FALL 2014

The News Media AND THE LAW

THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS

Reporters and Digital Security

Should encrypted communications be the standard in newsrooms?

TABLE OF CONTENTS

Published by

The Reporters Committee for Freedom of the Press

Editor Bruce D. Brown

© 2014 by the Reporters Committee for Freedom of the Press. Published four times a year. 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.

Please note that this PDF is created from our ePub version of the magazine, and is mean to be easily readable online. It is not intended primarily as a print publication.

The encryption decision

With all the relevations in the last few years about the government's snooping on communications data, what should the responsible journalist do to protect their confidential sources?

That question was the central focus of a conference organized by The Reporters Committee for Freedom of the Press, the Freedom of the Press Foundation, and New America's Open Technology Institute, held at The Newseum in Washington, D.C., on November 7.

The discussions, described more fully in the following articles, made a few things clear. To summarize: encryption is too difficult to use, scares sources when mentioned, and raises red flags for those snooping around to find the sources. But security in electronic communications is incredibly important, not just to protect sources and whistleblowers against retaliation but to protect journalistic work product from all prying eyes -- governmental and private, domestic and foreign.

Some reporters believe that electronic communications are so completely compromised that they simply cannot be used in discussions with sources. Discussions about sensitive information -- especially concerning leaks of sensitive or classified government information -- must be done in person, in parking garages and public parks and other places where meet-ups won't seem suspicious.

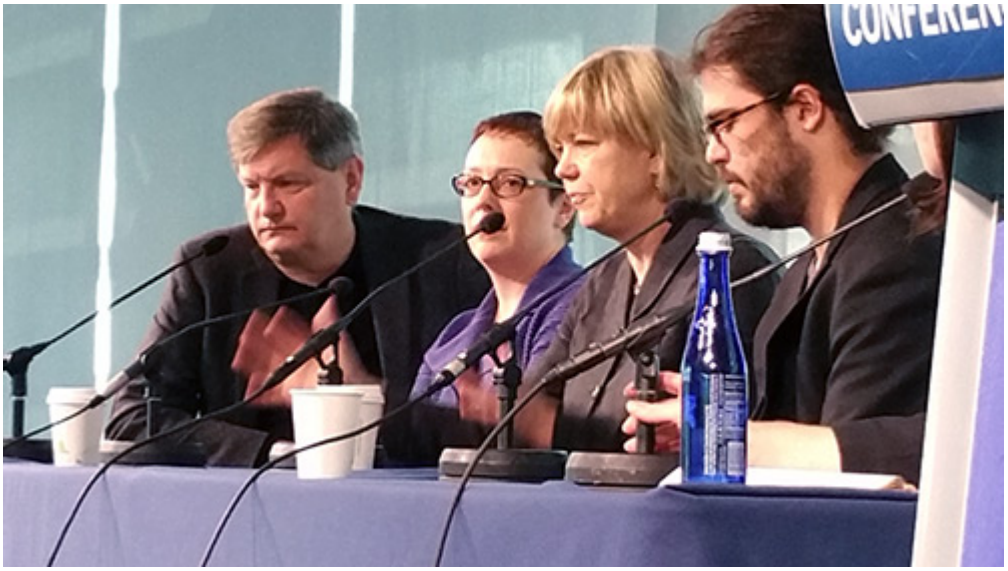
But the other view is that encryption works, and once it becomes pervasive enough that it doesn't raise flags and intimidate journalists and sources with its complexity, we'll have a workable solution for engaging with sensitive sources by electronic communications.

So how do we get to that stage? As some panelists pointed out, big media companies need to dedicate resources to digital security, so that the odd collection of open source solutions can grow into a body of professional yet easy-to-understand programs. But journalists can start using those digital solutions now (described in a sidebar to our main story), to get more comfortable with the technology. And these things have a way of snowballing; if more journalists see other journalists using encryption, they will be encouraged to adapt as well.

Of course, journalists should keep up the important tradition of meeting with sensitive sources in person. But electronic communication will continue to become more important, and journalists can start adapting to technological methods of ensuring secrecy. Hopefully, this issue of *The News Media & The Law* will help many more journalists start down that road.

Encryption: Is it enough, or too much?

And is the Snowden situation the exception, or the new rule?



James Risen of The New York Times; Julia Angwin of ProPublica; Dana Priest of The Washington Post, and Christopher Soghoian of the ACLU's Speech, Privacy and Technology Project discuss real-world encryption problems for journalists.

By Hannah Bloch-Wehba

Journalists worldwide are turning to enhanced operational security to safeguard their communications from surveillance. But panelists at the "News Organizations and Digital Security" conference on Nov. 7 emphasized that encryption-based tools, while important, are of limited utility so long as they remain uncommon and difficult to use.

Participants in a panel on "Real-World Encryption Problems" argued that, while securing electronic communications through encryption is important under some circumstances, it is difficult to convince sources to do so. Dana Priest, an investigative reporter at the Washington Post, opened by saying that her sources, many of whom have worked for the government for decades, would feel "very uncomfortable" communicating with her electronically. "I'm a low tech reporter," Priest said.

James Risen, an investigative journalist at the New York Times, agreed that trying to convince sources to use encrypted communications channels is difficult. Telling a source that he or she should use encryption because the newsgathering process can be dangerous, he said, is "not very good advertising." Even tech reporter Julia Angwin, of ProPublica, agreed that encryption is difficult for most people to use. "Most of the people I talk to on encrypted channels are cryptographers," she said.

One reason that sources often choose not to use encrypted communications channels, even when they are aware of the risk of communicating openly, is that encryption itself can be seen as a "red flag" by colleagues or investigators. All the panelists agreed that until encryption is widespread, using PGP or encrypted mobile apps will likely continue to draw unwanted attention to sources simply because they are taking extra precautions to secure their communications.

The conference, which was co-sponsored by the Reporters Committee for Freedom of the Press, the Freedom of the Press Foundation, and the Open Technology Institute at New America Foundation, was designed to bring journalists, technologists, and lawyers together to discuss journalists' security in an environment of ubiquitous metadata surveillance. Surprisingly, however, panelists at the conference emphasized that in many ways, the strategies and tactics of journalism remain traditional despite new technological threats.

