SOURCES AND SECRETS – BACKGROUND BRIEF

A Forum on the Press, the Government and National Security
March 21, 2014, at the TimesCenter in New York City
More information here: http://www.sourcesandsecrets.com/

By Josh Meyer, Medill National Security Journalism Initiative
josh@northwestern.edu, 202-365-2401, @JoshMeyerDC

The battle between media organizations and the government over access to information – especially about national security – has existed for centuries. It has intensified exponentially in the post-9/11 era, especially in recent years due to WikiLeaks, Edward Snowden, an aggressive anti-leak campaign by the Obama administration and other developments.

Many of these conflicts came to a head last summer after it became clear that the Obama Justice Department had made unprecedented intrusions into reporters' efforts to gather information and obtain government documents.

First came the news that the Justice Department had secretly subpoenaed a wide array of Associated Press phone records in an effort to find the source of information for a story about counterterrorism operations in Yemen.

That was soon followed by disclosures about how the FBI had obtained secret subpoenas for Fox News reporter James Rosen's private emails a few years earlier by suggesting he broke the law in an effort to get information about North Korea from a State Department source.

Then came the avalanche of disclosures about previously undisclosed National Security Agency surveillance programs, spurred by Snowden, a former NSA contractor, which raised additional questions about the lengths to which U.S. intelligence agencies were monitoring the public at large – and reporters.

All the while, the Obama administration has been spearheading the largest number of leak investigations in history, with at least eight felony prosecutions since 2009 using provisions of an archaic law – the Espionage Act of 1917 – that many legal experts say was never intended to be used to thwart efforts to report on national security. That's compared with a total of three such prosecutions in all previous U.S. administrations. This recent report by the Committee to Protect Journalists provides more detail.

And the administration continues to try and put author and New York Times reporter James Risen in jail for refusing to disclose the source of information for his 2006 book, "State of War: The Secret History of the CIA and the Bush Administration."

In response, there have been mounting calls for reform, some of which have been answered – or at least addressed.

One key development is the Obama administration's recent efforts to update the Justice Department guidelines that regulate its dealings with the media, including who it can subpoena and prosecute and what other steps it can take when trying to stop leaks to journalists and to find out their sources.

The second major development is the rekindling of efforts to get Congress to pass a federal shield law that protects journalists – and directly or indirectly their sources – from government attempts to stop the flow of information between them.

This briefing paper will discuss both of those new developments, as well as offer a short and, hopefully, readable primer on some related issues, including:

- the use of the Espionage Act and other statutes to go after reporters' sources
- the erosion of the reporter's privilege in defending against subpoenas and other demands for information
- leak investigations aimed at national security journalists and their sources
- the Justice Department guidelines on subpoenas, including recent revisions
- the provisions and prospects of a federal media shield law
- the relevant provisions of the USA PATRIOT Act

THE ESPIONAGE ACT AND OTHER APPLICABLE STATUTES

Two landmark legal cases firmly established basic media freedoms, including ensuring an unfettered press that can publish news about national security matters. They are New York Times Co. v. Sullivan, a ruling from 50 years ago this month. Seven years later, New York Times Co. v. United States – the Pentagon Papers case – upheld the right of the Times and The Washington Post to publish the explosive revelations leaked by Daniel Ellsberg and a RAND Corporation colleague.

Given such media protections, the government has been left with two basic options, as described by Julia Atcherley and Lee Levine in their chapter in the American Bar Association's 2012 book "National Security Law in the News."

- Prosecute journalists and news organizations *after* they have published; not for criticizing public officials, but for disseminating classified government information that the government says may harm the nation's security, and

- Compel journalists to disclose confidential sources of such information

There are many statutory provisions throughout the U.S. Code that allow the government to pursue these two options. By far the most common, especially in the decade since the 9/11 attacks, has been the Espionage Act of 1917. But the government's use of it has been

controversial; many experts say its broad provisions were never intended to be used to go after journalists, or even to inhibit their sources except in narrowly proscribed circumstances.

The Espionage Act was created as the U.S. was entering World War I to stop the threat of subversion, sabotage and malicious interference with the war effort, especially the reinstatement of the draft. And while those threats were real, Congress rejected attempts by the Woodrow Wilson administration to include some level of press censorship regarding efforts during wartime to publish any information determined to be "of such character that it is or might be useful to the enemy."

Specifically, The Espionage Act instituted harsh penalties for the encouragement of "insubordination, disloyalty, mutiny, or refusal of duty" to the United States, and interference with the draft. The Sedition Act of 1918 added penalties for "disloyal, profane, scurrilous, or abusive" writing about the US government.

The Sedition Act was repealed by Congress by 1921. But the Espionage Act – in the way the courts have interpreted it – had until recently navigated the tensions fairly well, in terms of balancing the government's desire to protect national security secrets and the press's desire to write about them.

One of the best and most comprehensive summations of the Espionage Act and its impact on the media is Gary Ross's 2011 book, "Who Watches The Watchmen? The Conflict Between National Security and Freedom of the Press." Another is this 2011 Congressional Research Service report. The Lawfare blog has posted numerous news articles and analyses of the statute and its evolving use, including this piece on the Obama administration's use of the Espionage Act in third-party leak prosecutions.

