The End of National Security Reporting?

Jeff Stein

A few days after I started working for the Washington Post in 2010, the paper’s in-house lawyer gave me and other new hires a reminder about the pitfalls of covering national security in the Barack Obama era.

Don’t write anything down that you don’t want the government to see, he said. Not in your notes, and certainly not in emails. Give your sources code names. Avoid talking about anything sensitive on the phone.

“Go back to park benches and parking garages,” he said, with a hint of a smile. It was a reference, of course, to the paper’s legendary Watergate reporter, Bob Woodward, who famously met “Deep Throat” in an underground garage in 1972—and only after changing cabs two or three times to see if he was being followed. At least one other top national security reporter at the Post was doing the same, he said.

The issue wasn’t so much that the feds were casually browsing through our email or telephone records (although later National Security Agency [NSA] revelations made reporters wonder). It was what would happen after we wrote something that piqued the interest of the intelligence agencies, the Pentagon, or the US Department of Justice. Federal prosecutors were what we had to worry about, he said. In federal court, especially in cases involving national security, reporters had nothing but the First Amendment to protect them from having to reveal sources—a thin reed these days. We could only hope the courts sided with us, lest we go to jail.

The recent record offers faint hope. Currently, 37 states and the District of Columbia have press shield laws, varying in scope, that allow reporters to protect their sources (http://tinyurl.com/pft9nnk). But as Gregg Leslie, legal defense director for the Reporters Committee for Freedom of the Press, explains, they “only apply in state courts, and there is no federal shield law, so shield laws do not apply in any national security investigation, which will always be in federal court.”

The upshot is that federal prosecutors have wide leeway in getting subpoenas to track reporters’ emails and telephone calls and compel testimony in court.

Worrisome Precedents

No one needed reminding about Judith Miller, The New York Times correspondent who spent 85 days in jail in 2005 for refusing to give up her source. A federal judge demanded that she name the official who told her that Valerie Plame, the wife of former US diplomat Joseph C. Wilson, was a Central Intelligence Agency (CIA) undercover operative who had a hand in helping him dispute the Bush administration’s case that Saddam Hussein was building a nuclear weapon.

Only when her source, I. Lewis “Scooter” Libby, US Vice President Dick Cheney’s chief of staff, released her from her pledge of confidentiality did she relent and testify, under threat of prosecution.

Times’ Matthew Cooper nearly went to jail in the same case, after the magazine lost its appeal of his contempt citation for refusing to testify on Plame. Cooper told the judge that he “went to bed ready to accept the sanctions for not testifying,” but at the last minute, his source, later identified as top White House political operative Karl Rove, freed him to testify.

Six reporters were hauled before the court to testify on Plame, among them Bob Woodward and Walter Pincus, the Washington Post’s dean of national security reporters. They each identified other Bush administration officials as sources who had also tried to discredit Wilson by outing his wife, but only Libby went to jail—for lying to investigators. (President George W. Bush later commuted his sentence.)

The CIA had been outraged by the Bush administration’s outing of Plame and successfully lobbied the Department of Justice to prosecute the leaks under the Intelligence
Identities Protection Act, which made it a crime to unmask undercover operatives (http://tinyurl.com/yp9mhe). But the groundwork for pursuing journalists had been laid in 2003, when a federal judge in Chicago, Richard Posner, ruled that a group of authors contracted to write a biography of an Irishman charged with terrorism had to turn over their tapes and notes.

In swift progression, the Department of Justice and the Federal Bureau of Investigation (FBI) began pursuing journalists for accepting leaks from whistleblowers concerned about government waste, fraud, and abuse. And in a truly disturbing development, it seemed like the gumshoes were now viewing reporters as criminal co-conspirators.

Respected former television reporter Mark Feldstein got a whiff of the government’s new attitude when two FBI agents came to see him in 2006. Feldstein, then a journalism professor at George Washington University, was writing a book about Jack Anderson, the late syndicated columnist whose revelations of skullduggery had so rattled the Nixon White House that a plot was spawned to assassinate him. The FBI agents told Feldstein they were investigating whether officials of the American Israel Public Affairs Council, or AIPAC, Washington’s most powerful pro-Israel lobby, had trafficked in classified documents. They said they wanted access to Anderson’s papers, the names of researchers who might have seen classified documents in them, and the identity of any of Anderson’s former reporters “who were pro-Israel in their views or who had pro-Israeli sources,” according to Feldstein’s later testimony to a congressional committee (http://tinyurl.com/q24x2th).