Priest commented that her best practices in handling sources "have probably changed little after the revelations during the last several years." Priest, like many of the panelists, finds that the easiest way to safeguard sources is to take additional precautions in setting up face-to-face meetings. Priest noted that "instances like the Snowden documents are rare." And Risen added, "Edward Snowden is not a model for journalism. If it is, we're going to have a lot of lawyers — and a lot of problems." The documents are not the only unique aspect of the Snowden revelations. "I've never met a source who said, 'I want to leave the country and live in Moscow because this story is so important to me,'" Angwin said. "In fact, every single one of them wants to still go home and tuck their kids in at night."

But document-heavy stories like the Snowden revelations, while uncommon, are important —and risky. The problem is that the mere process of setting up clandestine in-person meetings can make sources and journalists vulnerable to surveillance. Under Section 215 of the Patriot Act, the National Security Agency collects vast troves of domestic telephony metadata on U.S. citizens. This metadata includes phone numbers and duration of incoming and outgoing domestic calls, which can reveal a good deal of reporter-source communications. Some opponents of the bulk collection of telephony metadata note that location may be collected as well, although the government has denied that it collects cell site location information pursuant to Section 215. And metadata collected pursuant to Section 215 can be used in investigations of unauthorized leaks, heightening reporters' and sources' concerns. The process of safeguarding sources becomes more complex when it is impossible to set up a meeting by phone without the fact of the initial contact being recorded.

Christopher Soghoian, a policy analyst and technologist at the American Civil Liberties Union, noted that many sources who share these concerns come to him and other users of encryption technology precisely because they worry about "conventional" journalists' exposure to risk. "During your careers, many of you have gotten phone calls out of the blue from interesting people," Soghoian said to the other panelists. "In 2014, a phone call out of the blue is too dangerous." The risky environment has resulted in a chill to sources as well as reporters, as explored in a recent report by Human Rights Watch, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy*. Sources are at risk of losing their security clearances, their jobs, and their livelihoods. Against this background, Soghoian emphasized the importance of obscuring the trail of metadata that would otherwise reveal the existence of a reporter-source relationship.

Risen's own experience aptly illustrates the pitfalls of communicating via telephone, even when the substance of the communications remains secure. In 2008, Risen was subpoenaed to identify his confidential source for a report in his 2006 book *State of War: The Secret History of the CIA and the Bush Administration*. The report dealt with an alleged covert operation by the CIA to provide Iran with flawed nuclear designs. Risen has been fighting the subpoena for over six years. In 2011, U.S. District Court Judge Leonie Brinkema quashed the subpoena. In that decision, Judge Brinkema noted that even if Risen did not testify, the government could and would rely on a wealth of telephone records of calls between Risen and his alleged source, former CIA agent Jeffrey Sterling. Judge Brinkema's decision was reversed on appeal, and the Supreme Court declined to step in. Whether prosecutors still intend to subpoena Risen is unclear, but Risen has vowed not to reveal his source.

While the problem of setting up the first contact between reporter and source is difficult to solve, the panelists agreed that the solution is not to push more communications online, even with

better technologies to secure those communications. Angwin noted that even if a message is encrypted, the record of the communication having taken place will likely still exist. Rather, panelists noted that classic journalistic methods remain vital to reporters, even those with access to the best and most usable technologies. Priest remembered that when she was attempting to set up secret meetings with sources, she would often make phone calls from other locations than her office, including law firms or universities that she happened to be visiting, in order to obscure her contacts. And face-to-face meetings remain the safest way to communicate with sources. "The cloak-and-dagger meeting in the garage is the ultimate goal. That's why we got into journalism," Angwin said.

Although many agree that the current administration is among the most hostile to the press in American history, Priest noted, "Every government tries to control information." But the atmosphere of ubiquitous surveillance is, perhaps, unique. Speaking about Watergate, Angwin said, "The fact that that secret was kept for 30 years is unimaginable in today's world. If a determined prosecutor wanted to know who Deep Throat was today, he would find him." Ironically, high-tech surveillance has shown journalists that even the most carefully encrypted communications are vulnerable to interception. Panelists agreed that the safest way to meet a source is to have an offline, coded signal: to be holding a Rubik's cube in a hotel lobby (like Snowden), or to place a flowerpot on a balcony (like Bob Woodward). Encryption helps journalists and sources maintain their relationships, but it is not a panacea; it's just one tool in the modern journalist's toolbox.

Beyond PGP

The institutional news media's approach to digital security

Panelists Jack Gillum of the Associated Press; Xeni Jardin of Boing Boing; Morgan Marquis-Boire of First Look Media, and Nabiha Syed, of Levine Sullivan Koch and Schulz discuss digital security issues with moderator Marcia Hofmann.

By Kimberly Chow

The main impediment to implementing digital security in traditional newsrooms may be that reporters avoid learning about it and news organizations don't dedicate appropriate resources to it, according to panelists at a November 7 conference cosponsored by the Reporters Committee.

The panel, composed of an Associated Press journalist, a digital security expert, a media lawyer, a digital media commentator, and a digital rights lawyer, discussed the ways that the institutional press is currently protecting its writers and the many ways it can do better.

The panel, “Beyond PGP, Protecting Reporters on an Institutional Level,” was part of the conference “News Organizations and Digital Security: Solutions to Surveillance Post-Snowden,” organized by the Reporters Committee, the Freedom of the Press Foundation, and the New America Foundation’s Open Technology Institute.

Morgan Marquis-Boire, director of security for First Look Media, framed the problem by explaining that journalists often give up on learning about the technology they could use to protect their work because they want to focus on writing.

The panelists agreed that media organizations need to do a lot more to prioritize security procedures, including providing more support to journalists from those well-versed in the technology.

Associated Press reporter Jack Gillum had two main recommendations for how news organizations can improve their institutional security. The first, he said, was that they need to "stop being cheap" and start spending the kind of money they spend on physically securing their buildings on helping their reporters be more digitally secure. The second is approaching newsgathering overall with an eye toward being secure—for example, remembering that there are many other ways besides hacking into e-mail that can reveal a reporter's trail, including public transportation data, security camera footage, and credit card information.

"We need to have this mindset of security that is beyond just the tools," Gillum said.