In May 2010, a Senate Judiciary Subcommittee held an especially informative hearing on "The Espionage Act: A Look Backward and a Look Forward" that went into great detail about its use over the years, and constitutional scholars' concerns about it.

And perhaps the best law article on the use of the Act in media cases remains the 1973 Columbia Law Review article The Espionage Statutes And Publication Of Defense Information by Harold Edgar and Benno C. Schmidt, Jr. They wrote that the Espionage Act is "in many respects incomprehensible,'' with provisions "so sweeping as to be absurd."

The most likely source of such a prosecution within the broad parameters of the Espionage Act is 18 U.S.C. § 793 (Section 793), on "Gathering, transmitting or losing defense information." Even more specifically, subsection 793 (e), which prohibits the unauthorized possession, retention or communication of documents or other tangible materials or information "relating to the national defense which … the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation…"

But the Espionage Act has at least nine provisions that impact reporters, which are linked to below, thanks to the Cornell Law Library:

§ 792. Harboring or concealing persons
§ 793. Gathering, transmitting or losing defense information
§ 794. Gathering or delivering defense information to aid foreign government
§ 795. Photographing and sketching defense installations
§ 796. Use of aircraft for photographing defense installations
§ 797. Publication and sale of photographs of defense installations
§ 798. Disclosure of classified information

Ross has a good summary in his "Who Watches The Watchmen?" book, which was published by the U.S. government's National Intelligence University. He says sections 793, 794, and 798 are particularly applicable:

Section 793 prohibits the disclosure of "national defense information" to "any person not entitled to receive it," while Section 794 specifically proscribes disclosures to "any foreign government."

Sections 793 and 794 both include a requirement that the disclosure be committed "with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation."

Section 798, a 1950 amendment to the Act, contains several key distinctions from its predecessors, Ross adds. That section criminalizes the disclosure of "classified information," specifically involving cryptographic or communications intelligence. Importantly, Ross writes, Section 798 does not include an "intent" provision, only a requirement that the disclosure be performed "knowingly" and "willfully."

Section 798 is also the only section that expressly prohibits the publication of classified information, according to Ross. All are punishable by lengthy prison terms, with violations of Section 794 punishable by up to life in prison, with provisions for seeking the death penalty under certain circumstances.

Stephen I. Vladeck, law professor and associate dean for scholarship at American University's Washington College of Law, echoes some of the same concerns as Edgar and Schmidt. He says there are significant problems with the Espionage Act, most of them stemming from "seemingly overlapping and often ambiguous provisions'' that leave open to debate whether intent to harm the national security of the United States is needed for prosecution.

Ben Wittes of the Lawfare blog articulates similar concerns in several posts, including "Problems with the Espionage Act," which was written in December 2010 amid calls for prosecuting Julian Assange and shutting down Wikileaks.

Wittes, who is also senior fellow and research director in Public Law at The Brookings Institution, says there are particularly troubling issues with using the Espionage Act to go after the receivers of information, including reporters.

Besides being very old and very vague, he says the Act "contains no limiting principle in its apparent criminalization of secondary transmissions of proscribed material," according to the

relevant section [18 U.S.C. 793 (e)], on gathering, transmitting or losing defense information. In other words, he writes, it criminalizes "not merely the disclosure of national defense information by organizations such as Wikileaks, but also the reporting on that information by countless news organizations,'' and potentially even discussions of those stories by members of the general public.

The second problem, according to Wittes, is that the Espionage Act covers only material "relating to the national defense,'' not the broader array of national security topics, such as the State Department cables disclosed by WikiLeaks.

The first use of the Espionage Act involving a leak to the media was the Pentagon Papers case.

In 1971, two analysts from the RAND Corporation, Daniel Ellsberg and Anthony Russo, were indicted for leaking classified documents about how badly the Vietnam War was going to the New York Times, The Washington Post and other media outlets. The indictments came down after the Supreme Court refused to stop the press from publishing the Pentagon Papers. The case against the leakers was ultimately dismissed.

One little-known footnote of the case against the Times and The Post is that six of the Supreme Court justices "openly contemplated the possibility of postpublication criminal prosecution of the newspapers" under Section 793, according to Atcherley and Levine in their book chapter, "The First Amendment and National Security."

Also, Justice Byron White, in a separate, concurring opinion, opened the door to possible prosecution of the media under the Espionage Act for publishing classified information. "This radical reinterpretation of the statute's meaning would have profound effects in the years to come," writes Lincoln Caplan in a fall 2013 piece for The American Scholar titled, "Leaks and Consequences; Why treating leakers as spies puts journalists at legal risk."

The Espionage Act was used to prosecute Navy analyst Samuel L. Morison in 1984 for providing classified satellite photos of a Soviet aircraft carrier to the British publication Jane's Defence Weekly. Morison was convicted (and later pardoned), but Jane's was never charged.

In fact, the only third party, or recipient of information, ever charged under the Espionage Act is believed to have occurred in a 2005 prosecution that became known as the AIPAC case.

Two lobbyists for the American Israel Public Affairs Committee, Steven J. Rosen and Keith Weissman, were arrested and charged with conspiring illegally to receive classified information from a government official, Defense Department analyst Lawrence Franklin, and transmitting that information to others in violation of Espionage Act sections 793 (d) and (e).

It was the first time the Justice Department sought to prosecute private citizens for doing something journalists do every day; obtain and disseminate information from someone who might not have been authorized to release it, especially classified information relating to national security.

