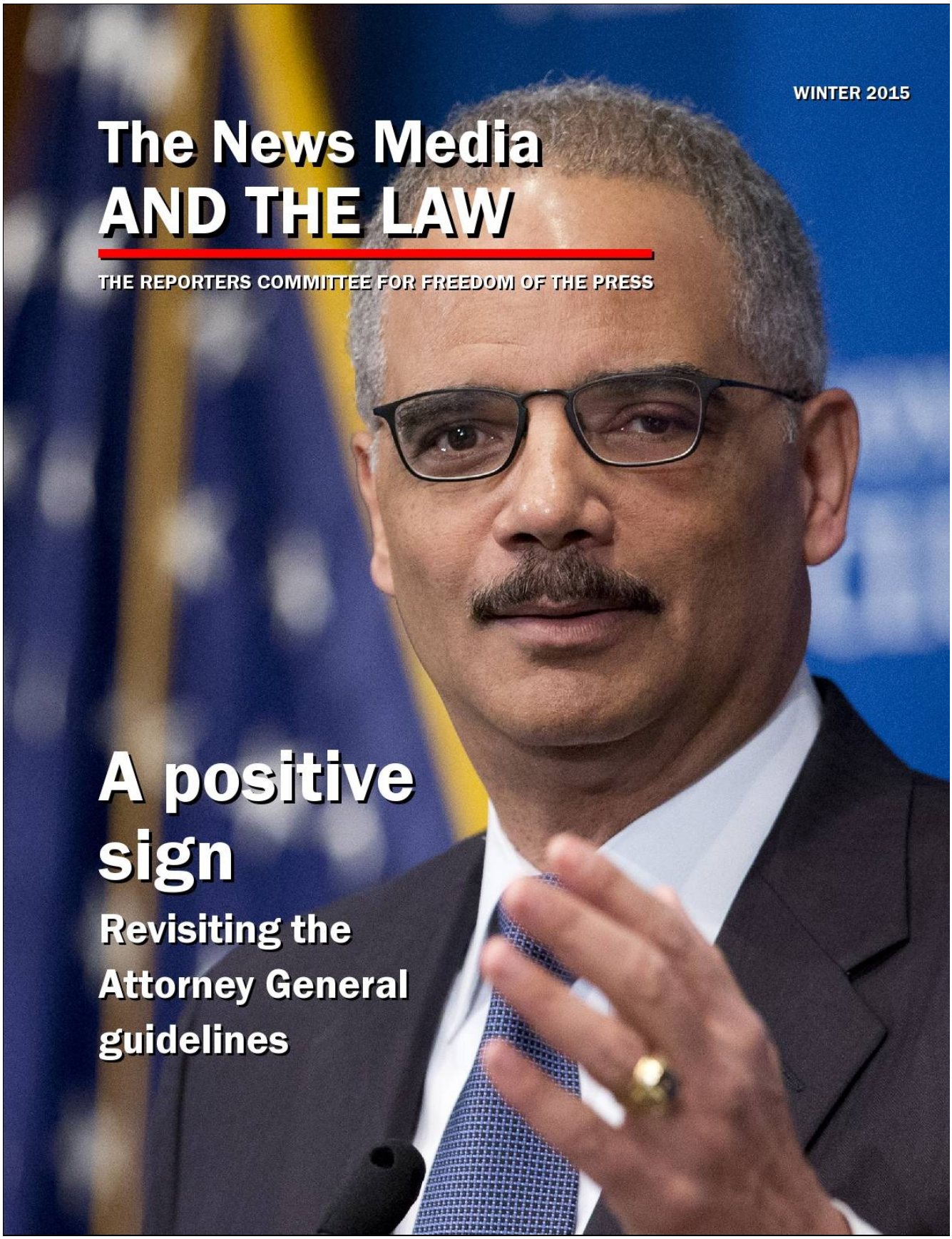

WINTER 2015

The News Media AND THE LAW

THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS

A positive sign

Revisiting the Attorney General guidelines

The News Media & The Law

Winter 2015

CONTENTS

Published by
The Reporters Committee for Freedom of the Press
Editor Bruce D. Brown
Editor Gregg P. Leslie
Contributors Kristin Bergman, Hannah Bloch-Wehba, Kimberly Chow, Tom Isler, Adam Marshall, Amelia Rufer, Katie Townsend
Administration Lois Lloyd, Michele McMahon

Price: $20/year. Address correspondence to:
The News Media and The Law, 1101 Wilson Blvd.,
Suite 1100, Arlington, VA 22209
Telephone: (703) 807-2100
E-mail: magazine@rcfp.org
ISSN: 0149-0737

Tracking FOIA Projects

Need help tracking your FOIA requests? Be sure to use the Reporters Committee's iFOIA service, a free system that handles FOIA requests by email and keeps everything organized for you.

To learn more, view our tutorial or go straight to iFOIA.org.

Revising the Attorney General's guidelines

Dialog with reporters leads to further changes on federal regulations on subpoenaing reporters

By Kimberly Chow

A year after the Department of Justice began a dialogue with representatives of the news media, it issued a second set of revisions to its internal guidelines for media subpoenas.

While the Obama administration has been criticized for actions including targeting the phone records of journalists and labeling one journalist a co-conspirator in violations of the Espionage Act, the Department's decision to work with the media to put better safeguards in place for the future has been a positive sign.

Media lawyers pointed to the revised subpoena guidelines as evidence of Attorney General Eric Holder's willingness to establish a conversation with the media and foster more sensitivity to their concerns within the Department of Justice.

Kurt Wimmer, an attorney at Covington & Burling LLP and a member of the News Media Dialogue Group, which was formed in February 2014 and has been meeting regularly with Holder and other department representatives, called the revisions "a real step forward," and said he hopes that this dialogue continues.

"The Department was quite open and productive in listening to our concerns and acted on those concerns, and that's pretty extraordinary," Wimmer said.

After the disclosures in May 2013 that the Justice Department had secretly seized Associated Press toll records and the emails of Fox News reporter James Rosen, the Justice Department initiated a review of its internal media subpoena guidelines. The ongoing James Risen subpoena battle intensified the pressure on the government to institute tighter controls on media subpoenas in the future. The guidelines have been around since 1970 and originally applied only to subpoenas served directly to journalists, but were amended in 1980 to include telephone records held by a third party service provider.

In the summer of 2013, Holder invited interested groups to propose changes to the guidelines. A set of revised guidelines were released in February 2014 and included much of what press advocates had sought, including provisions making it

more difficult for DOJ to withhold notice to a journalist or media organization when it subpoenas a third party and forbidding the use of the Privacy Protection Act's "suspect exception" — which allows the government to obtain a search warrant for material belonging to a journalist who is suspected of a crime — when the journalist is engaged in "ordinary newsgathering activities" and is not the target of the criminal probe. But "ordinary newsgathering" was not defined and was an entirely new term.

Members of the media felt that this term and several other aspects of the revised guidelines were unclear, incomplete, or even harmful to the interests they were meant to protect. At roughly the same time, prosecutors began meeting with the News Media Dialogue Group, whose creation the Department had first promised in the summer of 2013, and the group started to discuss with DOJ leadership the possibility of further revisions to the guidelines. Led in part by Reporters Committee executive director Bruce Brown, the dialogue group met with DOJ representatives throughout 2014, and in January 2015, new guidelines were released.

January 2015 guideline revisions

A sampling of the 2015 revisions to the media subpoena guidelines follows.

Members of the press were concerned that the qualifier "ordinary" in "ordinary newsgathering activities" could be used to withhold protection from journalists who were engaged in what the government could subjectively determine was newsgathering it disapproved of, such as receiving leaked information from government officials. That phrase appeared multiple times in the 2014 guidelines, even though it was not in the original regulations and had never come up during the discussion process.

The dialogue group expressed its concerns to DOJ that the vagueness of the term created a large exception where prosecutors and future attorneys general could decide that a wide range of activities that they would find unacceptable would be deemed "extra-ordinary."

DOJ officials said they did not intend for the term to restrict the protections offered in the guidelines, but in the 2015 revisions, the word "ordinary" was removed so that the guidelines refer simply to "newsgathering activities."

The 2014 revisions added sections stating that the Attorney General "may" authorize subpoenas when the Director of National Intelligence certifies that the investigation concerns the unauthorized disclosure of properly classified information. This language was ambiguous as to whether, when such a certification is made, the Attorney General could then ignore the rest of the guidelines' prescriptions.

