Unmasking "John Doe" Leaks

By John Fraser

The federal government leaks secrets to a shocking extent, and yet there is at least one commonly available litigation tool that the government has failed to deploy to combat leaks. In the world outside the government, the right to control confidential information, to protect trade secrets, and to maintain the confidence of business allies, is protected by use of "John Doe" lawsuits.[1] These civil lawsuits name an unknown John Doe defendant and seek immediate discovery from nonparty businesses to unmask the defendant and seek civil remedies for unauthorized uses of information. The federal government has never embraced the broad use of this tool.

John Doe suits have been heavily publicized in recent years as effective tools in the investigation and deterrence of the misuses of intellectual property. In particular, thousands of John Doe suits have been filed by the entertainment industry to unmask anonymous thieves. Private industry has publicized these suits as a deterrent to piracy of intellectual property. If the federal government is to deter the unauthorized disclosure of classified information by employees and contractors, it should borrow the John Doe lawsuit from the private sector, file and publicize such suits, and educate the federal workforce as to the use of this tool. Frequent and well-publicized use of John Doe lawsuits by the government will help to erode the culture that has developed within the federal government that tolerates leaks or regards them as unstoppable.

John Doe lawsuits should be used to supplement criminal law processes that were not specifically designed to identify anonymous sources of leaks. In any event, few defendants are identified through criminal processes, and very few are punished.[2] Because John Doe lawsuits and subpoenas are civil proceedings, and because business corporations may not assert Fifth Amendment rights, John Doe lawsuits are effective in unmasking anonymous actors in the private sector. Accordingly, John Doe lawsuits are crucial in identifying the heretofore unknown actors.

Civil discovery procedures allow for broader discovery than do criminal procedures. Obtaining evidence from media corporations via search warrants in a criminal case is limited under the Privacy Protection Act, whereas a subpoena of media corporation records in the civil context is not so restricted. The fruits of civil discovery may be used to initiate proceedings to suspend and revoke security clearances, to discipline errant employees and contractors, and to support criminal referrals.

The Department of Justice (DOJ) is fully authorized to represent the government in civil proceedings, and research reveals no legal bar to governmental use of John Doe lawsuits to combat unauthorized releases of classified information. DOJ needs to include this tool in its arsenal to combat the unauthorized release of classified information. DOJ should authorize and encourage U.S. attorneys to use John Doe suits to further develop those cases that cannot be successfully prosecuted in the criminal courts.

Defining the Problem and the Opportunity

The government's historical use of criminal law to deter unauthorized disclosures of information[3] has not deterred the torrent of unauthorized releases of classified information that have occurred in recent years.[4] For example, a 2013 Rand report concluded that the organizational culture of the Department of Defense treats leaks of classified information as a "risk free" enterprise.[5] Edward Snowden, who now resides in Russia and conducts a campaign of leaks against the National Security Agency that once employed him as a system adminsitrator, has been lionized in the press. President Barack Obama's administration has forcefully sought to use criminal law processes to deter leaks by employees and contractors of federal agencies.[6] However, to be deterred, government employees and contractors who leak classified information must first be unmasked.

Criminal Law Is a Limited Deterrent

Historically, the government has relied on criminal law and criminal investigative procedures to deter and pursue anonymous leaks.[7] Executive Order 12333 requires that leaks of classified information be reported to the U.S. attorney general as criminal acts.[8] While some administrative remedies are available against employees and contractors who choose to commit unauthorized releases of classified information, the penalties are ineffective against anonymous actors.[9] The primary reliance on criminal law is due to the fact that the U.S. Code contains many criminal penalties for unauthorized releases of classified information but no directly relevant civil penalties.[10] For example, the Espionage Act provides criminal law remedies against unauthorized release of classified information when the release is intended to aid a foreign enemy, and in other circumstances.[11]

However, criminal law procedures are of limited use against anonymous leaks. Under current practice, the FBI handles leaks reported to DOJ under the relevant executive order. Attempts to narrow down the possible source(s) of a leak follow well-known investigative paths.[12] Criminal grand jury subpoenas are sometimes issued to reporters seeking the names of sources.[13] However, to be effective, all of the criminal law remedies are dependent on being able to name and indict the source of the leak after the investigation is complete.[14] An unknown number of criminal investigations are commenced and then closed when a defendant cannot be identified. In the normal course of a leak investigation, the FBI will be stymied by the inability to identify the source of the leak. [15] After exhausting all the resources of the criminal process, the matter will then be closed pending further developments. The referring agency will then be notified that the FBI is unable to move forward on the matter due to inability to identify the proper defendant. [16]

Very few employees or contractors have been indicted for unauthorized releases of classified information.[17] Judging from the recent flow of leaks, the criminal law remedies employed by the government do not adequately deter anonymous unauthorized releases of classified information.

Criminal leak investigations regularly impinge on the publishers of classified information because the publishers have directly relevant information about the source of the information they publish.[18] When a policy decision is made to prosecute a leak and compel grand jury testimony from a publisher, each such use of criminal legal process is met with protests about First Amendment values and the right of the public to know and the right of the media to publish otherwise classified information that belongs to the government.[19] Wealthy media interests and some public-interest groups argue that any use of the criminal legal process to investigate or prosecute leaks is extreme, unbalanced, a threat to the First Amendment, contrary to public policy, and a political act against a free press.

Some of the accusations about political suppression of press rights are based on the argument that a government-issued subpoena addressed to a publisher is selective prosecution for a leak that the government did not authorize. In response to the accusation of selective prosecution, the attorney general has re-issued guidelines requiring prosecutors to use criminal and civil investigative processes against publishers and journalists only after exhausting all other approaches.[20] In a typical case, this exhaustion is accomplished through an FBI investigation of all nonmedia sources of information. When the defendant cannot be identified, the matter ends, because DOJ has elected not to proceed in civil court. In the private sector, a different approach is taken.

Media Companies Use Civil John Doe Suits To Protect Their Rights and Property

Media and news companies have long been tenacious in using civil processes to protect their exclusive information rights and property.[21] Media entities are particularly vigilant about protecting their own trade secrets and confidential information.[22] In one such case, a magazine went so far as to sue a competing magazine and several of its former employees to protect its confidential process for binding its magazines and other trade secrets.[23] Media companies and publishers also zealously guard against copyright or trademark infringement by other media companies and individuals.[24] In a recent example, the Associated Press sued a news-monitoring service for copyright infringement, because the news-monitoring service delivered excerpts of 33 articles registered to the Associated Press.[25] While the news-monitoring service's excerpts ranged from 4.5 to 60 percent of the registered articles, the court found the defendant's assertion of fair use and other defenses unpersuasive and granted the Associated Press' motion for summary judgment.[26] Overall, these cases illustrate the lengths to which media companies go to protect their own confidential information from disclosure or use. Yet, when media companies use the federal discovery processes to enforce exclusive information claims, the First Amendment is not typically raised by other media parties as a bar to discovery.[27]

Other Private Sector Businesses Have Aggressively Deployed John Doe Suits To Protect Confidential Information

In recent years, in response to the problem of leaking intellectual property owned by private-sector businesses, the federal courts have considered thousands of John Doe suits filed by business plaintiffs against anonymous leakers of confidential information. These suits include efforts to enforce the Copyright Act, [28] securities laws,[29] trade secret laws,[30] defamation laws,[31] and numerous other claims.[32] These John Doe suits utilize nationwide civil discovery to unmask John Doe defendants and proceed against them as named defendants. All of these suits start from the premise that the John Doe procedure is available to protect the confidentiality of information entrusted to persons who have violated a trust.[33]

The Federal Government Uses Civil John Doe and Pseudonym Suits Sparingly

In contrast to private-sector cases, research reveals only a handful of instances where the United States has employed the John Doe civil procedure tool as a plaintiff or as a Freedom of Information Act (FOIA) party.[34] None of these cases involve government use of the John Doe procedure to combat leaks of classified information. However, in 2011, the United States did employ a civil complaint against a pseudonymous defendant to seek civil remedies. Steps were taken in civil court against a defiant and open release of classified information by a former CIA employee. In *United States v. Ishmael Jones,* the government successfully sought a permanent injunction, imposition of a constructive trust for the proceeds of a published book, and a declaration that federal law condemned the unauthorized releases of classified information.[35] The civil remedies in *Ishmael Jones* were decreed against a former employee who knowingly and intentionally provided classified information to a commercial publishing house for the purpose of publishing and selling a book.