Nabiha Syed, a media lawyer at Levine Sullivan Koch & Schulz, LLP, said one of her main challenges is reminding journalists of all types that it is not just reporters who cover national security who need to be mindful of their data. She counsels reporters that this is an issue for "anyone who crosses a border, or anyone who does a variety of different kinds of reporting."

Gillum pointed out that there are many resources available for reporters to take control of their security.

"Since Snowden, there are more tools out there for journalists," he said. "It may be a little bit of a brainpower exercise, but there are tools."

Digital media commentator and blogger Xeni Jardin agreed, citing a "tide of public awareness" post-Snowden that showed why it was important for everyone to be mindful of these challenges.

Marquis-Boire reminded the audience that when it comes to law enforcement demanding journalists' passwords and encryption keys, there is only so much that the software can do to protect that material. Instead, he advocated a holistic organizational approach to security, apart from the tools.

"I'm really wary of trying to solve real-world coercion problems with code," he said.

Sidebar

The tools of data security

By Adam Marshall

There were several breakout sessions at the conference devoted to exploring a variety of encryption technologies and tools. These sessions were devoted to Tor (an internet anonymity and security network), Tails (a secure operating system), PGP (used for email encryption), mobile security, SecureDrop (a secure whistleblower submission system for newsrooms), and off the record internet chats. Although the Reporters Committee does not specifically endorse any, the following are some of the tools and guides mentioned at the conference:

General Guides

· *Electronic Frontier Foundation:* EFF's Surveillance Self-Defense Guide

· *Freedom of the Press Foundation:* Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance

· *Tow Center for Digital Journalism:* Resources for Source Protection

· *ProPublica:* The Best Encrypted Messaging Programs

· *TorrentFreak:* Virtual Private Network (VPN) Guide

· Terms of Service Didn't Read (summaries of terms of service agreements)

Secure Operating Systems

· Tails

Internet Anonymity and Security

· Tor

Mobile Security

· Multi-Platform: ChatSecure; Ostel

· Android only: TextSecure; Red Phone

· iPhone only: Signal

Email Encryption

· Windows: Gpg4win

· OSX: GPG Suite

Secure Chat

· Multi-Platform: Cryptocat

· Windows: Pidgin (chat client); OTR (plugin for Pidgin)

· OSX: Adium (chat client with built-in OTR support)

Whistleblower/Source Submission Tools

· SecureDrop

Standard Practices

Examining Internet, cloud storage and social networking providers

By Amelia Rufer

Before trading in the park bench for a Gmail account, journalists must decide if technology companies' terms of service are enough to protect their sources from government surveillance.

Online service providers Apple, Dropbox, Facebook, Google, Microsoft, Twitter, WordPress.com and Yahoo include policies in their terms of service that require the government to obtain a warrant for content and that promise to notify users if the government requests their information.

Since 2011, the Electronic Frontier Foundation (EFF) has evaluated online service providers based on privacy and transparency policies concerning government request for data. The 2014 edition of "Who Has Your Back" shows that technology companies are working harder to protect user privacy rights.

EFF Staff Attorney Nick Cardozo, who co-authored the report, says significant improvements in industry standards since 2013 are a reaction to Edward Snowden's NSA disclosures.

The providers who require a warrant and notify users about demands also publish transparency reports and law enforcement guidelines and defend users' privacy rights in Congress, according to the report. Additionally, all but WordPress defend those user privacy rights in the courts.

According to Cardozo, now these companies include a "binding promise" in their terms of service to alert users to data requests with the exception of gag orders and emergency situations marked by exigent circumstances.

Despite their increasing compliance with user protection policies, none of these online service providers distinguish between journalists and any other subscriber.

"They're starting to treat everybody in a fairly uniform way, partly because I doubt they are able to identify who's a journalist and who's not," said Lucy Dalglish, dean of the University of Maryland's journalism school and former director of the Reporters Committee for Freedom of the Press. "The public has spoken and these companies have decided it's good business to listen to them."

"We treat everyone as if they were the New York Times," according to Paul Sieminski, the general counsel for Automattic, Inc., which owns and operates WordPress.com. "We have the same rules for everyone."

"I think anybody that's writing and publishing on the internet, which we make easy for anyone to do, is a journalist or has a potential to be one," Sieminski added. "I would say all of our info requests are for journalists in some way."

But according to Dalglish, “These companies are not doing this because they want to help confidential sources. For them, they’re doing this because it’s better business practice. They’re going to fight but they’re not legally bound to.”

While that’s not inherently problematic, Dalglish said it does foretell how far they will go to defend user rights.

“After they exhaust the first legal processes they tell you they can do, is someone at Google going to go to jail? No, they’re not.”

The government’s habit of exercising alternative methods to the warrant — methods that carry some of the same weight as a warrant without the probable cause or judicial oversight — also raise important concerns.

National Security Letters, issued and overseen by the FBI, are one method of sidestepping these terms. NSLs cannot be used to request actual content, but they do grant law enforcement agents access to communication records.

“No judge has to sign off on them and they come with a gag order that the FBI can impose unilaterally,” said Cardozo. “We’re challenging the constitutionality of this.”

On October 8, the EFF argued *Under Seal v. Eric Holder* before the U.S. Court of Appeals for the Ninth Circuit. EFF is fighting to uphold a district court’s ruling that the Patriot Acts’ NSL provisions are unconstitutional. Cardozo said they expect a ruling sometime this spring.

According to Cardozo, Google is also fighting at least one but potentially multiple NSLs it had received.

“This case is not technically public, but there was a slip up and the filing docket was temporarily made public by mistake,” said Cardozo. The files were posted on the Internet but taken down when the parties were notified. “Google is gagged so they’re not allowed to say anything.”

Google isn’t the only service provider engaged in negotiations. In 2007, Yahoo fought an order for records from the FISA court.

“Yahoo did as much as they could’ve done. They couldn’t even talk about it until this year,” Cardozo said. “We gave them separate credit [in the report] for that fight because it was one they fought in secret; they couldn’t even take credit for it.”