Franklin ultimately pleaded guilty to passing government secrets to Rosen and Weissman, as well as giving classified information to Israel, and was sentenced to almost 13 years in prison. The charges against Rosen and Weissman were dropped after a judge suggested that the government would have had to prove that they had acted intentionally to damage national security.

Over the past decade, the Espionage Act has been used many times in connection with media cases. Here are some of the major cases. PBS has a good explanation of the particular statutes used against each:

THOMAS DRAKE – A former senior NSA executive, Drake was investigated as a possible source of information for newspaper stories about the NSA's surveillance programs. He was prosecuted in 2010, for allegedly "mishandling" and retaining classified information about NSA programs. His defenders claim he was targeted because of his criticism of a problem-plagued data program called Trailblazer. All 10 original charges against him were dropped in 2011, and he pled guilty to one misdemeanor count of exceeding authorized use of a computer.

SHAMAI LEIBOWITZ – A former FBI contract linguist, he pled guilty in May 2010 to giving classified information about U.S. "communication intelligence activities" to a blogger who then published the information, and was sentenced to 20 months in prison. Although the Justice Department wouldn't comment, published reports said the information in question focuses on U.S. efforts to gather intelligence on the Israeli embassy in Washington, in part through wiretaps.

BRADLEY (NOW CHELSEA) MANNING – An Army private, Manning was charged in July 2010 with several violations of the Espionage Act, including disclosing U.S. government information to WikiLeaks, which then published them. A military judge found Manning not guilty of the most serious charge of aiding the enemy, but convicted her of other Espionage Act charges including stealing government property.

STEPHEN JIN-WOO KIM. A former contract State Department analyst, Kim was charged in August 2010 with illegally giving out classified information about North Korea's nuclear program. Almost three years later, the media reported that the FBI had sought, and a federal judge approved, a search warrant for the e-mails and other records of Fox News reporter James Rosen on the grounds that he aided and abetted Kim's illegal efforts to turn over the information. Kim was ultimately sentenced to a sentence of 13 months in prison for giving Rosen a June 2009 intelligence report about North Korea. Rosen was never charged.

JOHN KIRIAKOU – A former CIA case officer, Kiriakou was indicted in April 2012 with several counts of violating the Espionage Act for allegedly leaking to several reporters the names of at least one agency operative involved in classified CIA counterterrorism programs, including the interrogation of high-value detainees. He was also charged with violating the Intelligence Identities Protection Act and making false statements. He was sentenced to 30 months in prison after agreeing to plead guilty to one count of passing classified information to the media in violation of the IIPA.

JEFFREY STERLING – A former CIA employee, Sterling was charged in Dec. 2010 with several violations of the Espionage Act and other laws in connection with allegedly disclosing information about Iran's nuclear program to Risen, the author and New York Times reporter. He has denied the charges, and the case is on hold while courts deliberate whether to force Risen to

testify about the source of his information. Sterling faces potentially decades in prison if convicted on all counts; Risen has been subpoenaed but not charged.

JAMES HITSELBERGER – A former Navy linguist, he was charged in Dec. 2012 with violating the Espionage Act for providing classified documents to the Hoover Institution at Stanford University allegedly revealed troop activities and gaps within U.S. intelligence about Bahrain.

EDWARD SNOWDEN – A former NSA contractor, Snowden was charged in a June 2013 criminal complaint with two violations of the Espionage Act; unauthorized communication of national defense information and "willful communication of classified communications intelligence information to an unauthorized person." He was also charged with theft of government property, and faces a maximum of 30 years in prison.

As these cases show, the government has refrained from prosecuting journalists under the Espionage Act. Instead, the government has sought to prosecute government officials for leaking information, and to compel journalists to reveal their sources through subpoenas and other means. And though U.S. law has long afforded the media a so-called reporter's privilege to contest such efforts, that protective shield has been steadily eroding over the past several decades.

Below is a discussion of the erosion of the Reporter's Privilege, and some key cases. But first, a quick summary of some of the other statutes that have been used against government officials suspected of, or charged with, leaking information to the media.

OTHER STATUTES USED AGAINST JOURNALISTS AND THEIR SOURCES

A patchwork of other statutes affects reporters and their sources as well. Critics say they are not only "overlapping, inconsistent, and vague," but not designed to apply to journalists and their sources – or in many instances to national security matters.

As a result, "the government has historically been forced to shoehorn national security `leaking' into criminal laws designed for far more egregious offenses (such as spying), or far more common offenses (such as conversion of government property)," Vladeck, the American University professor, writes in a draft chapter for an upcoming American Bar Association book. The book is tentatively titled, "National Security, Leaks, Whistleblowers, and the Media: A Guide to the Laws."

"Because of the poor and antiquated fit of the relevant criminal statutes," Vladeck writes, "and the related First Amendment questions that arise from such mismatch, the result has been a situation that the CIA's General Counsel once described as the `worst of both worlds.' ‘'

Here are some of the statutes that affect journalists and their sources, according to Vladeck and other constitutional law experts:
18 U.S.C. § 641. Known as the federal conversion statute, it makes it a crime for anyone who "embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States." This is often used in tandem with the Espionage Act, including in the Morison case).