There does not appear to be a reason why the government has rarely utilized the John Doe tool. In cases where the person(s) revealing secrets are not known, the civil process may well be superior to the criminal process.

Except for the self-imposed DOJ policy limits discussed above,[36] there are fewer restrictions on governmental use of civil discovery tools than are in place for the use of criminal procedures when media interests are involved in the case. Civil discovery is routinely recognized as more expansive than the limited discovery in criminal proceedings. Federal law and the Federal Rules of Criminal Procedure restrict the information that may be obtained from media corporations or reporters during a criminal investigation. For example, the Privacy Protection Act of 1978, 42 U.S.C. § 2000aa *et seq*., "generally prohibits government officials from searching for and seizing documentary materials possessed by a person in connection with a purpose to disseminate information to the public." The practical effect of this provision is to prevent law enforcement officials from using search warrants to obtain evidence from reporters in a criminal investigation unless the reporter possessing the evidence is a suspect in a crime other than receipt or possession of the information, the information the reporter possesses is classified or national defense related information, or the information is necessary to prevent death or serious bodily injury. While the Privacy Protection Act specifically addresses the use of search warrants in criminal prosecutions, there is no corresponding statutory limitation on subpoenas directed at media corporations or reporters during civil discovery.

The Government Should Consistently Deploy This Additional Tool and Publicize Its Use

The recent torrent of leaks, the inability to unmask these actors through criminal proceedings, and the limited effectiveness of the criminal remedies deployed by the government support the aggressive use of the John Doe civil procedure tool to protect confidential information. The John Doe tool is available to the government and, in an appropriate leak case, should be employed to unmask the source of the leak. Without the John Doe tool, the government will rarely identify, prosecute, and sanction bad actors.

In response to the accusation of selective prosecution, the attorney general has re-issued guidelines requiring prosecutors to use criminal and civil investigative processes against publishers and journalists only after exhausting all other approaches.

Can John Doe Suits Be of Practical Value to the Government?

Various legal, policy, and procedural questions must be addressed before a decision is made to pursue a John Doe civil action. These questions include:

- What are the legal bases for use of that procedure?
- What defenses, pitfalls, or defensive tactics should be expected to appear if a civil suit is filed?
- May evidence gathered by criminal grand juries or criminal investigations be used in the preparation of civil leak cases?
- May third parties be targeted for discovery in such a suit?
- How will media interests and public interest groups react to the use of the John Doe civil litigation tool?
- Does private sector experience with the John Doe tool permit an estimate of likely success if the government employs this procedural tool?

There can be no question that federal employees and contractors owe an enforceable fiduciary duty of care to the government that has entrusted them with confidential information.[37]

Further, the potential remedies that flow from a breach of the fiduciary duty are numerous. These remedies include establishment of an equitable trust to attach proceeds of the breach, including any payments, profits, and royalties.[38] A breach of the fiduciary duty is also a proper subject of a permanent injunction when a propensity to commit violations is shown.[39] Restitution or court-ordered return of the government's property (including documents) has also been ordered.[40] Punitive damages may be awarded by a jury, but a judge may do so only if a jury trial is waived.[41]

Compensatory damages are available for a breach of contract, in addition to disgorgement of profits. The secrecy agreement signed by each employee stipulates that the government is entitled to an injunction for a breach of confidentiality because there is no adequate remedy at law.[42]

Employees who release classified information without authorization face the full range of administrative discipline and penalties,

including clearance revocation and suspension, reprimand, loss of pay, reassignment, demotion, and termination.[43]

None of these remedies or administrative actions are available to the government to deter leaks of classified information unless the government can identify the source of the leak. When the government has exhausted the criminal investigative process, the law allows the Department of Justice to proceed to the civil side of the court system to seek a remedy.[44] Current DOJ policy permits the FBI to provide information from its criminal investigative files to support administrative sanctions and proceedings against federal employees who are suspected of leaking classified information.[45]

Once a civil suit has been used to unmask source of the leak, a criminal indictment may be sought, or civil proceedings may continue, so long as due process rights are protected in the process.[46] While the government cannot bring a civil case only to obtain information for use in a criminal prosecution, the government does have the authority to use information obtained in the course of a civil action in a criminal prosecution where appropriate.

In addition to the case law allowing use of information obtained in civil discovery in a criminal prosecution, DOJ policy explicitly calls for its attorneys to "consider investigative strategies that maximize the government's ability to share information among criminal, civil, and agency administrative teams to the fullest extent appropriate to the case and permissible by law …"[47] Further, the attorney general recently stated that "[c]ivil trial counsel should apprise prosecutors of discovery obtained in civil, regulatory, and administrative actions that could be material to criminal investigations."[48] Sharing information between civil litigators and criminal prosecutors is not only allowed but is encouraged by the attorney general.

Who May Be Targeted for Discovery in a Civil John Doe Suit?

Private persons and corporate publishers of confidential government information may be targeted for discovery under DOJ regulations in both civil and criminal matters only after other sources of information have been exhausted.[49] Recently announced DOJ policy guidelines require that media entities be targeted for discovery "only as a last resort, after all reasonable alternative investigative steps have been taken, and when the information sought is essential to a successful investigation or prosecution."[50] This new policy requires that all requests to use legal processes to obtain information from news media "be submitted to, and initially evaluated by, the Criminal Division's Office of Enforcement Operations before they are ultimately forwarded to the Attorney General for decision."[51] These procedures also require the express endorsement of the relevant U.S. attorney or assistant attorney general.[52] In addition, requests for authorization "to seek testimony from a member of the media that would disclose the identity of a confidential source" will also be routed through the News Media Review Committee to provide assessments of the requests.[53] In investigations of disclosures of classified information, DOJ's updated policy also requires that the director of National Intelligence "certify to the Attorney General the significance of the harm that could have been caused by the unauthorized disclosure and reaffirm the intelligence community's continued support for the investigation and prosecution before the Attorney General authorizes the Department to seek media-related records …"[54] It is important to note, however, that publishers who publish leaked confidential information are not themselves subject to civil liability for such publications.[55] While DOJ policy continues to be that reporters "will not be subject to prosecution based solely on newsgathering activities"[56], DOJ has succeeded in persuading federal courts to commit uncooperative reporters to jail on three occasions in the last 20 years in criminal leak investigations.[57]