Apple, Dropbox, Facebook, Google, Microsoft, Twitter, WordPress.com and Yahoo will only honor information requests that are legally binding. But legally binding requests for subscriber business records do not always come with a warrant based on probable cause. Under the Stored Communications Act, governmental entities can request a court order for customer information based on "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." An order under this provision may be accompanied by a delayed notice provision barring the recipient from notifying the user of the request.

When they are served with a subpoena or search warrant for subscriber information, these companies will usually notify the law enforcement agent that they plan to inform the user, said Cardozo.

The result is one of three scenarios: law enforcement will agree, withdraw the request or withdraw it and immediately resubmit one that includes a gag order.

“In our view, that’s exactly how it should be,” said Cardozo. “That’s the system functioning properly from our perspective.

The government can also invoke the so-called "third-party doctrine" to retrieve information that would otherwise require a warrant. The principle that information that has been disclosed to third parties like telephone companies was recognized by the Supreme Court in *Smith v. Maryland*, which upheld a lower court’s ruling that a phone company’s use of a pen register to apprehend a robbery suspect did not constitute an illegal search.

According to Cardozo, the government has stretched its application to equivocate that any data shared with a third party has no expectation of privacy, the legal justification for NSA tracking.

“We’re starting to see courts pushing back on that,” said Cardozo, who explained that the Sixth Circuit case, *United States v. Warshak*, ruled that “because there is a fourth amendment expectation of privacy, it does require a warrant to get email in all cases.”

End-to-end encryption may be a solution to government surveillance that would ease the burden on the Internet service provider. In end-to-end encryption, the content itself is encrypted—even to the company providing that communication.

“iMessage is a great example,” said Cardozo. “If you’re using iMessage from iPhone to iPhone, Apple cannot access the information from those messages, even if law enforcement comes with a warrant.”

And the same is true for FaceTime. But Apple is one of the few providers to offer such a service.

“Google is working on it. They’re not quite there, but they’re working on it,” said Cardozo, who explained that Apple is ahead of the pack because they control the software, the device and the servers. “They have complete control of the whole ecosystem.”

But Apple’s encryption has its own caveats. Cardozo said it would take the government at most about two weeks — and probably significantly less time — to access the content. Law enforcement can avoid cracking the encryption code altogether by focusing their efforts on identifying the iPhone owner’s four-digit passcode.

So while the only guaranteed solution to avoid having a service provider turn over records is not to entrust sensitive records to an outside source at all, there is progress in maintaining the confidentiality of reporters' work product held by these providers.

Open & Shut

A collection of notable quotations. Special edition: National security and data collection

Edward Snowden makes an appearance by webcam at the digital security conference.

Edward Snowden made an appearance by webcam at the "News Organizations and Digital Security" conference to talk about his experiences and what needs to happen with digital security. The talk came soon after FBI Director James Comey had said that the government wants even greater access to all communications data.

Comey, Oct. 16 speech:

"There is a misconception that building a lawful intercept solution into a system requires a so-called 'back door,' one that foreign adversaries and hackers may try to exploit. But that isn't true. We aren't seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law."

Snowden:

"We begin to enforce the Fourth Amendment not through letters on a page, but through the design of our systems."

"There actually is no real difference between a 'frontdoor' and a 'backdoor'. That's rhetoric. . . . By creating . . . backdoors in our products and services what we're doing is we're making the Internet less secure on a fundamental level."

"When FBI Director Comey asks for a 'front door,' we should remind him he already has it. It's called a warrant."

"We need journalists and institutions to look around and ask themselves: do they want to be condemned to having to fight with organizations in the intelligence community in the United States . . . just to report the news? Do we really have to fight our government to hold it to account?"

"If we don't demand answers from the government, we're not really going to get the best quality decisions and we're not really going to have the best quality government."

"The only people who know what's going on in our government right now are our enemies. And I don't think that's sustainable."

"It's not entirely about surveillance. Surveillance is the mechanism of understanding. But what we really saw was the beginning of discussion about how much the balance of power is shifting between the traditional institutions of our society — institutions such as the press, the civil society more broadly, the public — how we interact with our government."

Twitter:

“These restrictions constitute an unconstitutional prior restraint and content-based restriction on, and government viewpoint discrimination against, Twitter’s right to speak about information of national and global public concern.” — *in a complaint filed by Twitter in October against the U.S. government over compelled data collection.*

Ferguson and the right to photograph police

The summer protests shined a spotlight on coverage issues, and warned of things to come

AP Photo/Jeff Roberson

Protesters march on Nov. 23 in St. Louis, before the grand jury returned a decision.

By Kimberly Chow

While the country awaited a grand jury decision in Ferguson, Missouri, in late November, the protests following the death of Michael Brown in August served as an early reminder that members of the press can often be swept up as part of the story they are covering. As journalists vigorously covered the public unrest, many found themselves harassed or placed under arrest simply for engaging in the activity of filming or photographing the police activity around the protests. Some had guns pointed at them, and others were held overnight.

These events, as the Reporters Committee later wrote in a letter to local and state law enforcement groups on behalf of a media coalition, were "anathema to the First Amendment and to journalists everywhere." Courts have repeatedly held that the right to photograph police in the public performance of their duties is protected by the First Amendment. But it is still a regular occurrence for those who attempt to do so to be the targets of reprisal by the local law enforcement officers they are trying to monitor. Whether deficient training or heat-of-the-moment impulses are to blame, these reactions are almost predictable, and it is imperative that photojournalists know their rights. On the heels of several appellate court decisions and a recent Justice Department proclamation that the right to film the police is guaranteed by the Constitution, these rights have never been clearer.

(The Reporters Committee also released a guide on this topic, "Police, Protesters and the Press," in 2012.)

Typically, those who wish to sue law enforcement officials over harassment for filming or photographing rely on a federal statute, 42 U.S.C. §1983, which was enacted in 1871 to enforce the 14th Amendment. Section 1983 provides a private cause of action for the violation of constitutional civil rights by government actors who are acting in the scope of their employment.

Media plaintiffs usually sue under Section 1983 alleging violations of their First and Fourth Amendment rights. The First Amendment is implicated because it protects the right to speak on matters of public concern, and courts have widely held that police misconduct is a matter of public concern. The Fourth Amendment is often raised because of the unreasonable searches and seizures that take place when those who film are harassed, arrested, and have their cameras confiscated.