Feldstein refused. He testified that the FBI’s effort, however clumsy, “suggested that the Bureau viewed reporters’ notes as the first stop in a criminal investigation rather than as a last step reluctantly taken only after all other avenues have failed.”

The smoke had hardly cleared from the Plame case when, in May 2006, Attorney General Alberto Gonzales suggested that the Department of Justice might prosecute two New York Times correspondents, James Risen and Eric Lichtblau, for reporting that “President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying.” The reporters cited anonymous “government officials” as their sources (http://tinyurl.com/b6w2e9j).

In the uproar over the warrantless wiretapping, no one was prosecuted. Indeed, two top Department of Justice officials, one the head of the FBI, the other a future FBI director, threatened to resign over the program.

The NSA’s massive data mining programs even bothered some inside the agency’s headquarters at Fort Meade, Maryland. In 2007, the Baltimore Sun’s Siobhan Gorman launched a multipart series on the shortcomings of several massive surveillance programs costing billions of dollars (http://tinyurl.com/oa6rbld). Lucy Dalglish, then-executive director of the Reporters Committee for Freedom of the Press, called it “a multibillion-dollar boondoggle” exposed by Gorman’s “important public-interest reporting.”

But the Department of Justice didn’t see it that way. In 2010, prosecutors accused Thomas A. Drake, 52, a senior NSA official at the time, of being a Gorman source (without naming her in the indictment). Although no spies—or even classified information, in the eyes of most experts—were involved, Drake was accused of violating the 1917 Espionage Act, among other charges that could have sent him to jail for 35 years. (A year later, after battering Drake’s professional, financial, and emotional life, prosecutors dropped all charges against him. Their conduct was “unconscionable,” the judge in the case said; http://tinyurl.com/q8j2u4n.)

Meanwhile, the Department of Justice had again come after Risen. His 2006 book, State of War: The Secret History of the CIA and the Bush Administration, included a detailed account of an ill-considered CIA covert operation against Iran that went awry and ended up providing the regime with blueprints for its nuclear program.

The Department of Justice believed former CIA officer Jeffrey A. Sterling was Risen’s source, charging him with the unauthorized disclosure of classified information, again citing the 1917 Espionage Act even though no spies were involved. As a key part of its case, the feds wanted to compel Risen, identified only as “Author A” in the indictment, to testify that Sterling was his source.

Risen resisted. His lawyer filed a motion to quash the subpoena, which expired when the grand jury was dismissed at the end of its 18-month term. But that would not be the end of the affair.

False Hopes
Any hopes that the incoming Obama administration would rein in the Bush administration’s warrantless wiretapping or aggressive pursuit of reporters along with whistleblowers turned out to be misplaced.

In April 2010, the Department of Justice again went after Risen in the Sterling case. And again Risen fought its subpoena.

In an appeals hearing on the issue, according to the Huffington Post’s account (http://tinyurl.
to New Delhi, collaborated with foreign publications from London. McClatchy news group as well as Times. The New York Times was accused of being a publisher—in effect, a journalist. Even more infuriating to officials, leading US news organizations like The New York Times, Washington Post, and the McClatchy news group as well as foreign publications from London to New Delhi, collaborated with Assange in publishing vast troves of secret military documents.

The government opened an espionage investigation of WikiLeaks, and US journalists wondered if they might be next in line.

Their fears were well founded, considering the Department of Justice’s investigation of James Rosen, chief Washington correspondent for Fox News, after he broadcast a story, based on a top-secret document about North Korea’s nuclear strategy, that referred to “CIA sources” in the Hermit Kingdom. After obtaining Rosen’s phone records and emails, and examining his entries and exits from the Department of State (as recorded by his security badge), the FBI soon had Stephen Jin-Woo Kim, a Lawrence Livermore National Laboratory intelligence analyst on loan to the Department of State, in its sights.

The FBI’s affidavit (mysteriously dated 18 months after the investigation began) ominously said there was “probable cause to believe” that Rosen was committing a crime by reporting on the document. It called him “an aider and abetter and/or co-conspirator” of Kim in his alleged leak of “national defense information,” which was, it asserted, a violation of the 1917 Espionage Act. The two were being treated as Cold War–era spies.

The FBI kept its investigation of Kim and Rosen secret for three years, until it was exposed by the Washington Post’s Ann E. Marimow this past May.

Likewise, it wasn’t until this May that the Department of Justice informed the Associated Press (AP) that it had begun secretly poring through its reporters’ emails and telephone records following its 2012 story about a classified CIA operation in Yemen.