Unlike individual reporters, publishers of classified information may not simply plead the Fifth Amendment and refuse to testify in civil litigation. Individual reporters have the right to plead the Fifth Amendment and refuse to incriminate themselves by revealing a news source.[58] However, this right should not be confused with a reporter's so-called privilege to refuse to testify, which does not exist under federal law.[59] Moreover, the press may publish what it learns, but its ability to obtain information is limited by criminal law.[60] While an individual reporter may plead the Fifth Amendment to avoid prosecution[61], his corporate employer has no such right. In a civil proceeding in which a corporation is required under Fed. R. Civ. Pro. 30(b)(6) to provide a knowledgeable officer or employee to testify at a deposition[62], the corporate publisher may not refuse to truthfully answer questions on the ground of self-incrimination.[63] For example, a district court recently held that a news corporation was required to provide a corporate representative to testify under Rule 30(b)(6) when the reporter involved in publishing the article at issue invoked his Fifth Amendment privilege.[64] The court also indicated that the corporate publisher could be subject to sanctions if it failed to provide a representative to testify.[65]

If publishers may not refuse to participate in civil discovery, how will they respond? Publishers and reporters have a vested interest in seeking to discourage the government from using civil litigation to uncover leaks. As they do in criminal proceedings, many journalists will risk contempt of court and seek to claim Fifth Amendment self-incrimination privileges, First Amendment privileges, reporter privileges, and other privileges to obtain, print, and disseminate classified information. They will interpose many procedural and other hurdles in order to block discovery of the name of the John Doe defendant. John Doe defendants, publishers of leaked information, and civil liberties groups may move to intervene at the earliest stages of the litigation to oppose leave to discover the identity of a Doe defendant. Media interests and John Doe defendants will seek dismissal of the suit, move to block discovery against third parties, and resist amendment of the complaint to name the actual defendant when discovery is successful.

However, based on the success rates of private sector business plaintiffs in John Doe suits, it can be expected that the privilege assertions and procedural hurdles will not generally be successful.[66] Corporate publishers that have written documents, emails, faxes, telephone bills, or other records of communications with John Doe defendants will have to produce those records in civil proceedings, even when an individual reporter successfully claims a Fifth Amendment privilege.[67]

The service of discovery subpoenas may trigger a motion to quash on the ground that the First Amendment protects the subpoena recipient from having to disclose the identity of the defendant. This type of motion will be strongly supported by

various civil liberties and well-funded publisher and media interest groups.[68] However, the law that has developed in private sector John Doe cases (and other intellectual-property leak cases) strongly supports the government's use of expedited discovery to identify the defendant. Although some courts recognize a qualified reporters' privilege to protect news sources[69], the privilege can be overcome by the government. The government will need to show (1) a strong case on the merits, (2) a logical reason to believe that the particular recipient of a subpoena possesses directly relevant information, and (3) that all other known sources of information regarding the source of the leak have been developed and found wanting.[70] When the government demonstrates these three facts, the court should uphold the subpoena and require the publisher of the confidential information to identify its source.

Civil cases in which media companies have litigated with each other plainly establish that there is no general privilege for a media company to take the property of another person and then refuse to participate in civil discovery relating to that same taking.[71] Research has identified very few civil cases in which a media company has asserted the First Amendment when litigating the issue of leaked or stolen property.[72] This body of case law establishes that, when a media company is litigating against another media company, the court-compelled disclosure of confidential information does not present a First Amendment issue.

It is also possible that an objection will be raised that a John Doe suit filed by the government is unreasonable under the Fourth Amendment prohibition of unreasonable searches and seizures. However, the government may proceed against a John Doe when there is probable cause to believe that a violation of law has occurred and that the John Doe defendant may have committed the violation.[73] Any motion for expedited discovery should be drafted to satisfy the Fourth Amendment requirement for probable cause for a warrant or court order.

Publishers may also assert an absolute or qualified reporters' privilege under federal common law (Fed. R. Evid. 501) and the First Amendment.[74] In general, federal law does not recognize a privilege for reporters under the First Amendment.[75] Those courts that have recognized a qualified privilege have ruled in leak cases that when a leak of confidential information to a reporter is what caused the litigation, then the reporter is a proper target of discovery.[76] When a leak of confidential information to a reporter is the crux of the case, the statements or transmissions to the reporter are uniquely relevant, and the court will order their production if the court finds them relevant after *in camera* review.[77] In a civil leak case, where the central issue is who released what to the publisher of the confidential information, disclosure may be ordered when the plaintiff demonstrates the central relevance of the journalist's information.[78]

Conclusion

If the federal government is to make progress in deterring leaks of confidential information, it must look to all lawful sources of innovation. The private sector, led by giant media corporations, has deployed John Doe suits to deter and punish those who compromise its secrets. The federal government should learn from the example. ⊙

John A. Fraser III is a civilian attorney in the U.S. Department of Defense. The views expressed herein are personal to the author and are not the views of the U.S. government or any portion thereof.

Endnotes

[1]A John Doe suit includes any civil suit where the identity of at least one defendant is not known at the commencement of the suit. This includes suits against John or Jane Doe, suits against pseudonymous defendants where the true identity behind the pseudonym is not known, and suits against unnamed defendants.

[2]The January 2015 leak conviction of a former CIA intelligence officer under the Espionage Act was referred to in the popular press as one of only three such convictions to have occurred in history of the Espionage Act. www.nytimes.com/2015/01/27/us/politics/cia-officer-in-leak-case-jeffrey-sterling-is-convicted-of-espionage.html.

[3]*See* David E. Pozen, *The Leaky Leviathan, etc.,* 127 Harv. L. Rev. 512, 515-516 (2013) (describing limited number of criminal prosecutions in last 75 years).

[4]Both the chairman of the House Intelligence Committee and the chairman of the Senate Intelligence Committee have condemned the recent torrent of leaks. *Press Release of Intelligence Committee*, (July 25, 2012), intelligence.senate.gov/press/record.cfm?id=337333.

[5]James Bruce and W. George Jameson, *Fixing Leaks: Assessing the Department of Defense's Approach to Preventing and Deterring Unauthorized Disclosures,* page xi (Washington, D.C., Rand Corp., Dec. 12, 2013)

[6]Charlie Savage, *Former F.B.I. Agent to Plead Guilty in Press Leak*, The New York Times, Sept. 23, 2013, at A1, *available at* www.nytimes.com/2013/09/24/us/fbi-ex-agent-pleads-guilty-in-leak-to-ap.html?_r=0. In 2012, a former CIA officer named Kiriakou was indicted in a leak case. *See* Andrea Papagianis, *Former CIA Officer Charged with Leaking Info to Journalists,* Reporters Committee (Jan. 23, 2012), www.rcfp.org/browse-media-law-resources/news/former-cia-officer-charged-leaking-info-journalists*).* The administration was reported as aggressively pursuing a second criminal leak case against former CIA employee Sterling. Michael Calderone and Dan Froomkin, *'Reporter's Privilege' Under Fire from Obama Administration Amid Broader War on Leaks*, Huffington Post (May 18, 2012), www.huffingtonpost.com/2012/05/18/reporters-privilege-obama-war-leaks-new-york-times_n_1527748.html.

[7]*See* David E. Pozen, *supra* n. 2 at 515-516 (describing limited number of criminal prosecutions in last 75 years); *see also* Irina Dmitrieva, Note, *Stealing Information: Application of A Criminal Anti-theft Statute to Leaks of Confidential Government Information,* 55 Fla. L. Rev. 1043 (2003) (reviewing history of government use of some criminal statutes in anti-leak cases).