Courts acknowledge that these First Amendment rights can be subject to reasonable time, place, and manner restrictions. Thus, police have the right to protect themselves against actual interference with the performance of their duties.

The government defense that tends to doom many Section 1983 suits concerns qualified immunity. State actors are only liable for violations of constitutional rights that are "clearly established." If there is no controlling or persuasive authority recognizing the right, the police have qualified immunity against suit under Section 1983 for their actions that violated the plaintiff's constitutional rights. The right must be established "beyond debate," and courts examine whether a reasonable person in the government actor's position would have known that he was violating clearly established rights.

A clearly established right

Several appellate courts that have addressed the issue of whether the right to film the police is protected under the First Amendment have emphatically ruled yes. In *Glik v. Cunniffe* in 2011, the First Circuit held that "a citizen's right to film government officials, including law enforcement officers, in the discharge of their duties in a public space is a basic, vital, and well-established liberty safeguarded by the First Amendment." The *Glik* court pointed to the very brief discussions of other courts regarding the right to show that it was, indeed, "self-evident." In *ACLU v. Alvarez* in 2012, the Seventh Circuit likewise held that filming the police should be recognized as a longstanding right. The Ninth Circuit in *Fordyce v. City of Seattle*, a case involving the filming of police, also recognized a "First Amendment right to film matters of public interest" in 1995.

Yet even with courts' ringing endorsements, police continue to retaliate against those that film them. *Sharp v. Baltimore,* a case arising out of an arrest at a race track, illustrates how those filming can face immediate consequences from law enforcement officials, and how police departments in turn can face consequences as a result.

In May 2010, Christopher Sharp was spending the day at Pimlico Race Course in Baltimore, attending the Preakness Stakes horse race. When an intoxicated friend of his was arrested by the Baltimore Police Department, Sharp filmed the arrest with his cell phone. An officer approached him and said, "Do me a favor and take a walk. Now. Do me a favor and turn that off. It's illegal to videotape anybody's voice or anything else. It's against the law in the state of Maryland." Sharp twice refused when officers asked him to hand over his phone, but finally handed it over when an officer told him he needed to examine and possibly copy the video for use as evidence. When the phone was returned, Sharp found that all his video recordings had been deleted, including not only the two videos of the arrest but at least twenty personal videos as well. Sharp was stunned by the deletion, citing the loss of videos of his son at basketball games and other sentimental moments.

The case fired up First Amendment advocates, with the ACLU coming to Sharp's defense. But an unequivocally supportive — and surprisingly forceful — statement came from the U.S. Department of Justice. In a statement of interest filed in the case, the DOJ wrote, "The right to record police officers while performing duties in a public place, as well as the right to be protected from the warrantless seizure and destruction of those recordings, are not only required by the Constitution. They are consistent with our fundamental notions of liberty, promote the accountability of our governmental officers, and instill public confidence in the police officers who serve us daily." (The Department also sent further guidance for a settlement conference.)

The Baltimore Police Department ultimately settled the case with Sharp for $250,000. The DOJ statement continues to serve as a reminder that the branch of the federal government charged with executing the law of the land believes that the right to film the police is clearly established under the First Amendment.

The need for better training

A rash of recent cases involving filming the police, however, underscores the reality that — until supervisors and courts get involved — whether the photographer gets harassed or arrested is entirely up to the officer at the scene.

Datz v. Milton is illustrative of cases in which a police department ultimately has to answer for its longstanding practice of denying photojournalists access to the areas where other members of the public can observe police activity. The 2012 case, brought in the Eastern District of New York, involved a Suffolk County, Long Island police officer refusing to allow Datz, a professional photographer, to film a scene of police activity from a public sidewalk where other bystanders were watching, and then proceeding to arrest him after Datz moved a distance away to film.

Datz could already recount a plethora of other instances when Suffolk County officers had refused to let him film from public areas, told him they were extending crime scenes so that he would have to leave and then not actually done so, or driven police cars back and forth to obstruct filming. But on July 29, 2011, he found himself actually under arrest merely for doing his job. An officer charged over to him while he filmed on the sidewalk, grabbing his press lanyard and telling him to "go away" but not specifying an alternate location despite Datz's requests. When Datz drove away and resumed filming 500 feet from the police activity, the same officer drove his squad car directly toward him at high speed, stopping just in front of him. He then confiscated Datz's camera and arrested him. He was charged with "obstructing governmental administration."

Among the indignities Datz suffered, including an injured shoulder, was the withholding of the tape in his camera, which contained time-sensitive footage of other events of the day that he had intended to sell for use on that evening's news. By the time he got the tape back, the footage was useless.

The Suffolk County District Attorney voluntarily dismissed the charge against Datz on August 9, 2011. A suit followed, with Datz ultimately receiving a $200,000 settlement from the police department, as well as a commitment that the department would institute media relations training for its officers and form a media relations committee.

Robert Balin, an attorney at Davis Wright Tremaine who represented Datz, said he and his client were extremely pleased with the settlement, particularly the actions that the police department took in response to the case.

"They changed their policies to specifically recognize that there is a First Amendment right that is held by the public and the press to record police activities that occur in public places," he said. "Now their rules and procedures prohibit officers from interfering with that right."

Those new policies, combined with the increased training and awareness among officers of the right, are necessary parts of the solution, Balin emphasized.

"Ultimately it's not just about winning the case—it's about changing the culture," he said.

It is the training component that is critical, said Mickey Osterreicher, general counsel of the National Press Photographers Association.

"It doesn't really matter whether journalists know what their rights are if police don't know about or understand or respect those rights," he said. "Police departments can have policies, but if they don't have proper training, if they don't have appropriate discipline when people violate those policies, then the policies are just pieces of paper."

The road ahead

Osterreicher said he believes that the number of courts recognizing the right to film the police as clearly established has passed a "tipping point." With widespread acknowledgement of the right, it is possible that increasing numbers of people who are prevented from filming and who are arrested will sue police departments, he said.

A case this year from Texas, *Buehler v. City of Austin*, is an example of the growing recognition. Antonio Buehler was arrested several times for filming the police during arrests and traffic stops, sometimes violently and with verbal abuse. After he brought suit against the city and the police department, the trial court held that the police could not claim qualified immunity because the right to film the police was clearly established in the Fifth Circuit. It remains to be seen whether the defendants will appeal.