50 U.S.C. Sections 421-426. The Intelligence Identities Protection Act of 1982. Prohibits the intentional disclosure of any information that identifies covert intelligence officers, agents, informants, or sources by individuals with authorized access to classified information from which they learn such individuals' identity. Used in the Kiriakou case and the Valerie Plame leak investigation case. This Congressional Research Service report is a good primer on its uses in media cases.

50 USC 783. Prohibits the communication of classified information to the agent of a foreign government by a government employee or employee of a corporation in which the government is a majority owner.

18 U.S.C. § 952, (1933). Makes it illegal for a government employee to willfully publish or furnish to another any diplomatic codes or "any matter prepared in any such code," without regard to the specific content of the communications, the employee's motive or intent, or whether or not the disclosed information in any way harms the United States or benefits a foreign power.

18 U.S.C. § 1924, (1994). Prohibits the unauthorized removal, retention or storage of classified documents or material. It applies to U.S. government officers, employees, contractors and consultants.

18 U.S.C. § 1030, especially section (a)(1). Prohibits the disclosure of protected national defense and foreign relations information retrieved through unauthorized access of a computer, figured prominently in the Manning court-martial proceedings—and would also be relevant to future leak prosecutions in which the unauthorized disclosure originated in unauthorized access to a government computer.

§ 1905 More general statute that prohibit the disclosure of confidential information acquired in the course of employment "in any manner or to any extent not authorized by law," and the unauthorized removal and/or retention (without disclosure) of classified information. Used against former National Security Advisor Samuel (Sandy) Berger in his 2005 prosecution for removing Clinton era classified documents.

General charges of obstruction of justice and making false statements to investigators.

The Atomic Energy Act of 1954, which prohibits the communication of "Restricted Data" relating to atomic energy, with intent or reason to believe such data will be used to injure the United States, and the disclosure of any "Restricted Data" to unauthorized parties.

POST 9/11 EROSION OF REPORTER'S PRIVILEGE
And Related Leak Investigations

For decades, authorities have relied on these various statutes to investigate reporters and their sources, to issue them subpoenas and to use the threat of prosecution and incarceration to get them to cooperate.

In response, journalists and their lawyers have fought back by claiming reporter's privilege, with varying degrees of success.

The reporter's privilege, simply put, is the right not to be compelled to testify or disclose sources and information in court, or in grand jury proceedings or other venues – in each state and federal circuit. The law varies significantly by state, and by the interpretations of the various federal circuit and appeals courts.

Currently, the case that is likely to set legal precedent is that of the New York Times' Risen, whose legal team is now fighting the third subpoena demanding that he disclose the source of information about U.S. counter-proliferation cyber-operations against Iran.

Last July, a federal appeals court in Richmond, Virginia, ruled that Risen could not claim a reporter's privilege under the First Amendment to win exemption from being compelled to testify. A petition is now pending at the Supreme Court, though some legal experts are not optimistic that the High Court will take the case. "That would be a big blow" for advocates of a strong reporter's privilege, says Vladeck.

Risen's lawyers argue that by trying to compel him to testify, the Justice Department is essentially criminalizing the work that many journalists do in trying to obtain national security information for the purposes of publication. If reporters cannot reasonably guarantee confidentiality to sources, they say, those sources won't provide information that is vital to the public interest.

Risen is by no means the first journalist threatened with subpoenas, especially since 2003. That's when influential federal appeals court judge Richard Posner dealt the reporter's privilege a significant setback by issuing an opinion saying that journalists have virtually no right to protect their sources.

Specifically, Posner concluded that the landmark Branzburg v. Hayes case of 1972 actually did not establish the reporter's privilege that conventional wisdom held that it did. He said those seeking to subpoena a member of the media need only to make sure that it is "is reasonable in the circumstances."

Prosecutors have gone after reporters in numerous cases since then, often as a way to find out who was leaking information in the first place, even though legal precedent had been for authorities to undertake such efforts only after all other avenues have been exhausted. Reporters have had their emails and other information read or seized, they have been subpoenaed and deposed, and at least one has gone to jail or prison to protect their sources.

Here are some of the key cases and their outcomes:

More information can be found in several pieces (here and here) that Shane Harris wrote in Washingtonian Magazine about the erosion of reporter's privilege. Other good sources of information abound, including "Rethinking Reporter's Privilege" by RonNell Andersen Jones and "Deja Vu All Over Again: How A Generation of Gains in Federal Reporters' Privilege Is Being Reversed," by Lucy A. Dalglish & Casey Murray. Also: "'Preferred Position?' The Reporter's Privilege in the 21st Century and Beyond."

Fall 2004 – Special DOJ prosecutor Patrick J. Fitzgerald subpoenas at least five journalists in the Valerie Plame investigation to see whether White House officials leaked the identity of the undercover CIA operative to the media. New York Times reporter Judith Miller refuses and ultimately spends nine weeks in jail, even though she never published the information. TIME magazine ultimately agreed to comply with a federal subpoena and surrender reporter Matthew Cooper's notes and files.

September 2004 – Fitzgerald subpoenas two New York Times reporters' telephone records for an Illinois grand jury investigation into whether government employees leaked plans of a planned FBI raid on Global Relief Foundation, an Islamic charity suspected of funding terrorism.