[8]Exec. Order No. 12,333, Section 1.6(b), 46 Fed. Reg. 59941 (Dec. 4, 1981).

[9]Exec. Order No. 12,065, 43 Fed. Reg. 28949 (June 28,

1978) (employees who disclose classified information may be terminated from the civil service). Also 5 U.S.C. § 7532 (2013) authorizes dismissal of employees when necessary to protect national security. Similar provisions are found in 10 U.S.C. § 1609 and 50 U.S.C. § 3036(e). Administrative sanctions are also available against investigative and law enforcement personnel who disclose information without authorization under the Patriot Act, 18 U.S.C. § 2520(g).

[10]In 2012, the Senate considered a bill that would strip intelligence community employees who leak classified information of their pension rights, among other provisions. *Press Release of Intelligence Committee*, *supra* n.3. The 2012 bill was designed to overcome constitutional objections that doomed the Hiss Act, which deprived civil servants of pension rights if they engaged in espionage against the United States. *See Hiss v. United States Civil Service Commission,* 338 F. Supp. 1141 (D.D.C. 1972) (holding pension forfeiture statute unconstitutional as applied to Alger Hiss).

[11]18 U.S.C. § 793, *et seq*. In his book, *Necessary Secrets: National Security, the Media, and the Rule of Law,* Gabriel Schoenfeld offers a careful and well-reasoned defense of the use of the Espionage Act and other criminal statutes to prosecute media publishers of classified information and their insider sources. *See* Gabriel Schoenfeld, *Necessary Secrets: National Security, the Media, and the Rule of Law* (2010).

[12]In 2010, the Senate Judiciary Committee received a report from the Department of Justice describing in some detail the procedures followed by the FBI when a leak referral is received from the Intelligence Community. *Answers to Questions from Senate Judiciary Committee*, U.S. Department of Justice, April 8, 2010, www.fas.org/irp/agency/doj/intel-leak.pdf. The DOJ report concluded that criminal prosecutions are rare because of anonymity and suggested that agencies should seek to pursue administrative remedies. *Id.* No advice was offered as to how to overcome the problem of anonymity.

[13]*See In re Grand Jury Subpoena (Judith Miller),* 397 F.3d 964, 968-973 (D.C. Cir. 2005), *cert. denied*, 545 U.S. 1150 (2005) (leak of intelligence operative's name overcomes common law reporter's privilege).

[14]The government does have the option of seeking a John Doe indictment, which can later be amended to state the name of the actual defendant when that person is identified. To be an effective deterrent, this tool requires identification of the offender so that the Doe defendant may be named in an amended indictment. *See United States v. John Doe, aka Hagla*, 661 F.3d 550 n.1 (11th Cir. 2011) *cert. denied*, 132 S.Ct. 1648 (2012) (describing reason for use of John Doe indictment in criminal proceeding).

[15]The 2013 Rand report to the USD(I) identified the inability to identify the source of a leak as one of the three primary reasons for a perception in DoD that leaks are tolerated. Bruce & Jameson, *Fixing Leaks, supra*, n. 4 at 35-36.

[16]David E. Pozen, *The Leaky Leviathan*, *supra* n. 2 at 536 (describing historic indictment rate of classified leaks as below 0.3% and "probably far closer to zero.").

[17]One author concluded that only four federal employees have been indicted for leaks to media publishers in 94 years following the enactment of the Espionage Act. Ross, Gary, *Who Watches the Watchmen?* 17 (NI Press, 2011, Washington, D.C.). The ODNI announced on June 25, 2012, that it will assign an inspector general to follow up on leak cases that the FBI and the DOJ are unable to prosecute. It is unclear what investigative tools an inspector general will employ that are not available to the FBI. *See* Jack Goldsmith, *DNI Clapper Announces New Steps to Deter Leaks*, Lawfare Blog (June 25, 2012), www.lawfareblog.com/2012/06/dni-clapper-announces-new-steps-to-deter-leaks/.

[18]*See* Charlie Savage, *Former F.B.I. Agent to Plead Guilty in Press Leak*, The New York Times, A1, Sept. 23, 2013, *available at* www.nytimes.com/2013/09/24/us/fbi-ex-agent-pleads-guilty-in-leak-to-ap.html?_r=0; Evan Perez and Brent Kendall, *Holder Defends AP Phone-Records Seizure*, Wall Street Journal, May 14, 2013, online.wsj.com/news/articles/SB10001424127887324216004578483292722253924.

[19]Reporters and publishers complain vociferously when their privacy and confidential communications are invaded. *See International News Service v. Associated Press*, 248 U.S. 215 (1918) (seeking remedy under federal common law for piracy of news stories); *Reporters Committee for Freedom of the Press v. AT&T*, 593 F.2d 1030 (D.C. Cir. 1978), *cert denied* 99 S. Ct. 1431 (1979) (unsuccessful privacy suit against telephone carrier for releasing calling records to government).

[20]28 C.F.R. § 50.10 (2011). The further revised guidelines were released in January 2015 and are available at www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/01/14/revised_media_guidelines_0.pdf.

[21]*See, e.g., Int'l News Serv. v. Associated Press*, 248 U.S. 215 (1918) (seeking remedy under federal common law for piracy of news stories); *Viacom Int'l Inc. v. YouTube Inc.,* 676 F.3d 19 (2d Cir. 2012) (dispute over control of intellectual property on Internet); *Entm't Software Ass'n v. Swanson, Attorney General,* 519 F.3d 768 (8th Cir. 2008) (constitutional challenge to restrictions on videos); *Associated Press v. Meltwater U.S. Holdings Inc.*, 931 F. Supp. 2d 537, 551 (S.D.N.Y. 2013) (finding media monitoring service's use of Associated Press articles and headlines violated Copyright Act); *Sony Music Entm't Inc. v. Does 1-40*, 326 F. Supp. 2d 556 (S.D. N.Y. 2004) (successful use of Doe subpoena in Copyright Act case*)*. News organizations have long insisted on their own right to create, protect, and maintain exclusive control over information and have aggressively used federal laws to protect those rights and the right to determine who, when, and how information will be shared. For example, many wealthy media interests have used the Copyright Act to enforce the exclusive right to access and make copies of items of information. *See, e.g., Harper & Row Publishers Inc. v. Nation Enters.*, 471 U.S. 539, 558 (1985) (deciding whether publication of excerpts from presidential autobiography was fair use or violation of exclusive right to license publication); *In re Literary Works in Elec. Databases Copyright Litig.*, 654 F.3d 242 (2d Cir. 2011) (copyright dispute involving dozens of media companies); *Columbia Pictures Indus. v. Krypton Broad. of Birmingham Inc.,*259 F.3d 1186 (9th Cir. 2001), *cert denied* 534 U.S. 1127 (2002) (affirming verdict of $ 31,680,000 for infringement of exclusive copyright); *Nat'l Broad. Co. v. Satellite Broad. Networks*, 940 F.2d 1467 (11th Cir. 1991) (determining exclusive copyright in television broadcasts by satellite signals); *Cable News Network LP v. GOSMS.com Inc.*

