SEARCH WARRANTS AND JOURNALISTS:

A GUIDE FOR THE PERPLEXED

Compiled by the First Amendment Foundation and Freedom of the Press Foundation for print, web and broadcast newsrooms across America

August 2023

As we've seen from recent law enforcement raids on the Marion County Record in Kansas and the home office of Timothy Burke in Tampa, local police and federal agents seem all too willing to brush aside the law when it comes to executing search warrants on journalists that lead to seizures of documents and equipment like computers, hard drives and phones.

So what should reporters and newsrooms do to prepare for the unthinkable? How should you and your colleagues behave if officers arrive on your doorstep? What do you say?

To help answer that Florida's First Amendment Foundation and Freedom of the Press Foundation, building on previous efforts of others in earlier years, including the law offices of McGuire Woods, Thomas and LoCicero, as well as the Student Press Law Center, have created this short guide to help you if you ever find yourself staring at a warrant.

It is broken into four topic areas: the first is a brief pragmatic 10 step guide of what to do if law enforcement shows up at your newsroom or residence with a warrant. The second is information on using encryption to protect your most important files and source contacts. The third is a primer on the provisions of the 1980 Privacy Protection Act. And the final section is about state shield laws, using the Florida Shield Law as an example.

As we have seen in recent cases, the suspicion that a journalist has committed a "crime" may cause local law enforcement officers and federal agents to unthinkingly sweep these protections aside, even though they shouldn't. This guide will help you be prepared to respond if that happens.

We hope this is helpful,

Bobby Block (FAF), Seth Stern (FPF), and FPF's Digital Security Training team.

PART I:

THE 10 THINGS JOURNALISTS NEED TO DO IF POLICE COME KNOCKING ON YOUR DOOR

1. The most important first step is to be prepared well before a police action. Know that there's a federal statute called the Privacy Protection Act of 1980 (PPA) that requires law enforcement to get a subpoena, not just a search warrant when dealing with reporters and newsrooms. Subpoenas give you the opportunity to challenge a demand for your documents or equipment in court *before* police can seize them. There are narrow exceptions to the PPA's subpoena requirement, including when "there is reason to believe the journalist is taking part in the underlying wrongdoing." However, in general, the wrongdoing cannot relate to the receipt, possession, communication, or withholding of newsgathering materials or information.
2. Inform your staff and colleagues about the provisions of the PPA and make sure they have copies. (See Section III.) With remote work situations, it's increasingly likely that a warrant will be executed at a journalist's home so they should keep a copy ready at their residences too.
3. If law enforcement appears with a search warrant, don't panic! If possible, begin recording your interaction with the police. Don't get into a shouting match. Maintain a professional demeanor. Ask to see the warrant and the officer's identification. Immediately call the publisher or top editor available and ask them to come up. Tell the officers what you are doing, and tell them your boss is on the way. Firmly but politely ask the officers not to begin the search until your boss arrives.
4. Have your boss call your lawyer ASAP. If your boss can't, the reporter should call right after informing the senior editor. Make sure all reporters and relevant staff have your lawyer's contact details. Email or text a copy of the warrant and the citation for the Privacy Protection Act (42 U.S.C. Section 2000aa, et seq.) to your lawyer so that they can pull the statute quickly and familiarize themselves with the warrant.
5. The publisher or editor should mention the PPA, give the officers a copy of it and tell them the search should be delayed until your

lawyer arrives. They should point out that the PPA provides for sanctions against officers who search newsrooms in violation of the act. That might slow them down. Also, do inform police that they are seeking materials intended to be published or broadcast. This is important because it puts police on notice about prior restraint and could be essential in any lawsuit challenging the seizure. Wearing press credentials or carrying camera/video can help let police know that the notice is from members of staff.