Winter 2006 **–** The Justice Department begins investigating who leaked information to Risen and colleague Eric Lichtblau of the New York Times, allowing them to disclose a top-secret NSA warrantless surveillance program. Attorney General Alberto Gonzales tells Congress that, "Obviously our prosecutors are going to look to see all the laws that have been violated. And if the evidence is there, they're going to prosecute those violations." Washingtonian magazine will later say, "This is the first time any administration official has hinted that the government might prosecute journalists under criminal law for reporting on national security information."

January 2008: The Justice Department issues a subpoena to Risen to determine who gave him classified information for his book State of War. Risen fights the subpoenas, and then two more, leading to a protracted legal battle that continues to this day.

February 2008: USA Today reporter Toni Locy is ordered held in contempt of court for refusing to identify her sources for articles on a scientist identified as a person of interest in the post-9/11 anthrax attacks. Former Army scientist Steven J. Hatfill, who denied wrongdoing**,** sued the government and subpoenaed Locy and numerous other journalists in an effort to determine who in the government had given his name. Locy faces $5,000 in fines for each day she refuses to testify, but avoids jail time when Hatfill settles his case against the government.

Fall 2012 – The Justice Department launches an investigation into who leaked information about Stuxnet and other cyber-operations mounted against Iran to New York Times reporter David Sanger for newspaper stories and his book "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power."

May 2013**:** The Justice Department investigates the Associated Press for a story on CIA efforts to stop a bomb plot emanating from Yemen, and issues broad subpoenas for the phone records and

other information pertaining to AP reporters. It is later disclosed that the subpoenas are so broad that the Justice Department obtained the communications of as many as 100 AP journalists in four offices.

Other cases in which reporters were subpoenaed:

- the trial of New York defense attorney Lynne Stewart for aiding terrorism by publicizing a client's statement against court orders
- the civil suit of former Los Alamos nuclear scientist Wen Ho Lee against two federal agencies for leaks to the media
- The San Francisco grand jury investigation into alleged illegal steroid distribution by BALCO, the Bay Area nutritional supplement company.

Much of the effort to go after reporters and their sources has been dictated not by law but by U.S. government policy, specifically the Justice Department guidelines governing when subpoenas can be used, and against whom – and, more recently, as in the AP and James Rosen of Fox News cases, whether the subject of the subpoenas even has the right to know about, and contest, them.

But the Justice Department regulations cover a lot more than that, as the document outlining the recently approved new guidelines suggests. Its title: "Policy Regarding Obtaining Information From, or Records of, Members of the News Media; and Regarding Questioning, Arresting, or Charging Members of the News Media."

JUSTICE DEPARTMENT GUIDELINES ON SUBPOENAS (and other efforts to investigate journalists)

Despite their importance, the Justice Department had operated under essentially the same set of guidelines regarding subpoenaing members of the media since 1970. They're found here, at 28 C.F.R. s. 50.10, with a good primer here from the Reporters Committee for Freedom of the Press.

In 1980, the guidelines were amended to cover telephone records held by service providers. But they were never updated to effectively cover the flood of more recent technological developments, including email, text messaging or Skype, or information gathered by NSA's vast signals intelligence capabilities.

Last year, Attorney General Eric H. Holder Jr. acknowledged the media's collective concerns, and initiated a comprehensive evaluation of DOJ's practices and policies regarding the use of subpoenas, court orders, and search warrants to obtain information from, or records of, journalists. DOJ held seven meetings with approximately 30 news media organizations as well as with First Amendment groups, media industry associations and academic experts, and invited others to submit suggestions as well.

The Reporters Committee coordinated a proposal from more than 50 media companies. Among its major proposed changes: Notice to the news media in all instances where the government makes a demand on third parties for a journalist's records. And expansion of the guidelines to cover all "investigatory instruments," including search warrants, warrants from the FISA court and national security letters, as well as all types of records, including email, credit card information, and other newsgathering materials.

Holder issued his report July 12, 2013, announcing proposed changes to the Department's policies. The changes were described as broadly stated policy statements that would eventually be made more specific and incorporated into federal regulations. On Feb. 27, 2014, the final updated DOJ policy was entered into the Code of Federal Regulations, and experts are still trying to figure out which of the proposals actually made it into the new policy. Some fear that not all of them did.

Holder says his July 12 report includes several key reforms to the department's protocols that "will help ensure the proper balance is struck when pursuing investigations into unauthorized disclosures." Here's a detailed summary of the changes from the Reporters Committee.

Journalists and First Amendment lawyers have been mostly positive, saying the stronger safeguards are an important step, but that more needs to be done. Influential media lawyer and longtime New York Times counsel George Freeman called the policy revisions "long overdue" in light of the technological changes that have transformed newsgathering.

According to DOJ, the revisions "are intended to ensure that, in determining whether to seek information from, or records of, members of the news media, the Department strikes the proper balance among several vital interests: (1) Protecting national security, (2) ensuring public safety, (3) promoting effective law enforcement and the fair administration of justice, and (4) safeguarding the essential role of the free press in fostering government accountability and an open society."

More specifically, DOJ says, the revisions:

- ensure more robust oversight by senior Department officials
- centralize the internal review and evaluation process
- set out specific standards for the use and handling of information obtained from, or records of, members of the news media;
- extend the policies to cover the use of subpoenas, court orders issued pursuant to 18 U.S.C. 2703(d) and 3123, and search warrants.