et al, 2000 U.S. Dist. LEXIS 16156 (S.D.N.Y. 2000) (Copyright Act suit by group of large media interests); *L. A. Times v. Free Republic*, 2000 U.S. Dist. LEXIS 5669, 54 U.S.P.Q.2D (BNA) 1453 (C.D. Cal. 2000) (Copyright Act enforcement suit to prevent violation of exclusive right to control text created by plaintiffs). Contracts and common law rights protecting competitively sensitive information are also the subjects of federal civil litigation when a media organization sees fit. *See, e.g., Video Pipeline Inc. v. Buena Vista Home Entm't Inc.,* 342 F.3d 191 (3d Cir. 2003) (deciding issue of copyright control over movie trailer); *Sunshine Media Grp. Inc. v. Goldberg,* 2010 U.S. Dist. LEXIS 74181(D.N.J. 2010) (granting injunction to protect publisher's business interests); *Globe Int'l Inc. v. Nat'l Enquirer*, 1999 U.S. Dist. LEXIS 23346 (C.D. Cal. 1999) (considering injunction against publication of confidential news account); *Inflight Newspapers v. Magazines In-Flight LLC,* 990 F. Supp. 119 (E.D.N.Y. 1997) (granting injunction to protect competitive secrets of newspaper); *Cobb Publ'g Inc. v. Hearst Corp. and Dow Jones & Co.,* 891 F. Supp. 388 (E.D. Mich. 1995*)* (breach of contract and copyright suit); *Woodbury Daily Times Co. v. L. A. Times-Washington Post News Service,* 616 F. Supp. 502 (D.N.J. 1985) (exclusive subscription dispute between publishers). Other federal statutes and rules are frequently relied on to determine who has exclusive control over information and signals. *See, e.g., CBS Broad. Inc. v. Echostar Commc'ns Corp.,* 532 F.3d 1294 (11th Cir. 2008) (suit to determine rights to satellite transponder signal); *Helferich Patent Licensing LLC v. The New York Times Co.*, 2012 U.S. Dist. LEXIS 64789 (N.D. Ill. 2012) (patent dispute involving various media companies).

[22]*See, e.g., Carpenter v. United States*, 484 U.S. 19 (1987) (affirming journalist's conviction for mail fraud based on his use of newspaper's confidential information to conduct insider trading); *Scranton Gillette Commc'ns Inc. v. Dannhausen*, 1999 WL 558134 (N.D. Ill. July 27, 1999) (upholding jury's finding that magazine employee breached fiduciary duty by removing or destroying the magazine's contact list and files of information); *Inflight Newspapers,* 990 F. Supp. at 119 (granting injunction to protect competitive secrets of newspaper).

[23]*Inflight Newspapers,* 990 F. Supp. at 131.

[24]*See supra* n. 20.

[25]*Associated Press*, 931 F. Supp.2d at 546.

[26]*Id*. at 561, 572.

[27]A First Amendment defense was raised in *Harper & Row Publishers Inc. v. Nation Enterprises*, 471 U.S. 539, 560 (1985) (refusing to allow First Amendment defense to copyright violation of publishing lengthy quotations from a yet unpublished presidential memoir).

28*In re Charter Commc'ns*, 393 F.3d 771, 776-778 (8th Cir. 2005) (denying John Doe subpoena enforcement); *Recording Indus. Ass'n of America v. Verizon*, 351 F.3d 1229, 1233-1236 (D.C. Cir. 2003), *cert denied* 543 U.S. 924 (2004) (upholding subpoena enforcement); *John Wiley & Sons Inc. v. Does 1-127*, 2012 WL 364048, 11 CIV 7627 (S.D.N.Y. 2012); *Next Phase Distribution Inc. v. Does 1-138*, 2012 U.S. Dist. LEXIS 27260 (S.D.N.Y. 2012); *Nu Image Inc. v. Does 1-3,932*, 2012 U.S. Dist. LEXIS 72432 (M.D. Fla. 2012); *VPR Internationale v. Does 1-1017*, 2011 US Dist. LEXIS 64656 (C.D. Ill 2011) (Copyright Act); *Millennium TGA Inc. v. Does 1-800*, 2011 US Dist. LEXIS 35406 (N.D. Ill. 2011); *Call of the Wild Movie LLC v. Does 1-1062*, 770 F. Supp. 2d 332 (D.D.C. 2011) (Copyright Act case); *Donkeyball Movie LLC v Does 1-171*, 2011 WL 1807452 (DDC 2011) (Copyright Act)*; USA Techs. Inc. v. Doe,* 713 F. Supp. 2d 901 (N.D. Cal. 2010); *Maverick Entm't Grp. Inc. v. Does 1-4,350,* No. 1:10-cv-00569 (D.D.C. 2010) (use of subpoena power in Copyright Act infringement case); *Subpoena to Univ. of N.C.,* 367 F. Supp. 2d 945, 950-956 (M.D.N.C. 2005) (upholding subpoena); *Sony Music Entm't Inc. v. Does 1-40*, 326 F. Supp. 2d 556 (S.D. N.Y. 2004) (successful use of Doe subpoena in Copyright Act case); *Malibu Media LLC v. Doe*, 2014 WL 25195 (D.D.C. 2014) (allowing third-party subpoena in Copyright Act case); *TCYK LLC v. Does 1-98*, 2013 WL 6834637 (E.D. Tenn. 2013) (Media copyright suit against unknown defendants); *Purzel Video GmbH v. Does 1-108*, 2013 WL 6797364 (N.D. Ill. 2013) (same); *Voltage Pictures LLC v. Doe*, 2013 WL 6827927 (D. OR 2013) (same); *Safety Point Products LLC v. Does*, 2013 WL 1367078 (N.D. Ohio 2013) (same).

[29]*USA Techs. v. John Doe*, 713 F. Supp. 2d 901 (N.D. Cal. 2010).

30*Qixtar Inc. v. Signature Team Mgt. LLC*, 566 F. Supp. 2d 1205, 1206 (D. Nev. 2008) (Lanham Act) *reversed*, *Anonymous Online Speakers v. United States Dist. Court (In re Anonymous Online Speakers*), *rev'd* 661 F.3d 1168 (9th Cir. 2011).

[31]*Alvis Coatings Inc. v. John Does 1-10*, 2004 U.S. Dist. LEXIS 30099, 2004 WL 2904405 (W.D. N.C. 2004) (defamation, etc.).

[32]*Doe I et al. v. Individuals Unknown (Autoadmit.com),* 561 F. Supp. 2d 249, 252 (D. Conn. 2008) (libel, invasion of privacy, emotional distress, copyright); *Best Western Int'l v. Doe,* 2006 US Dist. LEXIS 56014 (D. Ariz. 2006) (defamation, breach of contract, breach of fiduciary duty, trademark infringement, unfair competition).

[33]See the following articles for descriptions of the use of John Doe suits by private sector parties. Robert Larson and Paul Godfread, *Contemporary Issues in Cyberlaw: Bringing John Doe to Court, etc*., 38 Wm. Mitchell L. Rev. 328 (2011); Matthew Mazzota, Note, *Balancing Act: Finding Consensus on Standards for Unmasking Anonymous Internet Speakers*, 51 B.C. L. Rev. 833 (2010); Jessica L. Chilson, Note, *Unmasking John Doe: Setting a Standard for Discovery in Anonymous Internet Defamation Cases,* 95 Va. L. Rev. 389 (2009); Nathaniel Gleicher, Note, *John Doe Subpoenas, Toward a Consistent Standard*, 118 Yale L.J. 320 (2008); Carol M. Rice, *Meet John Doe: It is Time for Federal Civil Procedure to Recognize John Doe Parties,* 57 U. Pitt. L. Rev. 883 (1996).