6. Read the warrant slowly and carefully to see exactly what it permits. It should list specific items that can be seized.
7. Don't do anything to destroy or hide records. Don't get into a physical altercation of any sort. BE PROFESSIONAL.
8. If the search proceeds:
    - Get cameras rolling (actually, get them rolling the second law enforcement arrives).
    - Warn officers when they are intruding on confidential information. Be clear and document your warnings by taking notes indicating what was said, by whom, and when, just in case the recording doesn't capture all the details . Be particularly sensitive to protecting confidential sources.
    - Be conscious of what the warrant permits and clear when they're intruding beyond the parameters of the warrant. Continue to document all that happens and your warnings.
9. You should not impede the search, but you don't have to facilitate it either. That said, you might want to avoid having your premises ransacked. If the warrant is limited, you might choose to direct officers to the materials specified in the warrant to limit their search of your newsroom and protect as much information as possible.
10. If the search is by federal agents (as opposed to state or local police), there are regulations that require the U.S. Attorney General to approve the search. (28 CFR Part 50). You should ask to see if that approval was properly given -- or not -- and advise your lawyer.

PART II.

A CASE FOR ENCRYPTION

In a video recording of the police raid on the Marion County Record's offices, officers can be overheard discussing whether it is safe for them to switch off a computer. One officer can be heard saying: "I don't believe this is encrypted, so I think we're okay."

Encrypted laptops and phones are far more difficult and time-consuming for officers to search without your permission. When your devices are unencrypted, law enforcement can easily access your sources, notes and most sensitive data.

Here's what you can do to encrypt your devices. It'll make the lives of officers who illegally seize them more difficult and could buy you time to file legal challenges before it's too late.

A) Cellphones:

If you have an up-to-date iPhone or Android phone, your device is encrypted by default, just by having a password. Make sure your password isn't easy to guess (for example, your name or the name of your news outlet). A longer combination of non-recurring numbers, letters and special characters is better.

Older Android devices may not be encrypted by default, but you can check by going to your Settings app and looking under security settings for "disk encryption" or device encryption.

To learn more, you can review FPF's guide to securing your smartphone as well as its guide on what to do if your phone is seized by police.

B) Desktop and laptop computers:

Unlike your phone, your computer likely does not have encryption enabled by default so you'll need to enable it manually. On macOS you can enable device encryption in your settings using FileVault. On Windows, you can enable device encryption with BitLocker. The password and recovery code needs to be stored somewhere safe, like in a password manager like 1Password (discussed more below).

It's important to note that many types of device encryption are only activated when the device is fully turned off. If you have advanced notice that a search will occur, turn your phone or computer all the way off to sufficiently protect it with encryption — don't just put it to sleep. If you don't have notice, it may not be possible for you to turn your phone or computer off before police begin the search.

The longer and more random a password you have, the better. Many experts recommend a password manager, which can generate and store your passwords. 1Password is free to newsrooms under the 1Password for Journalism program.

Don't write down your passwords and keep them in the newsroom. Officers may be able to seize notes with your passwords and use them to access your devices. If you must write down your passwords, keep them secured away from the newsroom.

C) Backups

To minimize disruptions to your newsrooms from overzealous law enforcement officials, not to mention natural disasters and power surges, it is important to create and maintain several backup drives in more than one physical location. This will limit loss as well as help you inventory your files in case these devices are ever seized (or otherwise lost or damaged).

One of the easiest ways to make a backup on your own external hard drive is with Apple's built-in Time Machine tool on macOS, as well as Backup and Restore settings on Windows.

On Apple devices you can also make end-to-end encrypted backups using Apple's iCloud Advanced Data Protection mode, meaning even Apple can't read them.

Unfortunately, Windows machines do not have an end-to-end encrypted option at this time, making them vulnerable to legal requests.

D) Handwritten notes

In the raid on Timothy Burke's home office in Tampa in May, FBI agents seized some notebooks as well as computers, phones and hard drives. To help secure this information as well as to maintain a copy for yourself, it is worthwhile to store individual files and folders as well as photos of handwritten notes of important interviews and source data on USB storage devices that can be encrypted as well. For example, Windows users can use BitLocker To Go to encrypt external USB drives and macOS users can encrypt USB storage with Disk Utility. All major desktop operating systems support Veracrypt. Check out FPF's guides on picking which encrypted USB storage option works best for you.

Part III.