DOJ says the revised policy also strengthens the presumption that Department attorneys will negotiate with, and provide advance notice to, affected members of the news media when investigators seek to obtain from third parties communications records or business records related to ordinary newsgathering activities.

Some media organizations say the devil is in the details, and that potentially huge loopholes exist that will allow DOJ to keep them in the dark about subpoenas and other investigations, especially regarding national security matters. The key language: DOJ doesn't have to give advance notice

to media organizations when their records are subpoenaed if the Attorney General determines that giving such prior notice could “pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm.”

Under the new rules, prosecutors have a higher bar to meet when seeking permission to search journalists' materials. An exemption under the Privacy Protection Act, for instance, could only be used if the journalist is “the focus of a criminal investigation for conduct not connected to ordinary newsgathering activities.” In the past, the government has used that provision to access the records of journalists in cases where the effort to obtain information was the alleged crime itself.

Many media organizations say the new guidelines don’t go far enough, including the Reporters Committee, which said in a statement that the coalition it heads believes an impartial judge should be involved when there is a demand for a reporter’s records “because so many important rights hinge on the ability to test the government's need for records before they are seized."

Holder himself agreed, saying that some of the more substantive changes sought by the media cannot be done through administrative policy revisions, including an expedited judicial review. “While these reforms will make a meaningful difference, there are additional protections that only Congress can provide,” Holder said, in urging Congress to pass a federal media shield law.

Over the past year, President Obama also has pressed for passage of such a media shield law, also known as a source protection law. Some media representatives note with irony that Obama, like his attorney general, is pushing for such journalist protections even as they continue to oversee such an aggressive crackdown on leaks.

FEDERAL MEDIA SHIELD LAW

With Obama and his attorney general publicly calling on Congress to enact such protections, Sen. Charles Schumer, D-N.Y., last May reintroduced a federal media shield law proposal called the Free Flow of Information Act, which he had pushed several years earlier. Soon after, Rep. John Conyers of Michigan, the top Democrat on the House Judiciary Committee, reintroduced his version of the bill, which already had passed the House twice.

Forty-nine states and the District of Columbia already provide journalists with some form of reporter’s privilege that protects them – to varying degree –if a state government seeks to make them reveal confidential information, including the identity of a source. Wyoming is the lone holdout. Maryland apparently was the first, in 1896. Those protections, as this Congressional report explains, come in the form of as many as 40 actual statutes, known as “shield laws,” as well as through at least 16 court decisions that have created legal precedent.

Few of the state shield laws provide absolute immunity from subpoenas and other investigative efforts to get information from journalists. Most include carefully calibrated protections, and use “balance tests” to weigh the freedom of the press and the public's right to know on one hand, and the needs of law enforcement and civil litigants on the other. Here’s a good synopsis of what many of them do.

But no such protections exist on the federal level. And the landmark Branzburg v. Hayes case has only confused matters by including fuzzy legal language about how there is no right under the First Amendment for a journalist to withhold confidential information in a grand jury proceeding. The Court did note, however, that, ``Congress has freedom to determine whether a statutory newsman's privilege is necessary and desirable and to fashion standards and rules as narrow or broad as deemed necessary to deal with the evil discerned and, equally important, to refashion those rules as experience from time to time may dictate."

All three branches of government, and legal and constitutional scholars, have been trying to decipher that ruling ever since, with limited success. In response, many journalist organizations have pushed for a federal shield law, especially one that provides protection to journalists writing about classified information.

Various administrations, while supporting the concept of a federal shield law, have pushed back on the details, saying such legislation cannot undermine the government's interest in keeping secrets and in being able to prosecute those who endanger the national security by improperly or illegally leaking them.

Both bills are currently under consideration; Schumer's bill was approved by the Senate Judiciary Committee in September 2013. The provisions of the House bill are more friendly to reporters, in terms of requirements the government has to meet in order to obtain subpoenas to compel reporters to testify about their sources or to obtain their phone and email records.

Support for the legislation appears to have stalled as a result of the Snowden leaks, just as similar legislation in 2010 legislation died in the aftermath of the WikiLeaks disclosures, with some lawmakers saying they didn't want to appear to condone or protect those publicizing or leaking such potentially damaging national security information.

To distill down some immensely complicated legal language, the proposed legislation is intended to maintain the free flow information to the public by providing conditions for the federally compelled disclosure of information by certain persons connected with the news media.

There are reams of good reports and articles on the historical efforts to pass Shield Law legislation and on what the current bills would do. They include this report submitted to Congress on the Schumer bill and this roundup by the Society of Professional Journalists.

The pending bills would grant journalists some measure of a qualified privilege to protect the identities of sources and materials obtained during newsgathering. In most cases, instead of allowing the Justice Department to decide, federal subpoenas demanding that a reporter testify in court or turn over records would be subject to judicial review.

Under the pending legislation, the scope of protection for reporters varies according to whether it involves a civil case, a regular criminal case or a national security case. Reporters in civil cases would receive the greatest protection; those seeking to obtain their information or to compel them to testify would have to show why their need for those outweighs the public interest in having an unfettered press.

Reporters in regular criminal cases would have similar protections, but the burden would be on them—not the seekers of the information – to make a "clear and convincing" case as to why they do not need to turn it over. The public interest in the free flow of information would be weighed against the needs of law enforcement and investigators.