[34]*See, e.g., John Doe Agency v. John Doe Corp*., 493 U.S. 146, 148 n.1 (1989), *reh'g denied* 493 U.S. 1064 (approving use of pseudonyms by parties in confidential FOIA case); *Tenet v. Doe,* 544 U.S. 1, 10 n.5 (2005) (use of pseudonym approved to prevent disclosure of name of CIA employee); *Doe v. Casey*, 796 F.2d 1508, 1512 n.2 (D.C. Cir. 1986), *rev'd in part* 486 U.S. 592 (use of Doe name to protect CIA employee identity); *In the Matter of Tax Liabilities of John Does*, No 2:10-mc-00130 (E.D. Cal. December 15, 2011) (Mem. Opinion granting ex parte discovery order under specific statutory authority for ex parte discovery by IRS); *United States v. John Doe*,

No. 3:11-CV-00561-VLB (D. Conn 2011) (civil complaint seeking order permitting the government to take over control of a Botnet). *See also Doe v. Doe Corporation*, 709 F.2d 1043, 1044 n. 1 (5th Cir. 1983) (approving use of pseudonyms for both parties in suit by in-house counsel to prevent disclosure of confidential communications and facts, and other measures). The U.S. Attorneys' Manual published by DOJ deals with John Doe subpoenas in the Tax Manual. *See United States Attorneys' Manual*, Section 6-5.240, U.S. Department of Justice (1997), *available at* www.justice.gov/usao/eousa/foia_reading_room/usam/title6/5mtax.htm (last visited Jan. 17, 2014). The SEC has also issued John Doe subpoenas when conducting investigations under its statutory authorities. *See, e.g., John Doe v. United States S.E.C.,* 2011 U.S. Dist. LEXIS 133005 (N.D. Cal. 2011) (denying motion to quash John Doe administrative subpoena issued to Google during investigation of suspected securities law violation). In July 2014, a high-ranking DOJ official testified before the Senate Judiciary Committee regarding the creative, combined use of criminal and civil litigation options to combat international cybercrime. www.judiciary.senate.gov/imo/media/doc/07-15-14CaldwellTestimony.pdf.

[35]*United States v. Ishmael Jones, a pen name*, No. 10-cv-765 (E.D. Va. Mem. Op. and Order April 18, 2012).

[36]n. 21, *supra*.

[37]Multiple sources of federal substantive law create a duty of confidentiality for federal employees entrusted with confidential information. These include federal common law, *Snepp v. United States*, 444 U.S. 507, 515 (1980); *See United States v. Aguilar*, 515 U.S. 593, 605-606 (1995) (a federal judge, who obtained information about an investigative wiretap from another judge, violated federal statutory law when he leaked information about a wiretap order); *Haig v. Agee,* 453 U.S. 280, 309 (1981) (concluding that publication of intelligence identities is constitutionally unprotected); Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009). Executive Order 13526; written contracts; and numerous statutes ; 5 U.S.C. § 301 (housekeeping statute); 18 U.S.C. § 641 (theft of government property in the form of documents); 42 U.S.C. § 2277 (criminal penalties for release of restricted data); 50 U.S.C. § 3121 (covert agent identities protection) 50 U.S.C. § 783 (criminal penalties for government employees who disclose classified information to foreign governments). 5 U.S.C. § 301. Every federal agency has regulations that implement the record-keeping and record release obligations of federal employees. *See, e.g.,* 28 C.F.R. § 16.22 (2010) (DOJ regulations prohibit employees from complying with subpoenas in proceedings in which the government is not a party without the approval of designated department officials).

[38]*Snepp, supra*, 444 U.S. at 515.

[39]*Snepp, supra*, 444 U.S. at 514-515; *United States v. Snepp,* 595 F.2d 926, 934-935 (4th Cir. 1979), *rev'd, in part on other grounds,* 444 U.S. 507 (1980).

[40]*Pfeiffer v. CIA and United States*, 1994 US Dist. LEXIS 2650 **22-23 (D.D.C. 1994), *aff'd* 60 F.3d 861 (D.C. Cir. 1995).

[41]The government need only prove nominal damages to be entitled to punitive damages in a case requiring enforcement of a secrecy agreement. *United States v Snepp,* 595 F.2d at 936-938.

[42]The government is entitled to recover out-of-pocket costs as measured by traditional measures of breach of contract damages in a case where an intelligence officer breaches his pledge of secrecy. In *Snepp,* the Supreme Court said that such a remedy is available but inadequate to remedy the breach because the damages may be unquantifiable. *Snepp, supra,* 444 U.S at 514.

[43]Bruce and Jameson, *Fixing Leaks*, *supra* n. 4 at 17, 40.

[44]*United States v. Kordel*, 397 U.S. 1, 9 (1970).

[45]*See Answers to Questions from Senate Judiciary Committee*, U.S. Department of Justice, April 8, 2010, www.fas.org/irp/agency/doj/intel-leak.pdf.

[46]*See United States v. Stringer*, 535 F.3d 929, 939-40 (9th Cir.), *cert denied*, 555 U.S. 1049 (2008) (finding SEC did not act in bad faith because it did not share information with U.S. Attorney until the civil proceeding was well underway and did not involve "trickery or deceit" because an SEC form indicated that civil investigations could lead to criminal charges); *United States v. Posada Carriles*, 541 F.3d 344, 356 (5th Cir. 2008), *cert denied*, 556 U.S. 1130 (2009) (finding USCIS did not make material misrepresentations at naturalization interview when defendant was informed he could exercise right against self-incrimination and lying could lead to criminal penalties); *Securities and Exchange Commission v. Dresser Industries Inc.*, 628 F.2d 1368, 1377 (D.C. Cir.), *cert denied*, 449 U.S. 993 (1980) (refusing to block parallel criminal and civil investigations by DOJ and SEC absent a showing of prejudice to substantial rights of defendant or government).

[47]*See United States Attorneys' Manual*, Section 1-12.000, U.S. Department of Justice (1997), *available at* www.justice.gov/usao/eousa/foia_reading_room/usam/title1/12mdoj.htm. Given that DOJ policies allow for maximum use of evidence within criminal, civil, and administrative proceedings, information obtained during a civil Doe suit could also be used in administrative proceedings revoking an individual's security clearance and/or terminating his employment with the DOD. *Id.* The challenges raised in Kordel would not apply when evidence obtained in a civil suit is used in an administrative proceeding because the privilege against self-incrimination only applies to criminal prosecutions and the employee would still receive the benefit of due process protection during the civil and administrative proceedings. *Kordel, 397 U.S. at 9-13.*

[48]*Memorandum on Coordination of Parallel Criminal, Civil, Regulatory, and Administrative Proceedings*, Attorney General, Jan. 30, 2012, *available at* www.justice.gov/usao/eousa/foia_reading_room/usam/title1/doj00027.htm.

[49]28 C.F.R. § 50.10(f) provides: In requesting the attorney general's authorization for a subpoena to a member of the news media, the following principles will apply:

(1) In criminal cases there should be reasonable grounds to believe, based on information obtained from nonmedia sources, that a crime has occurred and that the information sought is essential to a successful investigation, particularly with reference to directly establishing guilt or innocence. The subpoena should not be used to obtain peripheral, nonessential, or speculative information. (2) In civil cases there should be reasonable grounds, based on nonmedia sources, to believe that the information sought is essential to the successful completion of the litigation in a case of substantial importance. The subpoena should not be used to obtain peripheral, nonessential, or speculative information. (3) The government should have unsuccessfully attempted to obtain the information from alternative nonmedia sources. (4) The use of subpoenas to members of the news media should,

except under exigent circumstances, be limited to the verification of published information and to such surrounding circumstances as relate to the accuracy of the published information. (5) Even subpoena authorization requests for publicly disclosed information should be treated with care to avoid claims of harassment. (6) Subpoenas should, wherever possible, be directed at material information regarding a limited subject matter, should cover a reasonably limited period of time, and should avoid requiring production of a large volume of unpublished material. They should give reasonable and timely notice of the demand for documents.