The 2015 revisions make clear that this is an additional step in leaks investigations and prosecutions. Both the sections on direct subpoenas and on third-

party subpoenas indicate that in approving a subpoena in a leaks investigation, the Attorney General "should take into account" both the DNI certification and the specific restrictions in the guidelines.

Most references to records held by third parties that were protected under the 2014 guidelines referred to communications records and business records, both of which are defined in the regulations. But a few references, particularly with regard to records held by communications service providers and those subject to search warrants, referred only to communications records. Those sections were amended in 2015 to include business records, and the definition of business records was expanded to specifically include "work product and other documentary materials."

The 2014 regulations stated that they did not cover journalists "who are the focus of criminal investigations for conduct not based on, or within the scope of" their newsgathering activities. The media coalition felt that "focus" was ambiguous and was inconsistent with the terms of art used elsewhere in DOJ rules and regulations. The 2015 regulations replaced "focus" with "subjects or targets." A similar change was made in the section regarding when the Privacy Protection Act "suspect exception" is invoked.

A new section was added regarding third-party subpoenas to mirror language regarding direct subpoenas: "Requests should be treated with care to avoid interference with newsgathering activities and to avoid claims of harassment."

A new section was added to require that even after any subpoena or other instrument is issued and negotiations with the media entity fail, prosecutors must consult with the Criminal Division before asking a judge to compel compliance with any direct or third-party subpoena or court order. The initiative for this new section came from DOJ and the media coalition endorsed it.

The 2014 regulations required that the news media be given notice of subpoenas to third parties before they are served, thus giving the media the opportunity to move to quash them. The 2015 revisions added similar language to the Statement of Principles.

In the section regarding requests for approval to question, arrest, or seek indictment of members of the news media, a new sub-section was added stating that the Attorney General must follow the Statement of Principles when considering such requests.

Reaction to the revisions

Much of what reporters can expect to come in the way of subpoenas in the future depends on the decisions of future attorneys general, but the tightened guidelines should operate to better protect media interests. It should be kept in mind that they are merely guidelines and not rules that can be enforced against DOJ. But with the great public scrutiny of subpoenas to the media, there is a measure of public accountability that will apply pressure on the government to follow them.

In addition, many subpoenas to reporters come from sources other than the Department of Justice, including state prosecutors, criminal defendants and civil litigants. The guidelines do not cover those subpoenas.

David McCraw, assistant general counsel of *The New York Times*, said that while the guidelines are not perfect, they are an important speed bump for federal prosecutors who will now have to think very hard about issuing subpoenas to reporters. A sobering example came from the Jeffrey Sterling case, in which DOJ pursued the testimony of journalist James Risen and got a victory in the Fourth Circuit denying the existence of a federal reporter's privilege. In the end, the government convicted Sterling under the Espionage Act without Risen's testimony. The revised guidelines will restrain federal prosecutors somewhat in those kinds of cases in the future, he said.

"In many ways the system has depended on the discretion of prosecutors to decide not to subpoena reporters," McCraw said. "If the law is uncertain as I think it now is after Sterling, we need, in order to protect sources, government prosecutors who will not take up a press subpoena lightly, who will not force the press to reveal sources in cases when it doesn't matter, when there is no need."

Susan Page, a member of the dialogue group and the Washington bureau chief for USA Today, said she appreciated that DOJ was willing to at least discuss all of the group's concerns and that their revisions addressed the most important points.

"Not that it's a perfect world and that there won't be confrontations down the line, but government agencies are not always willing to listen, to compromise, and to change what they're doing," Page said. "In this case the Administration was, and I think they deserve some credit for that."

DOJ spokesperson Brian Fallon was not available for comment.

Wimmer remains positive about Holder's engagement with the press and the example it sets for the department's future communications with the media, saying that Holder has "tried hard to do the right thing" by being open to concerns about issues such as the administration's use of the press to investigate leakers.

"I hope that is something that continues with future A.G.s, who have the ability to meet with the media group and continue the process of having an open dialogue," Wimmer said.

The failures of the information security infrastructure

Summit considers questions of data encryption and protection for journalists

By Jenn Henrichson

In an age of big data and mass state surveillance, the rapid expansion of interconnected networks without secure infrastructure is causing concern among many information security experts, lawyers, privacy advocates, and journalists.

To address these challenges and others, information security experts, policymakers, journalists, activists, and military officials convened at the New America Foundation's inaugural cybersecurity summit in Washington, D.C. on February 23. Amidst the diverse set of topics and speakers, several key takeaways and themes emerged, many of which have implications for the media.

Weakened encryption was once again debated. In line with recent statements made by government and law enforcement officials, NSA Director Adm. Mike Rogers defended the stance to weaken encryption products to allow for information gathering by the U.S. government. Rogers said he thought it would be possible for encryption programs to have an entry point, within a legal framework approved by Congress or some civilian body, that could be accessed by the NSA. This position was received with skepticism by many privacy advocates and information security experts who oppose weakening encryption because it makes products, services, and networks more vulnerable to exploitation by others, violates private communications, and limits freedom of expression. According to Chief Information Security Officer at Yahoo, Alex Stamos, there is no good way to build products that are safe against some actors and not others. "It's like the government asked us to drill a hole in a windshield and say, no you can only let the US government through that hole. Everyone knows that if you drill a hole in your windshield, eventually the whole thing will crack. You can't build a system that intentionally subverts its own security for one purpose and then make the whole thing safe."

Strong encryption is of particular importance for journalists. Encryption helps journalists protect the content of their communications by ensuring it is only readable to someone who can decrypt it. Anonymization tools like Tor help journalists obscure the metadata of their communications – including the location

and identity of the sender – to help prevent a journalist from passive Internet surveillance which can allow an outsider to ascertain who is talking to whom and thereby track interests and behavior.

The Reporters Committee addressed the importance of encryption and anonymity devices for journalists in a joint comment with the Committee to Protect Journalists to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Special Rapporteur David Kaye solicited input from nongovernmental actors – including civil society, corporate actors, international and regional organizations, and national human rights institutions – for his upcoming report to the United Nations Human Rights Council in the summer of 2015.

Another issue that arose at the NAF summit was the need for private citizens and journalists to better understand where their data is going and how it can be accessed without their permission. Only when we can see our "data exhaust" will we be more inclined to take steps to minimize and obscure our data. Projects like Tactical Technology Collective's (Tactical Tech) Me and My Shadow, a tool that shows users the traces they leave online and explores ways to mitigate them, and Tactical Tech's more recent trackography map, which explores how the global tracking industry is reading your online behavior, are good steps in this direction.

As Stamos said at the NAF summit, security and usability of tools should not be considered orthogonal. Software companies need to ensure security is embedded in tools to make sure they are usable by the majority of non sophisticated users. A secure tool that is not usable is ineffective because it cannot be implemented securely.

As much as the profession requires tools that have security built in, information security also needs to be taught in a consistent, on-going way to have tangible results. Recent research conducted by Chris Walker and Carol Waters at the Tow Center for Digital Journalism at Columbia University reveals that information security training for journalists is largely ad-hoc or absent from newsrooms and journalism schools, and that when it is taught, it is often taught in a way that does not result in skill acquisition or strong retention. Fortunately, they put together some recommendations to help address these gaps.

Information security trainers also need to understand the psychological underpinnings of technology adoption to ensure journalists properly implement digital and operational security protections and do not risk jeopardizing their communications and their sources. As Angela Mckay, Director of Cybersecurity Policy and Strategy at Microsoft, mentioned at the NAF summit, research that specifically leverages behavioral psychology is needed to better understand how individuals, including journalists, use technology, because it could help inform adoption and utilization. Programs like LevelUp provide resources for the global

digital safety training community, including information focused on understanding the psychological needs of participants undergoing security training, and individuals like Gus Andrews of the Open Internet Tools Project are researching ways to improve how we teach about technology, but more needs to be done.

Better technology is only one part of the solution. Legal and policy solutions are also needed. Information sharing across traditional organizational boundaries has long been heralded by government and law enforcement officials as an answer to deterring attacks, in part because it was a principal recommendation of the 9/11 commission. However, real risks pertain to the sharing of private citizen and journalist information without robust safeguards to ensure information is minimized and secured while in transit or stored.

