases, before distributing intelligence reports.

If Snowden’s sample is representative, the population under scrutiny in the PRISM and Upstream programs is far larger than the government has suggested. In a June 26 “transparency report,” the Office of the Director of National Intelligence disclosed that 89,138 people were targets of last year’s collection under FISA Section 702. At the 9-to-1 ratio of incidental collection in Snowden’s sample, the office’s figure would correspond to nearly 900,000 accounts, targeted or not, under surveillance.

‘He didn’t get this data’

U.S. intelligence officials declined to confirm or deny in general terms the authenticity of the intercepted content provided by Snowden, but they made off-the-record requests to withhold specific details that they said would alert the targets of ongoing surveillance. Some officials, who declined to be quoted by name, described Snowden’s handling of the sensitive files as reckless.

In an interview, Snowden said “primary documents” offered the only path to a concrete debate about the costs and benefits of Section 702 surveillance. He did not favor public release of the full archive, he said, but he did not think a reporter could understand the programs “without being able to review some of that surveillance, both the justified and unjustified.”

“While people may disagree about where to draw the line on publication, I know that you and The Post have enough sense of civic duty to consult with the government to ensure that the reporting on and handling of this material causes no harm,” he said.

In Snowden’s view, the PRISM and Upstream programs have “crossed the line of proportionality.”
“Even if one could conceivably justify the initial, inadvertent interception of baby pictures and love letters of innocent bystanders,” he added, “their continued storage in government databases is both troubling and dangerous. Who knows how that information will be used in the future?”

For close to a year, NSA and other government officials have appeared to deny, in congressional testimony and public statements, that Snowden had any access to the material.

As recently as May, shortly after he retired as NSA director, Gen. Keith Alexander denied that Snowden could have passed FISA content to journalists.

“He didn’t get this data,” Alexander told a New Yorker reporter. “They didn’t touch —”

“The operational data?” the reporter asked.

“They didn’t touch the FISA data,” Alexander replied. He added, “That database, he didn’t have access to.”

Robert S. Litt, the general counsel for the Office of the Director of National Intelligence, said in a prepared statement that Alexander and other officials were speaking only about “raw” intelligence, the term for intercepted content that has not yet been evaluated, stamped with classification markings or minimized to mask U.S. identities.

“We have talked about the very strict controls on raw traffic, the training that people have to have, the technological lockdowns on access,” Litt said. “Nothing that you have given us indicates that Snowden was able to circumvent that in any way.”

In the interview, Snowden said he did not need to circumvent those controls, because his final position as a contractor for Booz Allen at the NSA’s Hawaii operations center gave him “unusually broad, unescorted access to raw SIGINT [signals intelligence] under a special ‘Dual Authorities’ role,” a reference to Section 702 for domestic collection and Executive
Order 12333 for collection overseas. Those credentials, he said, allowed him to search stored content — and “task” new collection — without prior approval of his search terms.

“If I had wanted to pull a copy of a judge’s or a senator’s e-mail, all I had to do was enter that selector into XKEYSCORE,” one of the NSA’s main query systems, he said.

The NSA has released an e-mail exchange acknowledging that Snowden took the required training classes for access to those systems.

‘Minimized U.S. president’
At one level, the NSA shows scrupulous care in protecting the privacy of U.S. nationals and, by policy, those of its four closest intelligence allies — Britain, Australia, Canada and New Zealand.

More than 1,000 distinct “minimization” terms appear in the files, attempting to mask the identities of “possible,” “potential” and “probable” U.S. persons, along with the names of U.S. beverage companies, universities, fast-food chains and Web-mail hosts.

Some of them border on the absurd, using titles that could apply to only one man. A “minimized U.S. president-elect” begins to appear in the files in early 2009, and references to the current “minimized U.S. president” appear 1,227 times in the following four years.

Even so, unmasked identities remain in the NSA’s files, and the agency’s policy is to hold on to “incidentally” collected U.S. content, even if it does not appear to contain foreign intelligence.

In one exchange captured in the files, a young American asks a Pakistani friend in late 2009 what he thinks of the war in Afghanistan. The Pakistani replies that it is a religious struggle against 44 enemy states.
Startled, the American says “they, ah, they aren’t heavily participating . . . it’s like . . . in a football game, the other team is the enemy, not the other team’s waterboy and cheerleaders.”

“No,” the Pakistani shoots back. “The other team’s water boy is also an enemy. It is law of our religion.”

“Haha, sorry that’s kind of funny,” the American replies.

When NSA and allied analysts really want to target an account, their concern for U.S. privacy diminishes. The rationales they use to judge foreignness sometimes stretch legal rules or well-known technical facts to the breaking point.

In their classified internal communications, colleagues and supervisors often remind the analysts that PRISM and Upstream collection have a “lower threshold for foreignness ‘standard of proof’” than a traditional surveillance warrant from a FISA judge, requiring only a “reasonable belief” and not probable cause.