The US Attorney's Manual primarily deals with 28 C.F.R. § 50.10 in the Criminal Section of the Manual. *See United States Attorneys' Manual*, Section 9-13.400, U.S. Department of Justice (1997), *available at* www.justice.gov/usao/eousa/foia_reading_room/usam/title9/13mcrm.htm#9-13.400 (describing how Criminal Division of DOJ requests media subpoenas).

[50]*Department of Justice Report on Review of New Media Policies*, U.S. Department of Justice, July 12, 2013, www.justice.gov/iso/opa/resources/2202013712162851796893.pdf. This requirement is further reinforced by a January 2015 tightening of the policy. *See www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/01/14/revised_media_guidelines_0.pdf.*

[51]*Id*.

[52]*Id*.

[53]*Id*.

[54]*Id*. It should be noted that as of the writing of this note, DOJ policies including 28 C.F.R. § 50.10(f) have not been formally amended to reflect the DOJ's new stated policy on seeking information and evidence from news media.

[55]*Bartnicki v. Vopper*, 532 U.S. 514 (2001). On the issue of exhaustion of sources, the lack of a civil or criminal legal remedy against the publishers of government confidences may strongly suggest that the government has no choice but to go after the original source of the leaks. In other words, the publisher who aids and abets a leak is protected, so the source of the leak is the only person who may be deterred.

The media may not be prevented from publishing truthful information even when the information is leaked to the media in a knowing breach of trust. *Butterworth v. Smith*, 494 U.S. 624, 629-35 (1990) (grand jury evidence); *Landmark Commc'ns v. Virginia,* 435 U.S. 829, 842 (1979) (publication of confidential document from state proceeding); *Oklahoma Publ'g v. District Court*, 430 U.S. 308, 311-12 (1977) (publication of identity of juvenile defendant from closed hearing). *See Reuber v. Food Chemical News Inc.,* 925 F.2d 703, 719 (4th Cir.), *cert denied* 501 U.S. 1212 (1991) (there can be no liability for intrusion where the media defendant "played no role in leaking the letter" that formed the basis of its story and which had been provided by a source "in violation of government policy."); *Sheetz v. Morning Call Inc.,* 747 F. Supp. 1515, 1526 (E.D. Pa. 1990), *aff'd* 946 F.2d 202 (3d Cir. 1991) (rejecting claim that press unlawfully received confidential police report through a conspiracy with unnamed police sources).

[56]*Department of Justice Report on Review of News Media*, *supra* n. 52.

[57]The reporters were Vanessa Legget, Judith Miller, and Joshua Wolf . Ross, Gary, *Who Watches the Watchmen?* 160-161 (NI Press, 2011, Washington, D.C.).

[58]*In re Seper*, 705 F.2d 1499, 1501 (9th Cir. 1983) (citing *Manness v. Meyers*, 419 U.S. 449, 464 (1975).

[59]*Lee v. DOJ*, 413 F.3d 53 (D.C. Cir. 2005) (rejecting claim of reporter's privilege in civil leak case); *Lee v. DOJ*, 401 F. Supp. 2d 123 D.D.C. 2005) (holding reporter in contempt for refusing to answer deposition questions in civil leak case); *see also Convertino v. United States DOJ*, 2008 U.S. Dist. LEXIS 66889 (E.D. Mich. 2008) (considering motion to compel reporter to testify in civil leak case); *Hatfill v. Mukasey*, 539 F. Supp. 2d 96 (D.D.C. 2008); *Hatfill v. Gonzales*, 505 F. Supp. 2d 33, 35-36 (D.D.C. 2007); *Hatfill v. Ashcroft*, 404 F.Supp.2d 104, 106-108 (D.D.C. 2005) (Dr. Steven Hatfill, a former government scientist, was publicly described as a "person of interest" in the investigation of the 2001 anthrax attacks. He sued DOJ and sought to enforce subpoenas for the sources of the defamatory comments. When the reporter refused to reveal the identity of her government sources, she was found to be in contempt and fines escalating to $ 5,000 per day were imposed upon her.).

[60]*See, e.g., Zemel v. Rusk*, 381 U.S. 1, 16-17 (1965) (the right to publish does not carry with it an unrestrained right to gather information).

[61]*Burdick v. United States*, 236 U.S. 79, 94 (1915) (under the Fifth Amendment, government may not use pardon granted by president and contempt to force editor of newspaper to identify confidential sources to criminal grand jury if editor did not accept pardon); *but see Kastigar v. United States*, 406 U.S. 441, 462 (1972) (holding grant of derivative or derivative use immunity under 18 U.S.C. § 6002 is sufficient to supplant Fifth Amendment right against self-incrimination).

[62]*Hatfill v. New York Times Co*., 459 F. Supp. 2d 462, 468 (E.D. Va. 2006) (ordering news corporation under Rule 30(b)(6) to provide representative who knows identity of confidential sources).

[63]*Convertino v. United States DOJ*, 684 F.3d 93, 101 (D.C. Cir. 2012); s*ee also Convertino v. United States DOJ*, 2013 WL 153311 (E.D. Mich. 2013) (requiring the *Detroit Free Press* to prepare a corporate representative to testify despite reporter invoking Fifth Amendment right against self-incrimination); *United States v. White*, 322 U.S. 694, 698 (1944) ("The constitutional privilege against self-incrimination is essentially a personal one, applying only to natural individuals."); *In re Grand Jury Proceedings*, 576 F.2d 703, 705 (6th Cir. 1978), *cert. denied in Shiffman v. United States*, 439 U.S. 830 (1978) ("Since the privilege against self-incrimination is a purely personal one, it cannot be utilized by or on behalf of any organization, such as a corporation."); *Eller Media Co. v. Serrano*, 761 So.2d 464, 466-467 (Fla. Dist. Ct. App. 2000) (denying motion for stay of discovery and finding "Eller Media, as a corporation, has no Fifth Amendment right, and it cannot vicariously assert that right on behalf of its employees …"). *But see Convertino v. United States DOJ*, 2008 U.S. Dist. LEXIS 66889 (E.D. Mich. 2008) (denying motion to compel corporate publisher deposition without prejudice while plaintiff seeks other discovery); *Volmar Distrib. Co. v. New York Post Co.,* 152 F.R.D. 36 (S.D. N. Y. 1993) (court has discretion to stay corporate 30(b)(6) depositions in civil case when crucial individual witnesses invoke Fifth Amendment privilege).

[64]*Convertino v. United States DOJ*, 2013 WL 153311 (E.D. Mich. 2013).

[65]*Id*.

[66]The recipient of a subpoena sought by the government may make an allegation that the government has a motive to suppress

protected speech. See Elena Kagan, *Private Speech, Public Purpose: The Role of Governmental Motive in First Amendment Doctrine,* 63 U. Chi. L. Rev. 413, 414, 425-426 (1996) (First Amendment doctrine in general can be understood as the courts' search for impermissible government motive in regulating speech).