Although information sharing across government agencies about potential threats and attacks is encouraged by law enforcement and intelligence officials, information sharing via social media is not welcome, at least when it involves controversial topics like the Islamic State. At the NAF summit, John Carlin, the Assistant Attorney General for National Security at the U.S. Department of Justice, mentioned he would consider pursuing indictments against individuals who assist the Islamic State with its use and production of social media. Although the many acts of IS are despicable and horrific, punishing people for sharing information online could potentially infringe on First Amendment rights of free expression and free association.

Meanwhile, proposed changes to the already broad Computer Fraud and Abuse Act (CFAA) are also worrisome to security researchers and journalists. According to the Electronic Frontier Foundation's (EFF) legislative analyst Mark Jaycox, recent suggested changes to the CFFA could criminalize any unauthorized access to computer data—even if the data's owner leaves it unsecured. Doing so risks chilling or criminalizing work by security researchers who provide vulnerabilities to corporations about their products, and penalizes or prevents journalists from writing about information security issues.

In a time where every company is now a technology company, journalists and news organizations need to embrace information security training and information security experts need to develop tools that are both usable and secure. Transparency on the part of governments and corporations, along with continued activism and coverage of technological issues by journalists could create the space needed for constructive dialogue and solutions rather than defensive actions and entrenched positions.

Only by working together on these issues will we be better able to improve privacy, security, and transparency, and ensure First Amendment rights and freedoms are protected and respected.

Protecting anonymous commenters

Should news organizations look to shield laws in fighting subpoenas for posters' identities?

By Cindy Gierhart

This is a condensed version of a white paper on available means of protecting the identities of anonymous commenters on news web sites, which will be published in the near future.

By opening their web pages to anonymous online commentary, news organizations have opened themselves to subpoenas seeking the commenters' identities. Sometimes the subpoena is sought so the commenter, once identified, can then be sued for defamation. Sometimes a prosecutor or a defendant in a criminal trial would like to call the commenter as a witness, based on posts that suggest the commenter has relevant information of the crime. Sometimes prosecutors or defendants simply want to keep the commenters off the jury, based on their comments online.

Whatever the reason, news organizations have an interest in protecting the anonymous speech of those who post to their websites.

The emerging test setting forth guidelines for courts faced with requests to compel web sites to reveal identities of anonymous Internet speakers includes five factors: (1) the demanding party must make efforts to notify the anonymous commenter and allow a reasonable time for him or her to respond; (2) the demanding party must identify the exact statements made by the commenter; (3) the demand must set forth a prima facie cause of action, meaning it must present enough evidence for the demanding party, the prospective plaintiff in the libel claim, to win the case barring any defenses or additional evidence presented by the commenter; (4) the demanding party must bring forth sufficient evidence for each element of its defamation claim; and (5) the court must balance the speaker's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous commenter's identity.

This standard was developed in a 2001 New Jersey appellate case, *Dendrite International Inc. v. Doe No. 3*, and condensed in 2005 by the Delaware Supreme Court in *Doe v. Cahill*, which is favorable to anonymous commenters.[1] The approach requires that a prospective plaintiff must produce sufficient evidence to

establish the legal elements of defamation before they can uncover the identities of anonymous commenters. This threshold, as the Delaware high court noted in *Cahill*, discourages a "sue-first, ask-questions-later" strategy that would allow a plaintiff to unmask commenters by alleging specific defamation claims without evidence to back them up.

Using shield laws to protect anonymous commenters has produced mixed results.

The last decade has seen many cases where news organizations claim a reporter's privilege to protect anonymous posters, even when reporters did not use the posters as a source. These cases have mostly been handled at the trial court level without much guidance from appellate courts (with a few notable exceptions), and states are split on whether their shield laws apply to anonymous posters. Therefore, there is no surety in claiming a reporter's privilege for anonymous commenters, and, beyond that, news organizations may decide they don't want to stretch the privilege that far.

There is little commonality among the seven states that have applied a shield law to anonymous commenters and the four states that have not.

Colorado, Florida, Montana, North Carolina, Oregon, Texas, and – to an extent – Illinois have all applied their shield laws to protect anonymous posters.[2] Idaho, Indiana, Kentucky, and New Jersey have declined to extend their shield laws in such a manner.[3] Trying to draw patterns among the cases is difficult. Commenters were protected in both civil and criminal cases and *not* protected in both civil and criminal cases. Commenters were protected – and *not* protected – when posting to both traditional and non-traditional news websites. The statutes that were interpreted to protect anonymous commenters offered both absolute and qualified privileges, as did the statutes that were interpreted *not* to protect commenters. The North Carolina court found that the journalist who posted the story, which was later commented on, "was acting as a 'journalist,' all within the meaning of the Shield Law."[4] The Idaho court, conversely, found that the journalist who wrote a blog post hosted on his newspaper's website was *not* acting as a journalist but instead "as a facilitator of commentary and administrator of the Blog."[5]

Clearly, there is some room for interpretation, and it will be hard to achieve consensus on this topic until more appellate and state supreme courts weigh in.

Commenters as sources

Seven states have found that anonymous commenters are "sources" and that news organizations are engaged in the course of their business by receiving their information.

A trio of trial court decisions from Florida, Montana, and Oregon led the charge within about a month of each other in 2008. The first case was *Doty v. Molnar* from Montana, in which the plaintiff of a defamation lawsuit subpoenaed the *Billings*

Gazette, seeking identifying information for a number of online pseudonymous posters.[6] Montana's shield statute offers absolute protection, so that no news entity "may be required to disclose any information obtained or prepared or the source of that information in any legal proceeding if the information was gathered, received, or processed in the course of his employment or its business."[7] The court concluded that the statute is "very broad" and therefore protects the newspaper from having to reveal the anonymous posters.[8] The Montana Supreme Court later affirmed the decision without much discussion except to say there was no abuse of discretion.[9] The Oregon case was *Doe v. TS*,[10] and the Florida case was *Beal v. Calobrisi*.[11]

Texas trial courts twice applied its shield law to protect anonymous commenters, both times in murder trials. Texas has a qualified privilege in civil cases but an absolute privilege in most criminal cases where the information sought is from a confidential source, as in the cases here.[12] Both courts issued cursory, one-page orders granting the motions to quash, but the newspaper's attorney in *Martinez* and news reports in *Coe* indicate that the judges relied, at least in part, on the state's shield law.[13]

In another murder trial, a court in North Carolina quashed a subpoena seeking an anonymous commenter's identity from the *Gaston Gazette*. North Carolina offers "a qualified privilege against disclosure in any legal proceeding of any confidential or nonconfidential information, document, or item obtained or prepared while acting as a journalist."[14] In Colorado, a defendant sought the identity of a pseudonymous poster to *The (Colorado Springs) Gazette*, hoping the individual could help in his defense of a trespassing charge.[15] The judge quashed the subpoena based on the arguments raised by counsel, which included a shield law defense.

Finally, an Illinois trial court issued a perplexing decision that essentially found an anonymous commenter cannot be considered a "source" under the shield statute but then applied the statute anyway and protected the identities of three of the five subpoenaed commenters.[16]

It is worth noting briefly that, while a New York court has not decided whether to apply its shield law to online commenters, in two prior cases, New York courts have held that the state's shield law protects anonymous letters to the editor. In *Davis*, a New York family court held that a letter writer transmitted information to the newspaper confidentially, and that it was obtained "in the course of gathering news for publication."[17] In *Oak Beach Inn*, an appellate court held that the letter to the editor contained "news" because it contained accusations of a company's allegedly unsafe conditions, and therefore the shield law protected the anonymous writer's identity.[18]

There is little that all of these cases have in common, but several of them

required an analysis of who is a covered journalist or news entity; who is a "source"; and, if required by the statute (which was most often the case), whether the source's information was obtained during the course of newsgathering or as part of the reporter's employment. These courts chose a broad interpretation of their shield statutes, finding that comments posted online after a news story was written – but which continue the dialogue on issues of public interest – are protected under the reporter's privilege.