THE PRIVACY AND PROTECTION ACT OF 1980

The Privacy Protection Act of 1980 was passed in response to *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), which upheld broad law enforcement access to a newspaper's files. The PPA establishes procedures for law enforcement seeking access to records and other information from the offices and employees of a media organization. In general, it prohibits both federal and state officers and employees from searching or seizing journalists' "work product" or the "documentary materials" in their possession. Under the Act, in order to gain access to journalists' information, law enforcement must obtain a court subpoena, rather than a simple search warrant. Note that the PPA does not only apply in full-scale raids like what happened in Marion and Tampa but also in smaller scale searches and seizures of journalists' equipment (like seizures of phones from reporters arrested during protests).

Quick summary

- It is "unlawful" for law enforcement — including federal, state, and local law enforcement — to search and seize materials from journalists in connection with a criminal investigation or prosecution.
- There are two types of information protected (1) "work product materials" and (2) "documentary materials."
- "Work product materials" are items created or possessed for the "purpose of communicating such materials to the public" (whether published or not), such as drafts of articles, other newsgathering materials, video, or notes.
    - These can be searched or seized only if (1) there is probable cause that the journalist has committed or is committing a criminal offense which the materials relate to, *not including* offenses based upon the receipt, possession, communication, or withholding of materials or information contained in materials, unless such information relates to national defense, classified information, or restricted data, or (2) the seizure is

necessary to prevent the death or serious bodily injury of a person.

- "Documentary materials" are "materials upon which information is formally recorded," such as photographs or audio and visual recordings.
    - These can be searched or seized (1) for the same reasons as work product materials, (2) if serving a subpoena for the materials "would result in the destruction, alteration, or concealment" of the materials, or (3) if the materials have not been turned over in response to a court order directing compliance with a subpoena.
- Journalists can sue both the officer's employer and the officer personally in federal court to recover damages and attorneys' fees. The minimum statutory award is $1,000.
- Although the PPA generally prohibits the search and seizure of work product and documentary materials, it doesn't prohibit law enforcement from accessing these materials altogether. Rather, it requires police to obtain a *subpoena*, not a search warrant, to access work product and documentary materials. You may have other defenses to a subpoena for your work product and documentary materials, such as your state shield law.

<u>Here is the law in full from the DOJ's Website:</u>

§ 2000aa. Searches and seizures by government officers and employees in connection with investigation or prosecution of criminal offenses

a. Work product materials

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability

of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if--

1. there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or 798 of Title 18, or section 2274, 2275 or 2277 of this title, or section 783 of Title 50); or

2. there is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being.

b. Other documents

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize documentary materials, other than work product materials, possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if-

1. there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not

search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or 798 of Title 18, or section 2274, 2275, or 2277 of this title, or section 783 of Title 50);

2. there is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being;

3. there is reason to believe that the giving of notice pursuant to a subpena duces tecum would result in the destruction, alteration, or concealment of such materials; or

4. such materials have not been produced in response to a court order directing compliance with a subpena duces tecum, and--

    A. all appellate remedies have been exhausted; or

    B. there is reason to believe that the delay in an investigation or trial occasioned by further proceedings relating to the subpena would threaten the interests of justice.

c. Objections to court ordered subpoenas; affidavits

In the event a search warrant is sought pursuant to paragraph (4)(B) of subsection (b) of this section, the person possessing the materials shall be afforded adequate opportunity to submit an affidavit setting forth the basis for any contention that the materials sought are not subject to seizure.

§ 2000aa-5. Border and customs searches

This chapter shall not impair or affect the ability of a government officer or employee, pursuant to otherwise applicable law, to conduct searches and seizures at the borders of, or at international points of, entry into the United States in order to enforce the customs laws of the United States.

§ 2000aa-6. Civil actions by aggrieved persons

a. Right of action

A person aggrieved by a search for or seizure of materials in violation of this chapter shall have a civil cause of action for damages for such search or seizure--

1. against the United States, against a State which has waived its sovereign immunity under the Constitution to a claim for damages resulting from a violation of this chapter, or against any other governmental unit, all of which shall be liable for violations of this chapter by their officers or employees while acting within the scope or under color of their office or employment; and

2. against an officer or employee of a State who has violated this chapter while acting within the scope or under color of his office or employment, if such State has not waived its sovereign immunity as provided in paragraph (1).