As the tense situation in Ferguson continues to unfold and as the ubiquity of camera phones means that anyone can record, these confrontations will continue. Osterreicher has a number of recommendations for what to do when the police demand that filming stop, including trying to assert one's rights if the officer seems receptive, asking to speak to a supervisor, asking if there is an alternate location from which to film, keeping the camera rolling during the encounter to document any violations, and working in pairs so the other partner can continue to film.

On a larger scale, Balin said he expects that cases will keep moving forward and more and more appellate courts will recognize the right to film as clearly established. In particular, he said, he hopes the Second Circuit will hear a case soon and clarify the right in that jurisdiction. For now, photographers will have to keep trying to do their jobs in what can be a hostile environment.

"I wish there were fewer Fergusons, but I recognize that for every police department that is starting to do it right, there are still plenty that need to be prodded forward," Balin said. "These kinds of lawsuits are not going to go away, at least in the foreseeable future."

First step in unsealing court records: try asking

Sometimes a simple letter from a reporter will prompt a court to disclose sealed documents

By Tom Isler

Sometimes, it's amazing what you can get if you ask nicely.

Last month, judges in two different courts unsealed records in response to informal letter requests from journalists — not formal motions prepared by lawyers. The Reporters Committee for Freedom of the Press similarly caused documents to be unsealed last year after sending a letter to the clerk of the U.S. Court of Appeals for the D.C. Circuit, asking that the court to publicly explain its decision to seal a docket in an appellate case.

These are encouraging results for journalists or news organizations that do not have the resources to hire a lawyer every time they want secret court documents to be made public.

On October 8, 2014, Kyle Whitmire, a political commentator for the Alabama Media Group, sent a two-sentence letter to Family Court Judge Anita L. Kelly in Montgomery, Ala., requesting that she unseal the divorce records for U.S. District Judge Mark E. Fuller, who was arrested this summer on misdemeanor domestic battery charges.

The divorce file had been sealed in 2012 without a published opinion or order and over the objection Judge Fuller's then-wife, Lisa Boyd Fuller, fueling speculation that the file might contain evidence of other domestic violence incidents. It was known at the time that Ms. Fuller, in the course of litigation, had asked Judge Fuller to confirm or deny whether he had physically abused her.

"Court records in divorce cases are typically public documents," Whitmire wrote to Judge Kelly, "and we believe, in light of recent events involving U.S. District Judge Mark Everett Fuller and the criminal charges that he faces, it is in the public's interest that these documents in this court file again be open to public inspection."

Nine days later, Judge Kelly held a hearing about the documents, at which time Judge Fuller's lawyer consented to the file being unsealed. The divorce file, however, did not contain evidence of prior domestic violence, according to news reports.

A similar approach worked for reporter Charlie Savage of *The New York Times*, who, in August, urged Judge Royce C. Lamberth of the U.S. District Court for the District of Columbia to unseal grand jury materials related to a subpoena issued to reporter Mike Levine.

In 2011, the Justice Department sought to force Levine, then a Fox News reporter, to reveal his confidential sources for a July 2009 story that "several Somali-Americans were secretly indicted in Minneapolis for joining an al Qaeda-linked group in Somalia." Levine resisted the subpoena for 16 months, before the Justice Department decided to drop the matter.

To get the documents unsealed, Savage composed an e-mail to Judge Lamberth's administrative assistant, including a request for the judge to release any documents related to Levine's motion to quash the subpoena.

Savage didn't actually know that Levine had filed a motion to quash or that the court had denied the motion. He inferred the chain of events from the facts that Levine avoided testifying for so long and the Justice Department voluntarily withdrew its subpoena, rather than being told by the court to stop pursuing Levine.

Savage argued to Judge Lamberth that the documents were important historical records of an era of unprecedented leak prosecutions.

"As you are no doubt aware, the current administration has brought criminal charges in eight leak-related cases to date, compared with three under all previous administrations," Savage wrote. "One of those eight cases, involving the former C.I.A. official Roger Sterling, involves a subpoena to a reporter, James Risen, and has led to some groundbreaking litigation regarding the scope and limits of First Amendment protections for reporters . . . ."

He continued: "I submit that a careful release of the presumed litigation before you, with appropriate redactions to protect identity of the target or targets, would be both consistent with the legal policy purpose behind grand jury secrecy rules while also improving public understanding of this era and the important issues raised by it."

A few months later, Judge Lamberth unsealed the documents, with some redactions, after consultation with the parties.

Neither Whitmire's nor Savage's letter cited any legal precedent in support of his request, but both attempted to explain why the public could benefit from disclosure.

The Reporters Committee achieved similar results last year, after writing a letter to the clerk of the D.C. Circuit to inquire about an appellate docket that had been sealed in its entirety. The case appeared to involve a dispute between prosecutors and Jeffrey Thompson, a District of Columbia resident who was being investigated for allegedly financing an illegal shadow campaign in support of D.C. Mayor Vincent Gray, in violation of financial disclosure laws.

The parties appeared to be fighting about sealing or redacting documents seized from Thompson by federal investigators. The district court, in a sealed opinion, gave the parties 20 days to suggest redactions, and, later, issued a redacted memorandum and order that explained the redaction process. Thompson appealed, and the D.C. Circuit dismissed the appeal in an order that was, itself, sealed.

The Reporters Committee wrote to the clerk to ask "that in matters requiring sealing the Court issue orders on sealing and redaction separately from orders on the merits" so that the public can be better informed of the work of the court. The letter also requested that if the court intended to keep the materials under seal, the court place an order on the public docket justifying secrecy.

In a subsequent order, the D.C. Circuit said it construed the letter as a motion to intervene in the lawsuit and as a motion to unseal some of the court records, even though the Reporters Committee did not expressly ask to intervene. The court then ordered the parties to suggest redactions to its previous opinion, which they did, and the court later unsealed a redacted version.

Despite these successes, the strategy doesn't always work. In fact, in 2012, Judge Kelly in Alabama ignored a previous informal letter from journalists to unseal Judge Fuller's divorce case.