Four states have held that posting comments to a story after it has been published does not qualify for protection under a shield law. The New Jersey Supreme Court held that a blogger who *herself* posted on a message board could not claim a reporter's privilege, because she was not affiliated with a news organization or acting as a journalist by posting her comments, some of which cited confidential sources.[19] A Kentucky trial court declined to apply the state's shield law to a subpoena for a poster's identity.[20] Kentucky's absolute privilege is extremely broad, but a Kentucky court held that an anonymous comment posted after the story was written cannot qualify for the privilege.[21] An Indiana appellate court chose not to apply the state's shield law to protect an anonymous commenter accused of defamation for statements he made on the *Indianapolis Star* website.[22] The court determined that an anonymous commenter could not possibly be a source in the traditional sense because the comment was posted after the story was written.[23]

An Idaho trial court had a slightly different reason for denying shield law protection to anonymous commenters: it found that the employee who managed the newspaper's blog was not "acting as a reporter."[24] It is not terribly surprising that the Idaho court chose not to apply a reporter's privilege considering Idaho does not have a shield statute and has been reluctant to recognize a privilege at common law.[25]

Should news organizations use shield laws?

Regardless of whether a news organization *can* claim a reporter's privilege to protect anonymous commenters, the question remains whether they *should*. There are convincing reasons on both sides of the argument. News organizations should consider whether claiming a reporter's privilege for anonymous commenters advances their interests.

On the one hand, claiming a reporter's privilege for anonymous speech supports an evolving concept that news in the digital age does not end when the ink dries on the page. News reporting is fluid, and posting an article online does not conclude the newsgathering phase but begins it.[26] Not all anonymous commenters make worthwhile contributions to the dialogue, but many offer new information, insights, and commentary that advance the story.

A New York appellate court in 1983 wrote:

> [M]any people read the letters to the editor column for the same reasons

> they read any other news column in the paper - to learn what is happening around them, and the reactions of other people to these events. The beneficial purposes served by the Shield Law would be unnecessarily restricted by removing the letters to the editor column from its aegis.[27]

The same can be said of online commentary, the modern-day equivalent of letters to the editor. Commenters contribute to the discourse on matters of public interest in their own right.

The purpose of a reporter's privilege can be reconciled with shielding anonymous commenters, as well. Journalists are protected from having to reveal their sources because people would otherwise be unwilling to come forward and share stories of public importance without a guarantee of anonymity. So, too, are anonymous commenters unlikely to provide information in the comments section of news stories if their identities could easily be revealed.

Yet there are a number of reasons why news organizations may want to limit their use of the reporter's privilege to protect online commentary. The journalism profession has always urged caution when using anonymous sources in news stories.[28] After *The New York Times* suffered the scandal of reporter Jayson Blair inventing anonymous sources who didn't exist, the *Times* redrafted its policy in 2004 to tighten its standards and allow anonymous sources only "as a last resort."[29] As a result, the use of anonymous sources by *Times* reporters decreased by half between 2004 and 2007.[30] Considering the profession's desire to reduce its reliance on anonymous sources, it may not make sense to have the newsroom shrinking its association with them and the legal department expanding it.

Another potential problem is the barrier it can create for truly meritorious defamation claims, because the news organizations themselves are not liable for defamatory postings of their readers under Section 230 of the Communications Decency Act.[31] This could in turn prompt state legislatures to cut the potency of their shield laws. In the 1983 case where a New York court held that the shield law protects anonymous letters to the editor, the judge found it significant that the plaintiffs "can still of course pursue their [defamation] action against the [newspaper]."[32] The newspaper could protect the anonymous letter writer from being sued, but it could not itself escape liability for printing the allegedly defamatory statements. But that is no longer the case for speech online because of Section 230. First Amendment anonymous speech doctrine suitably protects anonymous commenters while at the same time allowing plaintiffs to unmask speakers if they can sufficiently show a meritorious cause of action. But some states' shield laws that offer absolute privilege will not allow any claims, meritorious or otherwise, to breach that barrier. Legislatures are not likely to let this stand. At best, they will rewrite their shield laws to clarify that anonymous commenters are not covered; at worst, they will downgrade absolute privileges to

qualified privileges or otherwise diminish the privilege.[33]

End notes:

[1] *John Doe No. 1 v. Cahill*, 884 A.2d 451 (Del. 2005); *Dendrite Intern., Inc. v. Doe No. 3*, 775 A.2d 756 (N.J. App. Div. 2001); *see also* Ashley I. Kissinger & Katharine Larsen, *Shielding Jane and John: Can the Media Protect Anonymous Online Speech*, Comm. Law., July 2009, at 5-9 (explaining how the various unmasking standards have been used across the country to quash subpoenas seeking anonymous commenters' identities).

[2] *Colorado Springs v. Bruce*, No. 09M3247 (Colo. Springs Mun. Ct. Oct. 27, 2009); *Beal v. Calobrisi*, No. 08-CA-1075 (Fla. Cir. Ct. Oct. 9, 2008), *available at* http://www.newsroomlawblog.com/uploads/file/Beal_v__ Calobrisi.pdf; *Alton Telegraph v. Illinois*, 37 Media L. Rep. 2084 (Ill. Cir. Ct. 2009), *available at* http://www.dmlp.org/sites/citmedialaw.org/files/2009-05-15-Alton Telegraph Decision.pdf; *Doty v. Molnar*, No. DV 07-022 (Mont. Dist. Ct. Sept. 3, 2008), *available at* http://www.dmlp.org/sites/citmedialaw.org/files/2008-09-03-Hearing and Oral Ruling on Billings Gazette Motion to Quash.pdf, *aff'd*, 317 P.3d 204, 2013 WL 4478215 (Mont. 2013); *North Carolina v. Mead*, No. 10 CRS 2160 (N.C. Super. Ct. Aug. 16, 2010), *available at* http://www.newsroomlawblog.com/uploads/file/Order - NC v_ Michael Lane Mead.PDF; *Doe v. TS*, No. CV08030693 (Or. Dist. Ct. Sept. 30, 2008); *Texas v. Coe*, No. 1227878 (Tex. Dist. Ct. June 15, 2010) (on file with the author); *Texas v. Martinez*, No. 17042-B (Tex. Dist. Ct. June 19, 2009) (on file with the author).

[3] *Jacobson v. Doe*, No. CV-12-3098 (Id. Dist. Ct. July 10, 2012), *available at* http://bit.ly/1opZCUm; *Ind. Newspapers Inc. v. Junior Achievement of Cent. Ind., Inc.*, 963 N.E.2d 534 (Ind. Ct. App. 2012); *Clem v. Doe*, No. 08-CI-1296 (Ky. Cir. Ct. Madison County Mar. 26, 2010); *Too Much Media, LLC v. Hale*, 20 A.3d 364 (N.J. 2011).

[4] *Mead*, No. 10 CRS 2160, at 2.

[5] *Jacobson*, No. CV-12-3098, at 7.

[6] *Doty*, No. DV 07-022; *Doty v. Molnar*, 317 P.3d 204, 2013 WL 4478215, at ¶ 4 (Mont. 2013).

[7] Mont. Code Ann. § 26-1-902 (2009).

[8] *Doty*, No. DV 07-022, at 29.

[9] *Doty v. Molnar*, 317 P.3d 204, 2013 WL 4478215 (Mont. 2013).

[10] *Doe v. TS*, No. CV08030693 (Or. Dist. Ct. Sept. 30, 2008).

[11] *Beal v. Calobrisi*, No. 08-CA-1075 (Fla. Cir. Ct. Oct. 9, 2008), *available at* http://www.newsroomlawblog.com/uploads/file/Beal_v__Calobrisi.pdf.

[12] Jason A. Martin, Mark R. Caramanica, & Anthony L. Fargo, *Anonymous Speakers and Confidential Sources: Using Shield Laws When They Overlap Online*, 16 Comm. L. & Poly' 89, 109–10 (2011).

[13] *Id.*

[14] N.C. Gen. Stat. § 8-53.11(b) (1999).

[15] Mot. of Third Party Witness Steve Pope to Quash Subpoena Duces Tecum, in *Colorado Springs v. Bruce*, No. 09M3247 (Oct. 21, 2009) (on file with the author) (explaining that the poster claimed to have seen the defendant collecting signatures at a Costco, which apparently would have helped his trespassing defense).

[16] *Alton Telegraph v. Illinois*, 37 Media L. Rep. 2084 (Ill. Cir. Ct. 2009).

[17] *Davis v. Davis*, 386 N.Y.S. 2d 992, 994 (Fam. Ct. 1976).

[18] *Oak Beach Inn Corp. v. Babylon Beacon, Inc.*, 92 A.D.2d 102, 104 (N.Y. App. Div. 1983).

[19] *Too Much Media, LLC v. Hale*, 20 A.3d 364, 371–72 (N.J. 2011).