“The records, obtained months earlier, include numbers dialed to and from phone lines in four AP offices, possibly implicating the communications of 100 journalists, over a period around two months,” Shane Harris summed up.

Journalists and constitutional scholars were appalled, not just that the feds seemed to be hurling time-honored protections of their work from government snoops, as enshrined in the First Amendment to the Constitution, but that Obama’s Department of Justice was characterizing them as spies and criminals.

The tactic was supremely hypocritical, many argued. Officials going back 240 years, from Thomas Jefferson to Obama’s national security aide, CIA director, top military officials, and countless bureaucrats in-between, had leaked secrets when it served their purpose—sometimes on the explicit direction of presidents, with no fear of prosecution.

But now an unusual mixed chorus of right- and left-wing civil libertarians and mainstream news organizations expressed outrage over the administration’s tactics. Attorney General Eric Holder, the administration’s top law enforcement official, tried to mollify critics, issuing a statement insisting that “[a]t no time during the leak case involving Stephen Kim, before or after the FBI sought the search warrant, have prosecutors sought approval to bring criminal charges against the reporter.”

“But the statement,” noted the conservative Washington Examiner, “does not explain why Justice Department officials failed to contact either Fox News or the Associated Press while making its case for a broad seizure of phone records and personal emails” (http://tinyurl.com/0jfevy8).

Holder’s sudden, belated embrace of a federal shield law, which had languished in the wake of WikiLeaks’ repeated release of classified military and diplomatic documents and video, was greeted with catcalls.
“When I heard this came out of the White House, I went, ‘Yeah, so?’” Daligham, now dean of the University of Maryland’s Philip Merrill College of Journalism, told the Daily Beast, which merged with Newsweek in 2010. “They think, ‘Oh, well, we threw this bone to them before and it sort of kept them happy.’ Give me a break. This doesn’t pass the smell test.”

Squeeze Plays

Reporters who cover national security are worried. They hear things about being watched. Because they’re plugged into Washington’s elite military, intelligence, and congressional oversight circles, they have to take such rumors seriously.

“In my 20 years of covering public policy, I have never felt so constrained in my ability to talk to sources and gather information as I do now,” Marisa Taylor, a national security reporter in McClatchy newspapers’ Washington bureau, said by email. “Many sources are afraid to be caught talking to a reporter even about unclassified matters that they believe the public has a right to know.”

On 20 June, Taylor and her colleague Jonathan S. Landay broke an exclusive story about the Insider Threat Program, an “unprecedented initiative” by the Obama administration that could punish government employees for discussing even unclassified information with journalists, and which encourages them to report “high-risk persons or behaviors” among coworkers—or risk punishment (http://tinyurl.com/ocakjvs).

To some, it conjured up East Germany’s feared secret police, the Ministry for State Security, or Stasi.

The government’s readiness to lodge overblown espionage charges against leakers has spread fear among potential Pentagon and intelligence whistleblowers who have been unable to get change from the inside, thinks Danielle Brian, executive director of the Project on Government Oversight, which regularly exposes government corruption and mismanagement. Drake, the senior NSA official who leaked massive cost overruns in a surveillance program to the Baltimore Sun, used every official channel to report the abuse, including Congress, to no avail, before turning to the press.

Intelligence agency employees are also exempted from the Whistleblower Protection Act. The title of a separate statute, “The Intelligence Community Whistleblowers Protection Act of 1998,” seems to offer more promise. But it permits CIA, FBI, NSA, and other national security agency employees to confine their complaints of waste, fraud, abuse, and other illegal conduct to Congress.

“I actually do think it has had an impact,” Brian said by email. “In the ’80s, when I started this work, we had far more people coming to us with documents from the national security agencies than we do now. This is in sharp contrast to the vast increase in people coming to us from other parts of government.

“It’s possible the problems in the Pentagon and intel agencies have been fixed,” she quipped, “but I seriously doubt it. I do have people occasionally saying, ‘I wish I could tell you—but I think the more significant impact is that they aren’t even reaching out in the first place.’

The number of intelligence contractors working on highly classified—and highly remunerative—NSA, CIA, and Pentagon programs has exploded since the September 11, 2001 attacks, employing thousands of retired officials and operatives (http://tinyurl.com/2e8cd5c). Some of those who might have felt free to meet with a reporter now face regular polygraphs, making them wary. Reporters are frustrated, but the public is the loser when the press can’t get “the real story” behind the government’s canned statements and evasions.

“Absolutely,” said a national security reporter from a large news organization, who asked for anonymity so as not to involve his employer in the discussion. “And, with the capabilities of mining email now, even innocuous email exchanges about getting coffee [together] can provide leads to these [government] investigators. This happened to one of my sources, and it’s made me even more wary of any email trail.”