Whether a simple letter request will be successful will depend on the circumstances of each case, including the nature of information under seal, the length of time the material has been sealed, whether justifications for secrecy continue to exist, and whether the material was properly sealed

in the first place. In addition, a lot will depend on the individual judge, who may be more or less devoted to principles of transparency, or who may prefer journalists to follow formal procedures.

But when there aren't any other options, simply asking the court for disclosure may just do the trick. And because it should not affect the ability of a news organization to later formally intervene, there's almost nothing to lose by trying.

Agencies want to know: Are you still interested?

Federal agencies want to clear their FOIA backlogs by forcing requesters to restate their interest

By Adam Marshall

Before we begin the time-consuming review process, we want to ensure that you are still interested in continuing the processing of this request. Please indicate your continued interest in pursuing these records within 7 days from the date of this letter, or we will assume you are no longer interested in this FOIA request, and the case will be administratively closed.

-- A 2013 letter from the Federal Emergency Management Agency (FEMA)

Federal agencies want to know: "Are you still interested" in open government?

The Freedom of Information Act (FOIA), passed in 1966, brought the promise of an open government where anyone could request information from federal agencies. Nearly 50 years later, backlogs, miscommunications, and insufficient resources hinder the ability of the media to obtain important information from the government in order to inform the public. But now, there's another factor that requesters need to contend with: agencies seeking to close FOIA through a controversial tactic whose legality remains unclear.

They're called "still interested" letters. These letters, sometimes mailed, sometimes emailed, are sent to FOIA requesters to ask whether they are "still interested" in having their request processed. They indicate that if a response is not received within a certain number of days, the request will be administratively closed.

"It was surprising to get the letter", says Matt Drange, a reporter with the Center for Investigative Reporting, who received such a letter from the Department of Justice regarding a FOIA request that had been unanswered for nearly a year. Drange hadn't heard anything in a while from Justice, despite making repeated inquiries about his request. Then, out of the blue, the letter arrived, demanding a response within ten days or else his request would be closed.

Although it is not exactly clear what happens when a FOIA request is closed in such a manner, presumably a new request would have to be filed in order to get the information that was originally sought. This would put the requester at the end of the agency's processing queue, despite the fact that the requester may have been waiting for months, if not years, for a response from the agency.

Many "still interested" letters concern FOIA requests that have been pending for some time. An article in this magazine from 2012 noted that a request sent in 1993 by Monte Finkelstein, a professor at Tallahassee Community College, produced a "still interested" letter in April 2011. But other letters have targeted requests that are hardly old at all, at least in the FOIA world. Amy Bennett, Assistant Director at OpenTheGovernment.org, said that she received such a letter in regard to a request she had filed just three months earlier.

An increasingly common phenomenon

The purpose of "still interested" letters seems to be aimed at reducing the backlog of pending FOIA requests, which decreased during the first few years of President Obama's administration but has recently increased in certain departments. Data from the Department of Homeland Security (DHS) reveals that its FOIA backlog nearly doubled in fiscal year 2013 to over 50,000 outstanding requests. As a whole, the federal government had more backlogged requests in 2013 than at any other time since 2008.

Use of "still interested" letters seems to be on the rise. Brad Heath, an investigative journalist at *USA Today* who makes frequent use of FOIA, says he doesn't remember getting "still interested" letters seven or eight years ago, but now gets one every month or so. Bennett shares Heath's experience: "It definitely seems to be something that agencies are embracing more," she said.

The increased use of "still interested" letters in recent years may not be a coincidence. An Executive Order issued by President George Bush in 2005, parts of which were codified into law in 2007, requires agencies to find ways to increase efficiency in processing FOIA requests and to report how long such processing takes each year. While the changes were intended to help improve FOIA response times, journalists and open government advocates are increasingly worried that there may be unintended side effects.

"If you look at the timing of when these letters come out, it's all driven around reducing backlog," Bennett said. "It's a sneaky way to make the agency's numbers look better." Several journalists and open government advocates contacted by the Reporters Committee noted that many "still interested" letters seem to arrive close to September 30, the end of the government's fiscal year.

In fiscal year 2010, the U.S. Department of Health and Human Services (HHS) received nearly 64,000 FOIA requests, 46,586 of which were directed to the Centers for Medicare & Medicaid Services (CMS). That year's FOIA report indicates that CMS administratively closed 11,652 FOIA requests "based on response and non response to continued interest calls and correspondence." The report does not include data that indicate the number of FOIA requests closed due to a lack of response. But by administratively closing more than 11,000 FOIA requests, CMS and HHS were able to report that they had processed more requests in 2010 than they had received, and thus reduced their backlog. CMS did not respond to inquiries made by the Reporters Committee.

Timing and delivery

For FOIA requesters, "still interested" letters are not always easy to spot, and they can come at inopportune times. Drange had a near miss with his letter from Justice, which he received just after returning from a vacation. "I couldn't help but think what if I had been out [of the office] when I got it," he said.

That's precisely what happened with a letter sent to Heath. Upon returning from vacation, Heath discovered that he had received a letter from a federal agency asking if he was still interested in the FOIA request he had filed with them. He had already missed the response window, so his request was administratively closed. "You've got to be kidding," Heath recalled thinking upon reading the letter.

Even more worrying is the communication that isn't received. A FOIA request sent to the General Services Administration (GSA) in April 2014 by Scott Amey, General Counsel at the Project on Government Oversight (POGO), was administratively closed in June. POGO only found out about the closure of its request in November after making a routine status call to the GSA. According to POGO, the GSA said that it sent a "still interested" email in June, requesting clarification of two minor points in their request within nine days or else it would be closed. However, POGO says it never received the email, or any other notification from the GSA that its request had been closed.

A GSA spokesperson did not respond to a request for comments by the Reporters Committee.

Uncertain legality

Part of the reason that questions about the procedures and legal effects of "still interested" letters are on the rise is that the legality of the practice remains unclear. There is no provision in the Freedom of Information Act that authorizes, or even contemplates, such a practice. Kirsten Mitchell, a Management and Program Analyst at the Office of Government Information Services (OGIS) who formerly worked at the Reporters Committee, said that "still interested" letters haven't been addressed in any FOIA regulations she has reviewed.