[20] *Clem v. Doe*, No. 08-CI-1296 (Ky. Cir. Ct. Madison County Mar. 26, 2010).

[21] *Clem*, No. 08-CI-1296, at 3.

[22] *Ind. Newspapers Inc. v. Junior Achievement of Cent. Ind., Inc.*, 963 N.E.2d 534 (Ind. Ct. App. 2012).

[23] *Ind. Newspapers*, 963 N.E.2d at 547.

[24] *Jacobson v. Doe*, No. CV-12-3098, at 7 (Id. Dist. Ct. July 10, 2012), *available at* http://bit.ly/1opZCUm.

[25] *See* Debora Kristensen, *Idaho*, in Reporter's Privilege Compendium, Reporters Comm. for Freedom of the Press, at 3, *available at* http://www.rcfp.org/rcfp/orders/docs/privilege/ID.pdf.

[26] *See, e.g., Doty v. Molnar*, No. DV 07-022, at 17 (Mont. Dist. Ct. Sept. 3, 2008), *available at* http://www.dmlp.org/sites/citmedialaw.org/files/2008-09-03-Hearing and Oral Ruling on Billings Gazette Motion to Quash.pdf (quoting the *Billings Gazette* editor as saying, "The on-line story comments have become an integral and necessary part of the *Gazette* business of gathering and disseminating news and information").

[27] *Oak Beach Inn Corp. v. Babylon Beacon, Inc.*, 92 A.D.2d 102 (N.Y. App. Div. 1983).

[28] *See, e.g., AP News Values & Principles*, Associated Press, http://www.ap.org/company/news-values (last visited Aug. 30, 2014) ("[W]e always strive to identify all the sources of our information, shielding them with anonymity only when they insist upon it and when they provide vital information – not opinion or speculation; when there is no other way to obtain that information; and when we know the source is knowledgeable and reliable."); *Anonymous Sourcing*, NPR Ethics Handbook, http://ethics.npr.org/tag/anonymity/ (last visited Aug. 30, 2014) ("Unidentified sources should rarely be heard at all and should never be heard attacking or praising others in our reports.").

[29] Clark Hoyt, Op-Ed., *Culling the Anonymous Sources*, N.Y. Times (June 8, 2008), http://www.nytimes.com/2008/06/08/opinion/08pubed.html.

[30] *Id.*

[31] 47 U.S.C. § 230.

[32] *Oak Beach Inn*, 92 A.D.2d at 104.

[33] *See Ind. Newspapers Inc. v. Junior Achievement of Cent. Ind., Inc.*, 963 N.E.2d 534, 548 (Ind. Ct. App. 2012) (arguing that the combination of shield laws and Section 230 immunity "could leave legitimately injured plaintiffs without a legal remedy") (quoting Kissinger & Larsen, *supra* note 1); Aaron Mackey, *Two Recent Cases Highlight Tension in Applying Shield Law to New Media*, News Media & L. (Summer 2011), *available at* http://bit.ly/1wXymGJ (quoting a Hawaii media lawyer who expressed concern over a Hawaii newspaper's use of the shield law to protect anonymous commenters - for a subpoena that was later withdrawn - because it could make already nervous lawmakers even more hesitant to support renewal of the shield bill).

Glomar surfaces in state courts

By Adam Marshall

U.S. Government photo

The Glomar Explorer

On March 1, 1968, a catastrophic incident aboard Soviet submarine K-129, sailing approximately 1500 miles northwest of Hawaii, led to the loss of all people and three ballistic nuclear missiles as the ship sank to the bottom of the seabed, almost 17,000 feet below the surface.

Alerted to the event, the CIA rushed to devise an operation that would recover K-129 with the help of a specially constructed ship — the *Hughes Glomar Explorer*. While the mission was only partly successful, the name of the recovery ship has lived on as a special exemption to the federal Freedom of Information Act (FOIA) that allows the CIA and other agencies to "neither confirm nor deny" the existence of information. Now, for the first time, the *Glomar* doctrine is beginning to emerge in state courts as law enforcement agencies seek new methods to keep their records out of the public eye.

The public first learned of the efforts of the CIA to recover K-129 in 1975, based on reporting by syndicated columnist Jack Anderson and *New York Times* reporter Seymour Hersh. Based on the revelations, Harriet Ann Philippi, the Washington correspondent for *Rolling Stone*, filed FOIA requests with the CIA to uncover additional information. Ms. Philippi was particularly interested in the CIA's efforts to persuade the media not to report on their covert mission. Unfortunately for Philippi, not only did the CIA refuse to release any records, it contended that "the fact of the existence or non-existence of the records" she requested would jeopardize national security.

Philippi filed suit in federal district court to challenge what the D.C. Circuit Court of Appeals would later characterize as "a case in which the Agency has refused to confirm or deny the existence of materials requested under the FOIA". No provision to issue such a response exists in the statute. In the normal course of business, after a FOIA request is submitted the agency must make a "determination" by going through its records and identifying which are responsive. Afterwards, the agency must either release the records or cite a specific exemption that allows them to be withheld.

Despite these clear statutory provisions, the trial court in Philippi's case allowed the CIA to refuse to answer whether or not it had responsive records in what has become known as a *Glomar* response. The D.C. Circuit ended up affirming the power of the intelligence agency to issue such a response but laid down procedural rules that were designed to ensure as much information as possible was made public to enable the requester to challenge the holdings.

Since the 1970s, *Glomar* responses have become a common phenomenon for those who seek information from intelligence agencies. It has even been codified in the current FOIA regulations for the CIA and the Department of Defense. *Glomar* responses have been particularly frequent in FOIA litigation since September 11, 2001, much to the dismay of requesters who face with an almost impenetrable veil of secrecy.

Part of the reason that *Glomar* cases are so difficult to challenge is that when the agency refuses to admit whether or not they have records related to the request, the nature of the case shifts to whether the subject of the request is generally something that could touch on national security. In doing so, courts give substantial deference to the conclusions of government personnel who are in control of the documents. With little information to challenge the government's assertions, a *Glomar* response almost always results in a win for secrecy.

Until recently, invocations of the *Glomar* doctrine had been limited to federal agencies. This follows the rationale that has been affirmed numerous times in federal courts—there are certain matters of national security that would be irrevocably harmed if the public were to learn that clandestine activity was being carried out with response to a certain subject.

But now, two state trial level courts — one in New Jersey and one in New York — have allowed state law enforcement agencies to neither confirm nor deny the existence of records in response to requests under local sunshine laws. Like the federal FOIA, the laws of these states make no mention of issuing *Glomar*-type responses. These two courts simply created new judicially recognized exemptions, the full impact of which has only begun to emerge.

In July 2013, a reporter at *Community News* in New Jersey sent an open records request to the Bergen County Prosecutor's Office, asking for law enforcement reports, complaints, 911 calls, and communications regarding Leo J. Butler, a pastor at a local church. The Prosecutor's Office responded by stating they "decline to indicate whether it possesses any records that are responsive [to the request]."

Community News brought suit in September 2013 to compel the Prosecutor's Office to release the records under both the New Jersey Open Records Act (OPRA) and the common law right of access. The trial court did not directly address the Prosecutor's *Glomar*-esque response, but rather skipped directly to an analysis of whether the general category of records sought — not the specific records in the

case — should be exempt from disclosure. It ultimately held the records need not be disclosed under the privacy provision of the New Jersey constitution. According to the court, "the investigation of an individual that has not been arrested nor charged with a crime generally must not be disclosed as privacy concerns outweigh the public's need for the information."

The decision has been appealed by *Community News*, which argues the court "created a new exemption in which a public agency is now able to deny access to public records while at the same time refusing to admit or deny whether records even exist." The Prosecutor's Office, however, contends that the trial court "merely recogniz[ed] and elucidat[ed] existing statutory exemptions". The Reporters Committee, along with twenty-five media organizations, submitted an *amicus curiae* brief to the appellate court describing the disastrous impact of the *Glomar* doctrine on transparency and the impropriety of its incorporation into state law. A ruling on the appeal has yet to be made.

A second decision, coming out of a New York trial court, is more worrisome to transparency advocates because it expressly adopts the *Glomar* doctrine. Talib Abdur-Rashid is a New York based Imam who heads the Mosque of Islamic Brotherhood, located at the site where Malcom X's congregation once gathered. In 2012, Abdur-Rashid submitted a request under the New York Freedom of Information Law (FOIL) to the NYPD requesting any records they had related to surveillance of Abdur-Rashid or his mosque.