Carrie Johnson, National Public Radio’s Department of Justice correspondent, said much the same.

“As a personal matter, I remind myself every day of the need to be careful about what I put in an email, in particular. Email is such a reflexive way of life for me, during work hours, in the early morning, and on weekends, that it’s hard for me to keep in mind that it has other uses for law enforcement that could be problematic. But the unsealed documents regarding the Kim case and the emails the Fox reporter used (with an alias) have helped to drive that home,” she said.

“I’m not sure aliases offer any real protection,” added Johnson, who previously worked for the Washington Post, “but I’m amenable to them if a source feels more comfortable [or] feels it’s necessary. I’m also trying to meet people in person more often. But I’m mindful of the fact that my [Department of Justice] badge can be used to track me there, just as it was at State for James Rosen.”

Some sources, like Drake, set up alternate email channels, such as Hushmail, to obscure their communications with reporters. Others, like Snowden, insisted that journalists use complicated encryption software to communicate with them. Particularly since the NSA data mining revelations, software developers have sensed a potential market in media organizations (http://tinyurl.com/n5aglw1).
If a source insists on it, that’s fine, with caveats, says the reporter for a large national news organization.

“I guess the thing I find unrealistic is for us to use that as our default way of doing business. If you are cold-calling some source and say, ‘Hi, I’m Jeff Stein, and I want you to tell me a bunch of classified stuff, but, since the government is probably monitoring our communication, I need you to set up a Hushmail account,’ who’s gonna say yes to that?”

And what if someone is inside your computer? Last year, after emailing the draft of a sensitive military story to my editor at the Washington Post Sunday Magazine, I got a late-night anonymous telephone threat.

“We know what you’re doing and we’re gonna take you down,” the caller said, and clicked off. As a national security reporter for 30 years, I’ve gotten a number of calls from nuts, so I didn’t take it seriously.

But after I endured five months of constant freezes and three hard-disk crashes on my reliable MacBook Pro, I began to suspect otherwise. The top Apple support people, who finally gave me a new machine, said they’d never seen anything like it. I could find no ready evidence of an intrusion and was too busy to send my laptop out for a complete (and expensive) forensic analysis.

My suspicions were reawakened in May, however, when Sharyl Attkisson, a CBS News investigative reporter, said that her personal and work computers had been compromised.

“I can confirm that an intrusion of my computers has been under some investigation on my end for some months, but I’m not prepared to make an allegation against a specific entity today as I’ve been patient and methodical about this matter,” Attkisson told Politico, the chronicler of inside-the-Beltway politics and media. “I need to check with my attorney and CBS to get their recommendations on info we make public.”

Since then, I’ve taken another look at the most deeply embedded systems in my machine, detected some unusual inroads from a Pentagon site, and reached out to an encryption expert. The results aren’t in yet.

The fact is, however, there’s not much you can do if the government starts targeting someone whose emails lead to you. Former CIA Director David Petraeus found that out when his lover, Paula Broadwell, started sending threatening emails to a rival, who then told an FBI agent about it. And when the NSA turns its sophisticated eavesdropping machinery on you, it’s too late. No alternate communication channels, code names, or encryption software offers much protection. Your cell phone alone can reveal your whereabouts down to the second.

“We talk a lot about that,” said Josh Meyer, a former Los Angeles Times investigative reporter who runs a national security teaching program for Northwestern University’s Medill School of Journalism in Washington, DC.

“We had a [former government] cybersecurity guy come in and talk about it. Scared the crap out of them.”

Mark Zaid, a Washington, DC, attorney who specializes in representing national security whistleblowers, said there’s one important step reporters can take to protect themselves, beyond minimizing telephone and email contact and using throwaway phones with a source.

“For one thing, at no time should any journalist ‘solicit’ classified information from a source,” Zaid said by email. “The wording of the espionage statute is broad enough to simply criminalize the solicitation, possession, and dissemination of national defense information (which may or may not be classified) and there is no exemption for journalists.”

It’s ludicrous to suggest that national security reporters—and sources outraged by government conduct—will be cowed by the Department of Justice’s zealous pursuit of leakers, Zaid and others said.

But “it is certainly best to take precautions in light of the US government’s ability, as a matter of law, to prosecute a journalist.”

Jeff Stein, a former military intelligence case officer in Vietnam, writes the SpyTalk blog www.and magazine.com/category/spytalk. html from Washington, DC.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.