At the heart of those bills: a provision to put federal judges in charge of deciding how soon the Justice Department must inform media organizations that their records have been subpoenaed, with a 90-day deadline from when the subpoena is served. The bill, amended to incorporate the new Justice Department guidelines, also would protect a wide array of third party documents such as credit card bills and communication records. But the legislation may not extend to websites, Internet service providers (ISPs) and phone companies.

Some critics say the proposed legislation contains too many broad exceptions when it comes to national security information, and that those exceptions all but negate the protections for journalists writing about key issues like counterterrorism, intelligence-gathering, surveillance and military operations. Others say some protections are better than none.

In national security cases, especially those involving the disclosure of classified information, the balancing test would be weighted far more on the side of prosecutors and against reporters. Under the Schumer bill, for instance, prosecutors could prevent judges from quashing a subpoena if prosecutors can show that the information they seek might help mitigate "acts that are reasonably likely to cause significant and articulable harm to national security," which one reporter described as "a phrase so full of ambiguities as to be essentially useless."

Some legal scholars agree that the measure affords prosecutors exceptional leeway.

"How do we define harm to the United States?" asks Jane E. Kirtley, the Silha Professor of Media Ethics and Law at the University of Minnesota, and the former executive director of the Reporters Committee. "Is the government always going to be able to play national security as a trump card to scare off journalists from reporting in the first place or to go after them once they do?"

Also, Kirtley says, the government historically has relied on the claim of national security in cases where there is no true national security interest. "Claims of national security are too easily made and for reasons that have nothing to do with actual security, but have more to do with things that are embarrassing, or that are undermining our political agenda."

"The new [Attorney General] guidelines provide some level of protection," she adds. "But once you get into the national security realm, it's pretty thin."

The proposed shield law is also controversial because it delineates who should be considered a journalist for purposes of legal protection, suggesting that bloggers and others working for non-traditional media companies might not be protected.

Some key media representatives worry that efforts to better protect journalists from subpoenas and other investigatory methods are in some ways moot, because the government is already getting their information – including confidential sources – through other, highly classified means, including the USA PATRIOT Act.

THE PATRIOT ACT

One of the most controversial and confusing clashes of national security law and policy when it comes to reporters is the USA PATRIOT Act.

The Patriot Act, which stands for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, was established six weeks after the 9/11 attacks in 2001, and amended several times since then. Its stated purpose: To "deter and punish American terrorists in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."

It accomplishes that by making significant changes to at least 15 existing federal statutes, dramatically expanding the powers of government to monitor and intercept electronic and digital communications through the use of wiretaps, pen registers and other means. It also has significantly increased the scope of subpoenas and search warrants while limiting judicial review of them, and expanded surveillance authority under the Foreign Intelligence Surveillance Act, or FISA, which regulates the collection of information for counterintelligence purposes.

Legal experts say that while none of the vast powers granted under the act are specifically tailored to journalists, it is so overbroad and far-reaching – especially the "other purposes" and similar clauses – that it has potentially grave potential abuses with regard to the media.

The problem is that so much of the investigative powers are cloaked in secrecy that no one really knows, except the administration, how frequently the provisions of the Patriot Act are being used against journalists. That is especially the case when it comes to monitoring and gathering phone calls, emails and other electronic and digital communications.

Kirtley has scoured the law for its implications on journalists, and concluded that, "There is nothing explicit in the law that says we'll go after the press. … "What concerns me is the degree of digital surveillance that the Patriot Act allows that can be specifically used against journalists, especially since we don't have a federal shield law."

As for the details, entire books have been written on the potential use (and misuse) of the Patriot Act, including the American Bar Association's excellent "Patriot Debates: Experts Debate the USA Patriots Act" and Patriots Debate: Contemporary Issues in National Security Law." And numerous civil liberties and constitutional law groups follow the many aspects of the Patriot Act closely, including The Federation of American Scientists' Secrecy Blog and EPIC, the Electronic Privacy Information Center. EPIC also has a good breakdown of the many PATRIOT Act provisions, including its regulation of wiretaps, search warrants, pen/trap orders, subpoenas, FISA or foreign intelligence surveillance and statutes regarding the provision of material support for terrorism.

Vladeck says the some critics' concerns are overblown. "I don't know where obsession with the PATRIOT Act is coming from. Yes, the phone records program under section 215 that Snowden

exposed would also encompass reporters, but there's no reason to think that the government is specifically targeting reporters under that section."

"Perhaps the larger point is how much easier it is for the government to undertake leak investigations with these surveillance tools, and so how much less significant issues like reporter's privilege might be, since the government wouldn't need to specifically subpoena a reporter to obtain call records, etc."

One primary concern for journalists has been the legal justification that the Patriot Act provides for the NSA's broad surveillance programs when used in conjunction with other laws and legal precedents such as the Foreign Intelligence Surveillance Act (FISA) of 1978 and Presidential Executive Order 12333.

The language in Section 215 is especially broad, experts say, because it allows the government to order the collection of "any tangible things" as long as the FBI specifies that it's for "an authorized investigation . . . to protect against international terrorism or clandestine intelligence activities."

Within the Patriot Act, Sections 214, 215 and 216 are of particular concern to journalists who fear that they can be used to collect vast amounts of wire or electronic communication metadata and other forms of information about them, their sources and their stories, according to legal experts. In many cases, the provisions don't require notifying the target of that surveillance and related information gathering efforts, including phone calls and emails to sources living overseas.