b. Good faith defense

It shall be a complete defense to a civil action brought under paragraph (2) of subsection (a) of this section that the officer or employee had a reasonable good faith belief in the lawfulness of his conduct.

c. Official immunity

The United States, a State, or any other governmental unit liable for violations of this chapter under subsection (a)(1) of this section, may not assert as a defense to a claim arising under this chapter the immunity of the officer or employee whose violation is complained of or his reasonable good faith belief in the

lawfulness of his conduct, except that such a defense may be asserted if the violation complained of is that of a judicial officer.

d. Exclusive nature of remedy

The remedy provided by subsection (a)(1) of this section against the United States, a State, or any other governmental unit is exclusive of any other civil action or proceeding for conduct constituting a violation of this chapter, against the officer or employee whose violation gave rise to the claim, or against the estate of such officer or employee.

§ 2000aa-7. Definitions

a. "Documentary materials", as used in this chapter, means materials upon which information is recorded, and includes, but is not limited to, written or printed materials, photographs, motion picture films, negatives, video tapes, audio tapes, and other mechanically, magnetically or electronically recorded cards, tapes, or discs, but does not include contraband or the fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or which is or has been used as, the means of committing a criminal offense.

b. "Work product materials", as used in this chapter, means materials, other than contraband or the fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or which is or has been used, as the means of committing a criminal offense, and--

1. in anticipation of communicating such materials to the public, are prepared, produced, authored, or created, whether by the person in possession of the materials or by any other person;

2. are possessed for the purposes of communicating such materials to the public; and

3. include mental impressions, conclusions, opinions, or theories of the person who prepared, produced, authored, or created such material.

c. "Any other governmental unit", as used in this chapter, includes the District of Columbia, the Commonwealth of Puerto Rico, any territory or possession of the United States, and any local government, unit of local government, or any unit of State government.

§ 2000aa-11. Guidelines for Federal officers and employees

a. Procedures to obtain documentary evidence; protection of certain privacy interests

The Attorney General shall, within six months of October 13, 1980, issue guidelines for the procedures to be employed by any Federal officer or employee, in connection with the investigation or prosecution of an offense, to obtain documentary materials in the private possession of a person when the person is not reasonably believed to be a suspect in such offense or related by blood or marriage to such a suspect, and when the materials sought are not contraband or the fruits or instrumentalities of an offense. The Attorney General shall incorporate in such guidelines--

1. a recognition of the personal privacy interests of the person in possession of such documentary materials;

2. a requirement that the least intrusive method or means of obtaining such materials be used which do not substantially jeopardize the availability or usefulness of the materials sought to be obtained;

3. a recognition of special concern for privacy interests in cases in which a search or seizure for such documents would intrude upon a known confidential relationship such as that which may exist between clergyman and parishioner; lawyer and client; or doctor and patient; and

4. a requirement that an application for a warrant to conduct a search governed by this subchapter be approved by an attorney for the government, except that in an emergency situation the application may be approved by another appropriate supervisory official if within 24 hours of such

emergency the appropriate United States Attorney is notified.

b. Use of search warrants; reports to Congress

The Attorney General shall collect and compile information on, and report annually to the Committees on the Judiciary of the Senate and the House of Representatives on the use of search warrants by Federal officers and employees for documentary materials described in subsection (a)(3) of this section.

§ 2000aa-12. Binding nature of guidelines; disciplinary actions for violations; legal proceedings for non-compliance prohibited

Guidelines issued by the Attorney General under this subchapter shall have the full force and effect of Department of Justice regulations and any violation of these guidelines shall make the employee or officer involved subject to appropriate administrative disciplinary action. However, an issue relating to the compliance, or the failure to comply, with guidelines issued pursuant to this subchapter may not be litigated, and a court may not entertain such an issue as the basis for the suppression or exclusion of evidence.

Updated January 22, 2020

PART IV:STATE JOURNALIST PROTECTIONS

Forty-nine states and the District of Columbia offer some form of protection for reporter's confidential sources or other work product. Some federal courts have also recognized a reporter's privilege in certain circumstances based on the First Amendment. However, there is no federal reporter's shield law.

The Reporters Privilege Compendium by the Reporters Committee for Freedom of the Press offers a comprehensive guide to shield laws and other reporter's privileges recognized in the United States. If you are subject to a newsroom search, you should consult the guide and your state reporter's privilege to determine what protections it affords.