In 2011, the Associated Press reported that the NYPD had set up a special "Demographics Unit" to surveil and track Muslims within the city. The Demographics Unit was set up with the help of Lawrence Sanchez, a CIA officer assigned to New York. Sanchez subsequently left the CIA to work full time with the NYPD. Another CIA officer was also assigned to work with the NYPD's Intelligence Division as part of a "management sabbatical."

No records were disclosed in response to Abdur-Rashid's FOIL request. After he filed a lawsuit to force the NYPD to turn over responsive records, the law enforcement agency submitted an unusual response. The NYPD's motion to dismiss asks the court to "recognize [the NYPD's] legitimate law enforcement need to withhold a substantive response to Petitioner's FOIL request, by allowing them to neither confirm nor deny the existence of responsive records." It states that the circumstances of Abdur-Rashid's case "provides the Court with ample basis to adopt the Glomar doctrine in connection with requests made under FOIL."

Instead of skirting the *Glomar* issue like the New Jersey court, Justice Hunt squarely addressed it, finding it entirely appropriate to adopt the doctrine into the New York FOIL. The decision, handed down in September 2014, acknowledges that numerous cases have found FOIA and its provisions inapplicable to state agencies, and therefore "[i]t should follow that when a local agency such as the NYPD is

replying to a FOIL request, the Glomar doctrine is similarly inapplicable."

Perplexingly, the court then goes on to state that as this was a case of first impression it was appropriate to look to federal decisions for guidance. In so doing, it determined that the NYPD's use of a Glomar response "is in keeping with the spirit of similar [federal] appellate court cases." According to the opinion, "disclosing the existence of responsive records would reveal information concerning operations, methodologies, and sources of information of the NYPD, the resulting harm of which would allow individuals or groups to take counter-measures to avoid detection of illegal activity, undermining current and future NYPD investigations." As a result, it granted the NYPD's motion to dismiss.

The case appears to be the first time in United States history that a state court has explicitly recognized the *Glomar* doctrine in an open records case. Abdur-Rashid has since appealed, but no decision is expected until later this spring.

After learning of Abdur-Rashid's case, the Reporters Committee submitted an open records request to the NYPD asking for communications between NYPD employees and federal government employees concerning *Glomar* responses. The NYPD denied RCFP's request on the basis that its request did not "reasonably describe a record in a manner that would enable a search to be conducted".

The Reporters Committee administratively appealed the denial, arguing that it described the records in more than sufficient detail to search for the requested records. In considering RCFP's appeal, Jonathan David, the NYPD officer assigned to the case, determined that there were no agreements, contracts, or memoranda between the NYPD and employees of the federal government concerning *Glomar* responses. However, David affirmed the denial of RCFP's request with respect to communications (including emails, letters, and notes) between the NYPD and federal government, stating that it did not describe a record "in a manner that could lead to its retrieval".

A third case from New York, a companion to that of Abdur-Rashid's, recently decided against incorporating the *Glomar* doctrine into state law. As a result of the AP reporting on the NYPD targeted surveillance program, Samir Hashmi, a student at Rutgers University, filed a FOIL request with the NYPD. He asked for any records related to surveillance of him or a Muslim student group he was affiliated with. The NYPD again issued a *Glomar* response, refusing to acknowledge whether records related to Mr. Hashmi's request existed or not. After Hashmi brought suit against them, the NYPD sought to have the case dismissed by asking the New York trial court to adopt the *Glomar* doctrine. But this time, with a different judge hearing the motion, the court refused.

Justice Moulton, the trial judge assigned to the case, strongly disagreed with the idea that the *Glomar* doctrine could, or should, be imported into New York's open government law. According to the opinion, doing so would be to judicially enact a

“profound change” to a statute that has been finely calibrated by the legislature over many years.

“The insertion of the Glomar doctrine into FOIL would build an impregnable wall against disclosure of any information concerning the NYPD’s anti-terrorism activities”, he wrote.

The opinion also challenges whether the disclosure of information would actually impede the NYPD. Justice Moulton wrote that “case law demonstrates that the NYPD has been able to protect sensitive information very well within existing procedures that FOIL currently provides.”

Finally, the court questioned why *Glomar* should be coming up in the state context at all. Justice Moulton noted that the *Glomar* response has been shaped in federal courts in the context of national defense and foreign policy by agencies that often deal with classified documents. The court stated that this history undermines its applicability to the NYPD, a domestic law enforcement agency with no classification authority.

The NYPD has appealed the decision, and the case is expected to be heard in the spring alongside that of Mr. Abdur-Rashid.

It remains to be seen whether New York and New Jersey are isolated incidents, or whether “neither confirm nor deny” responses will become as obfuscating at the state level as it has for the federal government. Journalists everywhere should be on the lookout for these responses when they interact with state agencies, especially law enforcement. Transparency groups, including the Reporters Committee, are on the lookout as *Glomar* continues to resurface.

Lynch hearing touches on FOIA issues

In hearing, Lynch says critical FOIA evalution of U.S. Attorney's office was "helpful"

By Sade Hale

AP Photo

U.S. Attorney Loretta Lynch at her confirmation hearing on Jan. 28.

Issues of compliance with the Freedom of Information Act received some attention during Loretta Lynch's eight-hour confirmation hearing on Wednesday.

Lynch said she will work with Congress to improve public access to open records, and described the Freedom of Information Act as "an important tool for the American people."

But Republican Sen. John Cornyn of Texas asked Lynch about "critical comments" made in a FOIA management evaluation of the U.S. Attorney's office of the Eastern District of New York, where Lynch was in charge.

The evaluation, released several days before the hearing, mentioned numerous FOIA issues, including: not substantially complying with the Executive Office for United States Attorneys Management Standards regarding management of the FOIA program, not responding to records requests in a timely manner, not effectively supervising its FOIA program, and not providing sufficient training to current and newly hired employees.

Lynch said her office immediately corrected these issues and found the evaluation to be very helpful.

"I specifically asked the evaluators to look at our management systems and our support staff systems to make sure we were in compliance and to bring any issues to our attention. They raised this issue, which was of great concern to me. We immediately took steps to rectify the issues that we found within our own office functioning," Lynch said.

"We have added increased personnel to handle Freedom of Information Act requests. We work closely with the Department of Justice to ensure they are handled

as expeditiously as possible. So I actually found it to be a very helpful evaluation process, and I find that I have learned the most when someone has pointed out to me an area which I might improve."

But witnesses before the committee did not talk about FOIA issues, and mainly seemed to raise concerns about the current attorney general. Former CBS News correspondent and investigative journalist Sharyl Attkisson was one of nine witnesses who testified on Thursday, the second day of the hearing. While none of the witnesses raised their hands when asked by Sen. Patrick Leahy, D-Vt., if they opposed Lynch, Attkisson did voice her concerns.

"The nominee, if confirmed, should chart a new path to reject the damaging policies and practices that have been used by others in the past. If we aren't brave enough to confront these concerns, it could do serious long-term damage to the supposedly free press," Attkisson said in her opening statement.

Attkisson, who is currently suing the Department of Justice and Attorney General Eric Holder for allegedly hacking her computer, criticized the federal government's handling of public records.

Calling it "pretty much pointless and senseless now," she suggested that FOIA is being "used as a tool to obstruct and delay the release of public information. It’s no good. FOIA is extremely broken at the federal level."

Like Attkisson, some committee members, too, wonder if Lynch will follow the same trail as Attorney General Holder. Throughout the hearing, Lynch assured the committee that "if confirmed as attorney general, I will be myself. I will be Loretta Lynch."

The committee will vote and make its decision on Lynch’s confirmation in the upcoming weeks.

An injunction remains, one year and counting

The ban on "Innocense of Muslims" from Garcia v. Google continues to violate the First Amendment

AP Photo

Cindy Lee Garcia, right, shown with her attorney, obtained an injunction against YouTube owner Google Inc. with a novel copyright argument over her appearance in the film "Innocence of Muslims."

On December 15, the Ninth Circuit reheard oral argument *en banc* in a case that has odd facts and has made terrible law. In *Garcia v. Google*, a panel of judges on the Ninth Circuit issued a broad mandatory injunction compelling Google to remove and take measures to prevent the publication of a controversial video — all based on a novel copyright theory.