One analyst rests her claim that a target is foreign on the fact that his e-mails are written in a foreign language, a quality shared by tens of millions of Americans. Others are allowed to presume that anyone on the chat “buddy list” of a known foreign national is also foreign.

In many other cases, analysts seek and obtain approval to treat an account as “foreign” if someone connects to it from a computer address that seems to be overseas. “The best foreignness explanations have the selector being accessed via a foreign IP address,” an NSA supervisor instructs an allied analyst in Australia.

Apart from the fact that tens of millions of Americans live and travel overseas, additional millions use simple tools called proxies to redirect their data traffic around the world, for business or pleasure. World Cup fans this month have been using a browser extension called Hola to watch live-streamed games that are unavailable from their own countries. The same trick is routinely used by Americans who want to watch BBC video. The NSA also
relies routinely on locations embedded in Yahoo tracking cookies, which are widely regarded by online advertisers as unreliable.

In an ordinary FISA surveillance application, the judge grants a warrant and requires a fresh review of probable cause — and the content of collected surveillance — every 90 days. When renewal fails, NSA and allied analysts sometimes switch to the more lenient standards of PRISM and Upstream.

“These selectors were previously under FISA warrant but the warrants have expired,” one analyst writes, requesting that surveillance resume under the looser standards of Section 702. The request was granted.

‘I don’t like people knowing’
She was 29 and shattered by divorce, converting to Islam in search of comfort and love. He was three years younger, rugged and restless. His parents had fled Kabul and raised him in Australia, but he dreamed of returning to Afghanistan.

One day when she was sick in bed, he brought her tea. Their faith forbade what happened next, and later she recalled it with shame.

“what we did was evil and cursed and may allah swt MOST merciful forgive us for giving in to our nafs [desires]”

Still, a romance grew. They fought. They spoke of marriage. They fought again.

All of this was in the files because, around the same time, he went looking for the Taliban.

He found an e-mail address on its English-language Web site and wrote repeatedly, professing loyalty to the one true faith, offering to “come help my brothers” and join the fight against the unbelievers.

On May 30, 2012, without a word to her, he boarded a plane to begin a journey to Kandahar. He left word that he would not see her again.
If that had been the end of it, there would not be more than 800 pages of anguished correspondence between them in the archives of the NSA and its counterpart, the Australian Signals Directorate.

He had made himself a target. She was the collateral damage, placed under a microscope as she tried to adjust to the loss.

Three weeks after he landed in Kandahar, she found him on Facebook.

“Im putting all my pride aside just to say that i will miss you dearly and your the only person that i really allowed myself to get close to after losing my ex husband, my dad and my brother.. Im glad it was so easy for you to move on and put what we had aside and for me well Im just soo happy i met you. You will always remain in my heart. I know you left for a purpose it hurts like hell sometimes not because Im needy but because i wish i could have been with you.”

His replies were cool, then insulting, and gradually became demanding. He would marry her but there were conditions. She must submit to his will, move in with his parents and wait for him in Australia. She must hand him control of her Facebook account — he did not approve of the photos posted there.

She refused. He insisted:

“look in islam husband doesnt touch girl financial earnigs unless she agrees but as far as privacy goes there is no room….i need to have all ur details everything u do its what im supposed to know that will guide u whether its right or wrong got it”

Later, she came to understand the irony of her reply:

“I don’t like people knowing my private life.”
Months of negotiations followed, with each of them declaring an end to the romance a dozen times or more. He claimed he had found someone else and planned to marry that day, then admitted it was a lie. She responded:

“No more games. You come home. You won't last with an afghan girl.”

She begged him to give up his dangerous path. Finally, in September, she broke off contact for good, informing him that she was engaged to another man.

“When you come back they will send you to jail,” she warned.

They almost did.

In interviews with The Post, conducted by telephone and Facebook, she said he flew home to Australia last summer, after failing to find members of the Taliban who would take him seriously. Australian National Police met him at the airport and questioned him in custody. They questioned her, too, politely, in her home. They showed her transcripts of their failed romance. When a Post reporter called, she already knew what the two governments had collected about her.

Eventually, she said, Australian authorities decided not to charge her failed suitor with a crime. Police spokeswoman Emilie Lovatt declined to comment on the case.

Looking back, the young woman said she understands why her intimate correspondence was recorded and parsed by men and women she did not know.

“Do I feel violated?” she asked. “Yes. I'm not against the fact that my privacy was violated in this instance, because he was stupid. He wasn't thinking straight. I don't agree with what he was doing.”
What she does not understand, she said, is why after all this time, with the case long closed and her own job with the Australian government secure, the NSA does not discard what it no longer needs.

*Jennifer Jenkins and Carol D. Leonnig contributed to this report.*

Barton Gellman writes for the national staff. He has contributed to three Pulitzer Prizes for The Washington Post, most recently the 2014 Pulitzer Prize for Public Service.