In October 2014, a coalition of open government and transparency groups sent a letter to OGIS requesting an investigation into the practice and its impact on FOIA requesters. The letter noted that using "still interested" letters "runs the risk legitimate FOIA requests will be improperly closed because the requester fails to respond within an arbitrary time period the agency has imposed."

The letter from the coalition included examples of "still interested" letters that had been sent from various components of DHS (among other departments), including the Transportation Security Administration (TSA), the Secret Service, and the Federal Emergency Management Agency (FEMA).

There is no provision in the DHS regulations implementing FOIA that allows for an administrative closure based on a lack of response to a "still interested" letter. A spokesperson for DHS referred questions on the use of "still interested" letters to the Justice Department, which did not respond to questions from the Reporters Committee.

A 2012 memorandum from Jonathan Cantor, Acting Chief FOIA Officer for DHS, directs its FOIA officers to adhere to guidance from the DOJ's Office of Information Policy on "still interested" letters. The DOJ's website states that "[w]hen done judiciously, [still interested letters or phone calls are] entirely appropriate because agency resources should not be expended on processing a request when the requester is no longer interested in the records." The guidance also states that agencies should "afford requesters a reasonable amount of time to indicate their continued interest."

"Still interested" letters reviewed by the Reporters Committee varied widely in the amount of time they afforded a requester to respond. Many agencies gave 10-15 days, but one letter sent by FEMA gave just seven days to respond – with no indication as to whether it was seven business or calendar days.

Mitchell stressed that the OIP guidance states that agencies need to give a "reasonable" amount of time for individuals to respond, but wasn't yet ready to state how many days should be considered reasonable. She did note, however, that if such a letter is mailed to a requester, not giving enough time to respond could be problematic. "When you think about it," she says "first it has to get out of the agency, then it has to get through the U.S. Mail, then if the requester is mailing [a response] it has to get back to the agency, and then back to the correct component of the agency."

It's no secret that federal FOIA offices have limited resources, and FOIA requesters understand why agencies might resort to "still interested" letters in an effort to reduce their backlog. Bennett says that "no one in the FOIA world wants agencies wasting resources going through records that no one wants any more, but to close a request in this way is not the right way to go about it."

Heath agrees: "It makes a certain amount of sense", he says, but the "meet our deadline or else" tactic, especially after the agency has failed to comply with its statutory and regulatory deadlines, isn't fair.

One suggestion that was fairly common among the journalists and open government advocates interviewed is to reverse the default result that follows from a lack of a response to an agency letter. Under this proposed practice, a FOIA request would only be administratively closed if the requester affirmatively responds that they are no longer interested in their request, instead of the agency closing it if no response is received.

Tips for journalists

According to Mitchell, OGIS is going to be looking into the use of “still interested” letters by agencies. She noted that in addition to the examples provided in the October letter from open government advocates, other individuals have independently contacted the oversight office to complain about the practice.

Until something changes with regard to these letters, there are some practical steps that journalists can take to avoid running afoul of agency-imposed deadlines. Drange says that he keeps a spreadsheet of all his FOIA requests that contains important information, such as the date it was sent, the date a determination is due, FOIA officer contact information, and more. He says journalists have to be persistent in following up with the government and always on the lookout for correspondence. (Journalists using the Reporters Committee's free iFOIA service can also track their requests through that system.)

Even if a request is closed, it might be possible to have the request reopened. Heath noted one instance in which he had some limited success getting an agency to reopen a request that was administratively closed (only to have it frustrated in other ways). He also says that when he responds to a “still interested” letter he always includes a paragraph admonishing the agencies for the practice in the hope that someone will listen.

Mitchell says that two-way communication between agencies and requesters is key when it comes to all FOIA requests. “It’s really about keeping the lines open.”

Asked & Answered

Q: I submitted an open records request, but now the (federal/state/local) government entity says it's going to cost a lot of money for me to get the records. Is there anything I can do?

A: The best way to avoid paying fees for an open records request is to make sure you address the issue before submitting your request. When filing an open records request to a federal, state, or local government entity as a journalist, the best practice is to include a request for a fee benefit and/or fee waiver in your initial communication to ensure that it can be considered from the start.

Under the federal Freedom of Information Act, in order to get a fee benefit (meaning you'll only be charged for duplication fees), all you need to show is that you're a "representative of the news media." This is usually fairly easy to prove, as the definition is quite broad. In addition to established media organizations, it is possible for both freelancers and bloggers to qualify for news media status.

In order to get a waiver of all fees at the federal level, you need to argue that (1) the information you're seeking is in the public interest because it will contribute to public understanding of the operations or activities of the government, and (2) it is not primarily in your commercial interest. There may also be agency-specific regulations that you can look to for additional guidance.

Fee provisions in state open government laws vary greatly. Some are based on the federal FOIA, while others have no provisions for fee benefits or waivers at all. You should research your state's open government law before making a request to determine what benefits may be available to you.

Even if your state doesn't have a provision that allows journalists to receive records at a reduced cost, you can always argue that no fees should be assessed in your case. Many states do not require the government to charge fees for copies of records, and agencies are often allowed to waive fees at their discretion. In these situations, it is helpful to identify yourself as a member of the news media and explain why the information you are seeking is in the public interest.

If you've already filed an open government request without including a request for a fee waiver or benefit, you can try responding to the fee estimate with an argument that it should be waived or reduced because you are a member of the media and it's important for the public to have access to the information. While there is no guarantee that the government entity will agree with you, many are willing to work with requesters who present good faith arguments.

Regardless of what stage of the process you are in, make your arguments convincing to someone who isn't familiar with the subject of your story. If possible, include links or citations to other stories or information that illustrates the importance of the subject.

If you can't secure a fee benefit or reduction, ask for a breakdown of the costs from the government. Compare this to your jurisdiction's laws and regulations to ensure that each category of fees is permitted to be charged. For example, some jurisdictions are allowed to charge fees for copying records, but not for searching for them. It may also be beneficial to determine who is going to process your request. Some jurisdictions have provisions limiting the hourly rate for persons who process open government requests.

Finally, if all else fails, consider narrowing your request if the fees are prohibitively high. You can contact the governmental entity to try and identify a more specific search query, which should lead to fewer responsive records, and therefore lower costs.