The injunction was issued in February last year. In March, the U.S. Copyright Office rejected the plaintiff's attempt to register her asserted copyright. Yet despite the plaintiff's exceedingly attenuated copyright interest, the injunction continues to be in force a year later, restraining Google from publishing the video.

Oral argument focused on the relatively dry area of the standard for a mandatory injunction. But as Google argued, that standard has real-world implications for the First Amendment. Quoting *Overstreet v. United Brotherhood of Carpenters*, Google argued that if "there is at least some risk that constitutionally protected speech will be enjoined, only a particularly strong showing of likely success, and of harm to the defendant as well, could suffice" to support an injunction. The Reporters Committee has joined amicus briefs at the rehearing and en banc stages supporting Google.

The *Garcia* case stems from the making of a notorious film in August 2011. Cindy Lee Garcia, an aspiring actress, answered a casting call for a film called *Desert Warrior*. She believed it to be an action film set in the Middle East. When the

film was released, however, it appeared on YouTube and elsewhere under the name *The Innocence of Muslims*. Garcia's formerly unremarkable lines were dubbed over with inflammatory dialogue about the Prophet Muhammad, and the film touched off protests and riots the world over.

Seeking to have the film taken offline, Garcia filed eight takedown notices under the Digital Millennium Copyright Act. When Google refused to comply, Garcia sued for injunctive relief, claiming that her performance in the film is copyrightable independent of the film itself. The district court declined to issue the injunction Garcia sought. But a panel majority in the Ninth Circuit reversed the district court and issued a mandatory injunction, ordering Google to remove the video and take steps to prevent its future publication. The Ninth Circuit reached this result despite finding Garcia's copyright interest "debatable." And, indeed, the Ninth Circuit cited no precedent in support of the notion that an actor retains an independent copyright interest in his or her performance in a film.

This case is troubling for a number of reasons beyond the implausibility of Garcia's actual copyright claim. The court utterly dismissed concerns that the injunction infringed on Google's First Amendment rights. If Garcia had sought an injunction as a remedy for tort, the court would have been forced to consider Google's First Amendment interests, because an injunction in a tort case is a classic prior restraint. But because the court determined that Garcia has a possible copyright interest, it evaded that First Amendment inquiry with the conclusory and unsatisfying statement that the "First Amendment doesn't protect copyright infringement."

The First Amendment doesn't protect defamation either, but courts don't issue injunctions in libel cases because of the heavy presumption of the invalidity of prior restraints. That we are even having this conversation *nine months* into the injunction is astonishing. In a comparable 1996 case, a federal district court issued a temporary restraining order barring *Business Week* from publishing sealed court documents it had obtained in connection with a commercial lawsuit brought by Procter & Gamble. After a few weeks, the court unsealed the documents, allowing *Business Week* to publish its article, but left an injunction against the magazine in place. The Sixth Circuit heard argument two months later and issued its decision three months after that, reversing the district court and holding that the injunction violated the First Amendment. In the seminal Pentagon Papers case, only fifteen days elapsed between the initial temporary restraining order that barred *The New York Times* from publishing its story and the Supreme Court decision striking down that order as an impermissible prior restraint. Contrast that to the *Garcia* case, where the Ninth Circuit waited seven months before granting rehearing en banc and has now delayed over nine months since the panel's order was issued. The urgency normally associated with restraints on speech has been completely absent from this

proceeding.

The case has direct ramifications for media organizations that reported on the film and the ensuing controversies surrounding it. Many articles about the riots after the release of the film linked to or embedded versions of the film. While the injunction is in place, Garcia could presumably seek to enjoin any news media organization's future publication of the film. This hampers discussion not only of the aftermath of the film itself, but also of Garcia's litigation.

While the cascading effects of the *Garcia* injunction on traditional media are an additional harm, to be sure, Google itself feels the effect of the restraint most strongly. An injunction restraining Google from disseminating information is no less concerning than a prior restraint directed at the traditional media. Although Google is not a content creator, it plays a hugely important role in the marketplace of ideas. YouTube is an essential service for conveying news, art, and information. The *Garcia* injunction prevents Google from fulfilling its commercial goals as well as exercising its First Amendment rights. This case should be treated as urgently as any other prior restraint would.

More broadly, the incoherence of the prior restraint doctrine between tort and copyright is nonsensical from a First Amendment perspective. In essence, the panel held that a mandatory injunction would be an illegal prior restraint if sought as a remedy in a tort case, but if the underlying claim sounds in copyright, even when the copyright claim itself is doubtful, the injunction is not only permissible but also does not even require First Amendment scrutiny. Yet, as the dissent pointed out, the doubtfulness of the plaintiff's claim makes the damage she alleges all the more attenuated, while this unprecedented infringement on Google's liberties is real and concrete. The Ninth Circuit failed to recognize that copyright is no more compelling a logic than tort to hamper constitutionally protected speech.

What's more, the impermissible injunction that the panel majority issued in February 2014 continues to bar Google from exercising its First Amendment rights, even after rehearing in December. Because the Ninth Circuit did not vacate the panel opinion when it granted rehearing, Google has no choice but to assume the injunction remains in force. As the Supreme Court has recognized, this type of injunction does not just "chill" speech — it "freezes" it. Let's hope that a thaw is on the horizon.

Grand jury secrecy comes at a cost

By Tom Isler

Two new lawsuits are challenging the continued secrecy of the grand jury investigations related to the deaths of Michael Brown in Ferguson, Mo., and Eric Garner in Staten Island, N.Y. The suits demonstrate just how secret the information gathered by a grand jury is, while also making a compelling case for the public interest in greater access.

Last week, an anonymous member of the Ferguson grand jury filed a federal lawsuit to establish his or her right to speak out about the grand jury experience. A Missouri state law makes it a misdemeanor for grand jurors to talk about the grand jury proceedings, and the juror, identified in public court documents as "Grand Juror Doe," seeks both a ruling that the law is unconstitutional as applied in this case and an injunction to prevent prosecutors from bringing charges against Doe if he or she speaks to the media about the proceedings.

Meanwhile, Letitia James, the New York City Public Advocate, and the New York Civil Liberties Union, are asking a state court judge in New York to release grand jury evidence in the Eric Garner case. The court will hear oral argument on the motions on January 29.

The two cases illustrate how strong the secrecy protections are for grand juries and how difficult it can be for the public to have any meaningful oversight of the process to guard against potential abuse.

The traditional justifications for secrecy include preventing escape of investigation targets, preventing tampering with witnesses or grand jurors, encouraging free and open witness testimony and juror deliberations, and protecting the identities of targets who are exonerated after investigation but before indictment.

In addition, courts and prosecutors typically justify secrecy by arguing that disclosure of witness testimony could have a chilling effect on future grand jury witnesses.

Secrecy isn't absolute, however.

Grand jury witnesses are generally free to disclose their own testimony, according to the U.S. Supreme Court's holding in *Butterworth v. Smith* (1990), but are prohibited from revealing other details about the process. Court rules and state laws usually prevent others — jurors, lawyers, court staff — from discussing what was revealed to, or discussed by, the grand jury. (A grand jury recently recommended that Pennsylvania Attorney General Kathleen G. Kane be indicted for

violating grand jury secrecy rules and leaking investigative material to embarrass political foes, according to the *Philadelphia Inquirer*.)

Penalties for disclosure can be harsh. In 1994, a former grand juror, who leaked information related to several mob prosecutions in Chicago, was sentenced to more than eight years in prison. More recently, a lawyer who leaked information from the BALCO steroids grand jury investigation, was sentenced to two and a half years in prison.

The public record of grand jury proceedings is usually filtered through what information prosecutors voluntarily reveal or seek a court order to disclose.

In Ferguson, St. Louis County prosecutor Robert McCulloch released thousands of pages of evidence and transcripts, telling reporters that he wanted to be transparent and that "everyone will be able to examine that same evidence and come to their own conclusion." (Although McCulloch originally sought a court order to release the documents, he withdrew that motion and disseminated the material on his own authority.)

But the lawsuit by Grand Juror Doe casts doubt on whether those disclosures paint an accurate picture of the proceedings, and whether grand jury secrecy allowed the prosecutor to manipulate the public's perception of the process and to shield atypical prosecutorial tactics from view. According to Doe's complaint, the proceedings in the Brown case were conducted differently from that of other grand juries, including focusing more strongly on the victim Brown rather than Officer Darren Wilson. The complaint alleges that the released documents "do not fully portray the proceedings before the grand jury."