[67]*See Reporters Committee for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1059 (D.C. Cir. 1981), *cert. denied* 440 U.S. 949 (1979) (rejecting claim under First and Fourth amendments that federal government may not subpoena business records relating to journalist activities).

[68]In one recent case, the court received more than 30 *amicus* filings from such groups.

[69]*Lee v. DOJ*, 413 F.3d 53 (D.C. Cir. 2005) (rejecting claim of reporter's privilege in civil leak case where reporter is not a party); *Zerilli v. Smith*, 656 F.2d 705, 715 (D.C. Cir. 1981) (declining to order testimony under reporter's "privilege" to decline to answer questions about a source in a civil deposition where the reporter is not a party; ruling depended on weighing of three factors, including how central the reporter's information is to the plaintiff's case); *Lee v. DOJ*, 401 F. Supp. 2d 123(D.D.C. 2005) (holding reporter in contempt for refusing to answer deposition questions in civil leak case).

[70]*Doe v. Omaha World Herald*, No. 4:04CV3306 (D. Neb. Sept. 20, 2004) (motion by the ACLU of Nebraska asking a court to enjoin a newspaper from revealing the name of a John Doe plaintiff in a case challenging the posting of the Ten Commandments, because the plaintiff had received death threats); *Doe v. Omaha World Herald*, No. 4:04CV3306 (D. Neb. Sept. 21, 2004) (Order denying the motion).

[71]*See, e.g., Associated Press v. Meltwater U.S. Holdings Inc.*, 931 F. Supp. 2d 537, 546 (S.D.N.Y. 2013) (discovery not contested on First Amendment or journalistic privilege grounds).

[72]*See Harper & Row Publishers Inc. v. Nation Enterprises*, 471 U.S. 539, 560 (1985) (refusing to allow First Amendment defense to copyright violation of publishing lengthy quotations from a yet unpublished presidential memoir).

[73]*United States v. Golden Valley Elec. Ass'n*, 689 F.3d 1108, 1115 (9th Cir. 2012) (upholding administrative John Doe subpoena against Fourth amendment challenge).

[74]Government issuance of civil subpoenas seeking information regarding anonymous individuals may raise First Amendment concerns. For example, in *NAACP v. Alabama ex rel. Patterson,* 357 U.S. 449, 462 (1958), the Supreme Court held that a discovery order requiring the NAACP to disclose its membership list interfered with the First Amendment freedom of assembly. Similarly, in *NLRB v. Midland Daily News,* 151 F.3d 472, 475 (6th Cir. 1998), the Sixth Circuit declined on First Amendment grounds to enforce a subpoena *duces tecum* issued by the National Labor Relations Board seeking to require a newspaper publisher to disclose the identity of an anonymous advertiser. *See also Los Angeles Memorial Coliseum Comm. v. Nat'l Football League,* 89 F.R.D. 489, 494-95 (C.D. Cal. 1981) (granting motion to quash civil subpoena seeking disclosure of confidential journalistic sources).

[75]*Branzburg v. Hayes*, 408 U.S. 665 (1972). *See McKevitt v. Pallasch,* 339 F.3d 530, 533 (7th Cir. 2003) (collecting cases). The Fourth Circuit has adopted a three-part test to determine when a reporter has a privilege to refuse to testify in a case where the reporter is not a party. *Ashcraft v. Conoco Inc.*, 218 F.3d 282, 287 (4th Cir. 2000). The test is "(1) whether the information is relevant, (2) whether the information can be obtained by alternative means, and (3) whether there is a compelling interest in the information." (citing *LaRouche v. National Broadcasting Company*, 780 F.2d 1134 (4th Cir.), *cert denied* 479 U.S. 818 (1986)).

[76]*New York Times Co. v. Gonzalez*, 459 F.3d 160, 170-171 (2d Cir.), *stay denied*, 549 U.S. 1049 (2006) (upholding grand jury subpoenas for reporter telephone records in criminal leak investigation); *CFTC v. Whitney*, 441 F. Supp. 2d 61, 65 (D.D.C. 2006) (holding that a reporter privilege does not overcome the public interest in a CFTC enforcement action that concerns information provided by a regulated entity to the publisher).

[77]*In re Special Proceedings*, 373 F.3d 37 (1st Cir. 2004) (enforcing grand jury subpoena by contempt power against reporter where the evidence was central to the investigation); *Doe v. Kohn, Nast & Graf, P.C.*, 853 F. Supp 150 (E. D. Pa. 1994) (denying production of TV interview outtakes after *in camera* review); *CFTC v. Whitney*, 441 F. Supp. 2d 61, 65 (D.D.C. 2006) (holding that a qualified reporter privilege does not overcome the government's need for discovery when the government proves that the discovery is central to proof of essential elements of its case, other sources have been exhausted, and the publisher received the information for use in its publication).

[78]*See, e.g., Herbert v. Lando*, 441 U.S. 153, 170 (1979) (editorial processes and news methods are not privileged from discovery when malice of publisher is at issue); *Desai v. Hersh*, 954 F.2d 1408, 1412 (7th Cir.), *cert denied* 506 U.S.865 (1992) (reporter does not have absolute privilege to withhold identity of sources in libel case based on leaked intelligence information); *LaRouche v. Nat'l Broad. Co. Inc.,* 780 F.2d 1134, 1139 (4th Cir. 1986) (NBC not required to reveal anonymous sources when plaintiff failed to exhaust other avenues); *In re Selcraig,* 705 F.2d 789 (5th Cir. 1983) (reversing contempt finding for reporter as premature when merits of defamation claim not yet demonstrated); *Zerilli v. Smith,* 656 F.2d 705, 710-11 (D.C. Cir. 1981) (declining to order journalist testimony despite essential nature of testimony); *Bruno & Stillman Inc. v. Globe Newspaper Co.,* 633 F.2d 583, 595-99 (1st Cir. 1980) (variety of factors must be considered before compelling disclosure of confidential sources under Rule 26); *Miller v. Transamerican Press Inc.,* 621 F.2d 721, 725 (5th Cir. 1980), *cert denied* 450 U.S. 1041 (1981) (affirming order to disclose journalistic source); *Riley v. City of Chester,* 612 F.2d 708, 715 (3d Cir. 1979) (reversing order compelling disclosure because party failed to exhaust other sources first); *Silkwood v. Kerr-McGee Corp.*, 563 F.2d 433, 438 (10th Cir. 1977) (reversing trial court disclosure order on ground of failure to require exhaustion of other sources); *Farr v. Pitchess,* 522 F.2d 464, 467-68 (9th Cir. 1975), *cert. denied* 427 U.S. 912 (1976) (denying habeas corpus relief to reporter jailed for declining to reveal sources of information about witness in criminal trial); *Baker v. F & F Inv.*, 470 F.2d 778, 779-80 (2d Cir. 1972), *cert denied* 411 U.S. 996 (1973) (civil suit over race discrimination in housing does not present compelling need for overriding claim of journalistic privilege); *Cervantes v. Time Inc.,* 464 F.2d 986, 992-93 (8th Cir. 1972), *cert. denied* 409 U.S. 1125 (1973) (denying order to reveal news sources when case on merits is extraordinarily weak); *Carey v. Hume*, 492 F.2d 631 (D.C. Cir.) *petition for writ of certiorari dismissed pursuant to Rule 60*, 417 U.S. 938 (1974) (ordering disclosure of reporter sources when central to the case.).