Even if authorities properly issue subpoenas rather than searching newsrooms, reporter's privilege laws impose limits on whether and to what extent they're entitled to discover source and newsgathering materials.

As an example, we summarize the protections in the Florida reporter's privilege. The reporter's privilege in Florida provides fairly broad protection to professional journalists wishing to avoid revealing their sources and newsgathering materials if summoned by law enforcement.

Florida's Reporter Privilege Summary

- Section 90.5015 protects reporters and their newsgathering materials when subpoenaed.
- The privilege protects "professional journalists" from subpoenas seeking "information … obtained while actively gathering news."
    - A "professional journalist" under this statute is defined as "a person regularly engaged in collecting, photographing, recording, writing, editing, reporting, or publishing news, for gain or livelihood, who obtained the information sought while working as a salaried employee of, or independent contractor for, a newspaper, news journal, news agency, press association, wire service, radio or television station, network, or news magazine."
- To overcome this privilege, a party seeking to enforce a subpoena must satisfy a stringent three-part test that requires proof that:

    - the information is relevant and material to unresolved issues in the case;
    - no alternative sources for the information exist; and
    - a compelling need for the information exists.
- Absent satisfying this stringent three-part test, a journalist will be successful in quashing a subpoena for newsgathering materials.

Law in Full:

Fla. Stat. § 90.5015

[Current through Chapter 316 of the 2023 Legislative Session]

Section 90.5015 - Journalist's privilege

(1) DEFINITIONS. - For purposes of this section, the term:
(a) "News" means information of public concern relating to local, statewide, national, or worldwide issues or events.
(b) "Professional journalist" means a person regularly engaged in collecting, photographing, recording, writing, editing, reporting, or publishing news, for gain or livelihood, who obtained the information sought while working as a salaried employee of, or independent contractor for, a newspaper, news journal, news agency, press association, wire service, radio or television station, network, or news magazine. Book authors and others who are not professional journalists, as defined in this paragraph, are not included in the provisions of this section.

(2) PRIVILEGE. - A professional journalist has a qualified privilege not to be a witness concerning, and not to disclose the information, including the identity of any source, that the professional journalist has obtained while actively gathering news. This privilege applies only to information or eyewitness observations obtained within the normal scope of employment and does not apply to physical evidence, eyewitness observations, or visual or audio recording of crimes.
A party seeking to overcome this privilege must make a clear and specific showing that:
(a) The information is relevant and material to unresolved issues that have been raised in the proceeding for which the information is sought;

(b) The information cannot be obtained from alternative sources; and
(c) A compelling interest exists for requiring disclosure of the information.

(3) DISCLOSURE. -\A court shall order disclosure pursuant to subsection (2) only of that portion of the information for which the showing under subsection (2) has been made and shall support such order with clear and specific findings made after a hearing.

(4) WAIVER. - A professional journalist does not waive the privilege by publishing or broadcasting information.

(5) CONSTRUCTION. - This section must not be construed to limit any privilege or right provided to a professional journalist under law.

(6) AUTHENTICATION. - Photographs, diagrams, video recordings, audio recordings, computer records, or other business records maintained, disclosed, provided, or produced by a professional journalist, or by the employer or principal of a professional journalist, may be authenticated for admission in evidence upon a showing, by affidavit of the professional journalist, or other individual with personal knowledge, that the photograph, diagram, video recording, audio recording, computer record, or other business record is a true and accurate copy of the original, and that the copy truly and accurately reflects the observations and facts contained therein.

(7) ACCURACY OF EVIDENCE. – If the affidavit of authenticity and accuracy, or other relevant factual circumstance, causes the court to have clear and convincing doubts as to the authenticity or accuracy of the proffered evidence, the court may decline to admit such evidence.

(8) SEVERABILITY. - If any provision of this section or its application to any particular person or circumstance is held invalid, that provision or its application is severable and does not affect the validity of other provisions or applications of this section.

Fla. Stat. § 90.5015

Amended by 2023 Fla. Laws, ch. 8, s 20, eff. 7/4/2023.s. 1, ch. 98 - 48.