Doe asserts that "the current information available about the grand jurors' views is not entirely accurate — especially the implication that all grand jurors believed that there was no support for any charges." Doe's goal is to "express opinions about: whether the release of records has truly provided transparency; Plaintiff's impression that evidence was presented differently than in other cases, with the insinuation that Brown, not Wilson, was the wrongdoer; and questions about whether the grand jury was clearly counseled on the law."

In New York, Public Advocate James seeks grand jury evidence because the "interest of the public and the perception of fairness make transparency vital," according to news reports.

If the courts do not rule in favor of increased transparency, the public may never get a richer picture of the two grand jury investigations that sparked protests worldwide.

Or, at least, the public may have to wait a while.

The Reporters Committee for Freedom of the Press, along with a coalition of historians and archivists, currently has a petition pending in federal court in Chicago to unseal witness transcripts from a grand jury investigation into the

Chicago Tribune dating back to 1942. Despite the fact that most of the known figures in the investigation died more than 40 years ago, the material remains sealed by default, and the U.S. Department of Justice opposes disclosure.

In the middle of World War II, the *Tribune* published a story that suggested the United States had broken the Japanese naval codes and had advance notice of Japanese plans to attack Midway Island. The government's investigation into the *Tribune* remains the only time in American history that the government sought to use the Espionage Act to indict members of the mainstream media.

Courts have long recognized the benefits of grand jury secrecy. But these law suits are a reminder that secrecy comes at a cost, and increased transparency may indeed be in the public interest.

"Citizenfour" filmmakers move to dismiss federal lawsuit

By Tom Isler

Still from citizenfour

A lawsuit over Edward Snowden's actions, detailed in the documentary "citizenfour," prompted a private lawsuit.

The makers of *Citizenfour*, the Oscar-nominated documentary film about Edward Snowden, have moved to dismiss a federal civil lawsuit that alleges they aided and abetted the "illegal and morally wrongful acts" of Snowden.

Filmmaker Laura Poitras, her producers and the entertainment companies behind *Citizenfour* were sued in December by Horace Edwards, the 89-year-old former secretary of the Kansas Department of Transportation, who seeks to have all of the film's proceeds reallocated to the United States treasury.

Because Snowden, who is also named as a defendant, held a position of trust with the government as a contractor for the National Security Agency, the lawsuit asserts, and because he breached his "fiduciary duties" to the United States and the American people, neither he nor the filmmakers should be allowed to profit financially from the "purloined" information.

The same (highly questionable) legal claims could be directed against any news outlet that reports on any unauthorized leak of classified information, and generates revenue related to those stories or broadcasts. Although Edwards did not name Glenn Greenwald, *The Guardian*, or any other journalists or news outlets as defendants, according to the logic of his own complaint, he certainly could have.

Edwards's suit is modeled after a 1980 Supreme Court case called *Snepp v. United States*, in which the government sued a former CIA agent who had written a book about his CIA activities without first getting approval from the CIA, in violation of a trust agreement Snepp had signed with the CIA. The Supreme Court ruled that Snepp had breached fiduciary duties to the United States by publishing the book without seeking approval and ordered that his profits be paid over to the government. (Coincidentally, Snepp appears in Rory Kennedy's new documentary, Last Days in Vietnam, which is nominated for an Oscar this year, alongside

Citizenfour).

The filmmakers, in their motion to dismiss, argue that *Snepp* presented a much different legal question. Here, unlike in *Snepp*, the alleged wrongdoer neither made a contract nor maintained any relationship of trust directly with the plaintiff. Because Snowden didn't personally owe Edwards any special duties, the filmmakers contend that they cannot be held liable for aiding or abetting any alleged breach of those nonexistent duties.

Another salient distinction is that in *Snepp*, the United States itself brought the lawsuit; it wasn't filed on behalf of the United States or the American public by a citizen who happened to buy a copy of Snepp's book. Although Edwards asserts that he has standing to sue the Citizenfour filmmakers because he bought a ticket to see the documentary, which "outraged" him, the filmmakers counter that simply buying a ticket isn't an economic injury of the type that would allow him to bring suit. By Edwards's logic, anyone who purchased a newspaper or maintained an online subscription could theoretically sue a newspaper to disgorge its profits related to a story about a national security leak.

In their motion to dismiss, the filmmakers also argued that filmmakers have a constitutional right to publish truthful information on a matter of public interest, even if it was obtained through unauthorized means—a right that the Supreme Court recognized in *Bartnicki v. Vopper* in 2001.

Additionally, the filmmakers contend that forcing them to pay over all proceeds from the film would be an unconstitutional restraint on speech, just as a special tax on the cost of paper and ink would violate the First Amendment rights of newspapers, even if the remedy doesn't directly prohibit speech. The filmmakers argue that forcing them to disgorge allegedly ill-gotten gains "would operate just as effectively as a use tax to check critical comments by the press on issues of public interest," which the Supreme Court has held is unconstitutional.

The filmmakers also argue that the lawsuit cannot be maintained in the federal district court in Kansas, a state which has no connection to the filmmakers or the allegedly wrongful conduct.

It's hard to imagine that the district court will ever reach the First Amendment issues raised by this case. Edwards could have a tough time convincing the court that he has standing to sue these defendants or that his claim — "constructive trust for breach of fiduciary duty" brought on behalf of the United States and the American people by an ordinary citizen — is a viable legal claim, particularly against filmmakers who played no role in obtaining the classified documents from the government.

It seems abundantly clear that the filmmakers and journalists who reported on the Snowden leaks engaged in constitutionally protected activity. Still, a contrary ruling here is scary to think about, perhaps as scary as Snowden's leaks appear to be

to Horace Edwards.

The creeping "right to be forgotten"

E.U. pushes "right to be forgotten" on U.S. search engines, claims limited effect on speech rights

By Amelia Rufer

The European Union has claimed the authority to regulate search results that appear on American servers in a November proposal regarding the 'right to be forgotten,' a proposition that is worrisome to U.S. journalists.

Under the current European privacy law, individuals can ask the European versions of search engines to remove links to information about themselves from search results. Sites like Google.uk and Google.de have been forced to comply with the requests unless the information serves a compelling public interest.

Users who want to access the delisted links are switching from European sites like Google.uk or Google.de to Google.com, which is hosted on U.S. servers.

In an attempt to stop the circumvention, Article 29 Working Party (WP29) — a committee of members from the European Data Protection Supervisor, national data protection authorities and the European Commission — proposed that individual privacy protection in the 'right to be forgotten' grants them authority to regulate search engines worldwide.

The WP29 proposal's assumption that "the impact of the exercise of individuals' rights on the freedom of expression of original publishers and users will generally be very limited," is flawed, according to Emma Llanso, the director of Free Expression at the Center for Democracy & Technology (CDT), a non-profit organization that advocates for digital rights.

"This is a vast understatement; the 'right to be forgotten' de-listing regime essentially amounts to a notice-and-takedown system where private parties can demand the removal of links to information that is, as the [Court of Justice of the European Union] recognized, true, public, and lawfully posted online," says Llanso. "Any legal framework that empowers third parties to interfere with others' access to lawful and public information necessarily raises significant freedom of expression concerns."

Under U.S. law, take-down requirements usually only follow a successful libel suit, where the information has been found to be both harmful and untrue. The current European privacy statute, which was adopted in May, applies to a much broader swath of information that an individual deems "inaccurate, inadequate,

irrelevant or excessive."

"Journalists and others who live under such a regime may only be able to find a self-selected version of a person's history," says Llanso. "It is particularly concerning that the European authorities continue to downplay the free expression concerns of this kind of government-authorized interference with the availability of lawful content, as this can serve to legitimize the censorship practices of other governments around the world."

Furthermore, by regulating what appears at the top of search results, the EU's proposal is rigging the game in a way that damages the integrity of search engines. These sites are useful to the extent that their results accurately reflect the search terms; failure to provide reliable results can prompt users to switch providers, Llanso says.

This tendency to choose a more reliable provider is the very reason for WP29's November proposal: European-Google users who switched to Google.com rendered the original statute meaningless.

"The European de-listing regime introduces an independent third party into this mix — the person who's demanding that links be removed from searches on the basis of his name — and complicates things for end-users," Llanso added. "The guidance from the Working Party 29 shows that there is still a significant divergence of opinion between the Data Protection Authorities and many journalists, researchers, academics, historians, and other free expression advocates."