# MEDILL NATIONAL SECURITY JOURNALISM INITIATIVE

NATIONALSECURITYZONE.ORG

## HOW TO AVOID LEGAL TROUBLE OVER SOURCES AND SECRETS

By JOSH MEYER



josh@northwestern.edu 202-365-2401 @JoshMeyerDC

This primer is based on extensive research done for a background brief for the Sources and
Secrets Symposium, a Forum on the Press, the Government and National Security that was held
March 21, 2014, at the Times Center in New York City and co-sponsored by the New York
Times.

More information on the Symposium can be found at  $\underline{sourcesandsecrets.com}$ .

### **TABLE OF CONTENTS**

INTRODUCTION	4
WHY YOU SHOULD CARE	4
THE EVOLVING DOJ GUIDELINES ON SUBPOENAS	6
STATUTES, INCLUDING THE ESPIONAGE ACT	8
WHAT IS THE ESPIONAGE ACT AND WHAT DOES IT DO?	8
HOW CAN THE ESPIONAGE ACT BE USED YOU?	9
THE IMPORTANCE OF 'INTENT'	10
EXAMPLES OF THE ESPIONAGE ACT BEING USED	11
OTHER STATUTES USED AGAINST JOURNALISTS AND SOURCES	13
THE PATRIOT ACT	15
MORE INFORMATION AND RESEARCH	18

#### INTRODUCTION

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 in the summer of 2013 after it became clear that the Obama Justice Department had made unprecedented intrusions into reporters' efforts to gather information and obtain government documents.

By using this guide, you can become familiar with these news developments and with the applicable regulations and laws – established by Congress or legal precedent – so that you can avoid getting your sources, and yourself, in legal trouble.

Among the topics this primer covers:

- Use of the Espionage Act and other statutes to go after reporters' sources.
- 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.
- Justice Department guidelines on subpoenas, including recent revisions.
- Relevant provisions of the USA PATRIOT Act.

#### WHY YOU SHOULD CARE

Even a minor skirmish with federal authorities can require journalists to spend huge amounts of money on lawyers, legal advice and associated costs, not to mention time. Such legal challenges, whether a subpoena or an investigation that could lead to charges, can be financially backbreaking.

That is especially the case for freelancers and those reporters working for the many small media outlets that now cover these issues, particularly in light of the aggressive stance of the Obama administration in going after reporters and their sources.

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 <u>recent report</u> by the Committee to Protect Journalists provides more detail.

#### Some examples:

• The administration continues to go after individual journalists, especially New York Times

reporter James Risen, who it is trying to put in jail for refusing to identify the source of information for his 2006 book, "State of War: The Secret History of the CIA and the Bush Administration." The Supreme Court said in June 2014 that it would not hear Risen's appeal, making him in contempt of court, but the administration had not yet said what it plans to do to get the presiding judge to enforce the contempt of court order.

- The Justice Department 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.
- The FBI, it was learned, 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.
- The avalanche of disclosures about previously undisclosed National Security Agency surveillance programs, spurred by Snowden, a former NSA contractor, raised additional questions about the lengths to which U.S. intelligence agencies were monitoring the public at large and reporters.

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 law that protects journalists and directly or indirectly their sources from government attempts to stop the flow of information between them.

#### LAW VERSUS POLICY

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 <u>document outlining the</u> <u>recently approved new guidelines</u> 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."

#### THE EVOLVING DOJ GUIDELINES ON SUBPOENAS

Despite their importance, the Justice Department had operated under essentially the same set of guidelines regarding subpoening members of the media since 1970. They're found <a href="here">here</a>, at 28 <a href="here">C.F.R. s. 50.10</a>, 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 advances, including email, text messaging or Skype, or information gathered by NSA's vast signal 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 about 30 news media organizations as well as with First Amendment groups, media industry associations and academic experts, and invited others to also submit suggestions.

The Reporters Committee coordinated a proposal from some 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, <a href="the final updated DOJ policy">the final updated DOJ policy</a> 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 <u>July 12 report</u> 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 <u>detailed summary of the changes</u> 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 -- 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 <u>in a statement</u> 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.

#### STATUTES, INCLUDING THE ESPIONAGE ACT

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 (March 2014).
- Seven years later, New York Times Co. v. United States the Pentagon Papers case which 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."

- 1. 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.
- 2. 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, as 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 AND WHAT IT DOES

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.

While those threats were real, Congress rejected attempts by the Woodrow Wilson administration to include some level of press censorship during wartime regarding publishing 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. Congress repealed it 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 <u>The Espionage Statutes And Publication Of Defense Information</u> 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."

#### HOW CAN THE ESPIONAGE ACT BE USED AGAINST YOU?

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 affect reporters, which are linked to below, thanks to the <u>Cornell Law Library</u>:

- § 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

Gary 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."

- 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.

#### THE IMPORTANCE OF 'INTENT'

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 "<u>Problems</u> with the <u>Espionage Act</u>," 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.

Wittes said that besides being very old and very vague, 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.

#### EXAMPLES OF THE ESPIONAGE ACT BEING USED

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 others. 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 post-publication 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 what journalists do every day; obtaining and disseminating 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. And Wikipedia is often a good place for a summary of these cases and links to the original case material, but be careful of the information and make sure you verify it).

- 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 <a href="mailto:making falsestatements">making falsestatements</a>. 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.
- <u>JEFFREY STERLING</u> 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. That could change now that the Supreme Court said in June 2014 that it would not hear Risen's appeal, making him in contempt of court (the administration had not yet said what it plans to do to get the presiding judge to enforce the contempt of court order. Sterling faces potentially decades in prison if convicted on all counts; Risen has been subpoenaed but not charged.

- <u>JAMES HITSELBERGER</u> 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 that allegedly revealed troop activities and gaps within U.S. intelligence about Bahrain.
- <u>EDWARD SNOWDEN</u> 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.

#### OTHER STATUTES USED AGAINST JOURNALISTS AND SOURCES

A patchwork of other statutes affects reporters and their sources. 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 <a href="Valerie Plame leak investigation case">Valerie Plame leak investigation case</a>. This <a href="Congressional Research Service report">Congressional Research Service report</a> 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.
- 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.

#### THE PATRIOT ACT

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

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 <u>Section 215 is especially broad</u>, 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 Patrio 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, <u>wrote a good piece</u> 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 "<u>The NSA Puts Journalists</u> <u>Under a Cloud of Suspicion</u>," 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 in 2011.

That official, Dalglish <u>wrote in a blog post</u> 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."

#### MORE INFORMATION AND RESEARCH

Experts who were consulted in the writing of this report.

- Steven Aftergood, director of the Federation of American Scientists' Project on Government Secrecy and writer of its Secrecy News blog.
- 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.
- Bruce Brown, executive director, and Gregg Leslie, legal defense director, 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 FBI.
- Wells C. Bennett, fellow in National Security Law at the Brookings Institution and managing editor of Lawfare.
- Harvey Rishikof, chair of the ABA's advisory Committee on Law and National Security.
- Former Department of Homeland Security Deputy Assistant Secretary for Policy Paul Rosenzweig, and Ellen Shearer and Tim McNulty of the Medill National Security Journalism Initiative, all of whom were co-editors of the ABA book, "National Security Law in the News"