Essentially, as this NYU Law School Brennan Center report explains, Section 215 allows the government to obtain a secret court order requiring third parties, such as telephone companies, to hand over any records if deemed "relevant" to an international terrorism, counter-espionage or foreign intelligence investigation. It notes that Section 215 orders may have been combined with requests under other provisions of the Patriot Act, like Section 216, which governs access to online activity such as email contact information or Internet browsing histories.

The collection and analysis of Verizon call records, including phone numbers and location data, have been authorized as the collection of "business records" under the PATRIOT Act. (Here's one of many good analyses).

The Snowden disclosures opened a window into how some of the programs authorized under the broad umbrella of the Patriot Act work, as well as Section 702 of the related FISA Amendments Act, a law first passed in 2008.

One of the most controversial programs disclosed by Snowden and the reporters he was working with is PRISM, which allows the NSA to access emails, search histories, audio chats and other content as authorized under 2008 amendments to FISA. PRISM allows the government to acquire foreign intelligence by targeting non-U.S. persons "reasonably believed" to be outside U.S. borders. That can be difficult to ascertain when dealing with internet or cell phone communications.

Another area of concern to journalists has been national security letters, or administrative subpoenas that authorize the FBI to compel the recipient to divulge subscriber and billing information relevant to a national security investigation. These letters require no judicial review and the recipient had been prohibited from challenging or even revealing the contents or existence of the letter, although that has been changed under Patriot Act amendments. EPIC has a good primer on them.

It is unclear how many times the provisions of the Patriot Act have been used to gain access to reporters' notes and confidential sources, mostly because of government doesn't have to notify the targets of much of the surveillance.

Back in 2003, the FBI invoked the PATRIOT Act at least 13 times to demand that journalists that had interviewed computer hacker Adrian Lamo preserve their notes and all other relevant information in anticipation of Justice Department subpoenas to hand over the material. The requests were dropped after complaints were made, and DOJ officials said the subpoenas were not authorized because they violated procedural departmental guidelines.

Mark D. Rasch, the former head of the Justice Department's computer crime unit wrote a good piece titled, "The Subpoenas are Coming!," contending that such uses of the Patriot Act were bypassing the First Amendment.

In May 2006, ABC News quoted a senior federal law enforcement official saying the government was tracking the phone numbers used by its reporters in an effort to root out confidential sources.

In a recent report for the Committee to Protect Journalists titled "The NSA Puts Journalists Under a Cloud of Suspicion," Geoffrey King interviewed William Binney, a former NSA mathematician and code breaker. Binney, who resigned from the NSA to protest what he said were mass privacy violations, said he believes the government keeps tabs on all reporters.

"They have a record of all of them, so they can investigate, so they can look at who they're calling--who are the potential sources that they're involved in, what probable stories they're working on, and things like that," he told CPJ.

Journalists, Binney added, are "a much easier, smaller target set" to spy on than the wider population, and in his view, the NSA most likely takes advantage of this.

Lucy Dalglish, who is now dean of the Philip Merrill College of Journalism at the University of Maryland, said such fears appeared to have been confirmed by a national security representative of the Obama administration at a dialogue with media leaders back in 2011.

That official, Dalglish wrote in a blog post when she was the executive director of the Reporters Committee, "told us (rather gloatingly) on our last day: We're not going to subpoena reporters in the future. We don't need to. We know who you're talking to."

ACKNOWLEDGEMENTS

The report couldn't have been done without the gracious assistance of a small army of experts. But special thanks goes to: Jane Kirtley, the Silha Professor of Media Ethics and Law at the University of Minnesota and the former executive director of the Reporters Committee for Freedom of the Press; Stephen Vladeck, law professor and associate dean for scholarship at American University's Washington College of Law; Rick Blum, coordinator of the Sunshine in Government Initiative; Connie Pendleton, co-chair, Media Law Practice at Davis Wright Tremaine LLP; Holly McMahon, staff director of the American Bar Association's Standing Committee on Law and National Security; Executive Director Bruce Brown and Legal Defense Director Gregg Leslie of the Reporters Committee for Freedom of the Press; Sophia Cope, director of Government Affairs/Legislative Counsel for the Newspaper Association of America; Kathleen Hirce and Dave Heller, staff attorneys at the Media Law Resource Center; Steven H. Levin of Levin & Curlett LLC; Benjamin Wittes of the Lawfare blog and senior fellow and research director in Public Law at The Brookings Institution; Marion (Spike) Bowman, former deputy, National Counterintelligence Executive and deputy General Counsel, National Security Law, for the Federal Bureau of Investigation; Steven Aftergood, director of the Federation of American Scientists' Project on Government Secrecy and writer of its Secrecy News blog; Wells C. Bennett, fellow in National Security Law at the Brookings Institution and managing editor of Lawfare; Praveen Madhiraju of the Center for American Progress; Harvey Rishikof, chair of the American Bar Association's advisory Committee on Law and National Security; and Ellen Shearer and Tim McNulty of the Medill National Security Journalism Initiative and former Department of Homeland Security Deputy Assistant Secretary for Policy Paul Rosenzweig, all of whom were co-editors of the ABA book, "National Security Law in the News."