NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 23, ISSUE 2: DECEMBER 2021

SMARTPHONE SECURITY FOR THE MOBILE JOURNALIST: SHOULD REPORTERS GIVE POLICE THE FINGER?

***By Frank D. LoMonte*[*] *and Philip J. Sliger*[**]**

As civil unrest flared across the United States following the police killing of George Floyd in Minneapolis, videographers and photojournalists—both professional and amateur—found themselves targeted by police for arrests, beatings, and harassment. Increasingly, journalists on the scene of civil unrest rely on smartphones as their primary tool for gathering and disseminating news. The advent of "smartphone journalism" presents an evolving set of legal and technological questions: Under what circumstances could a police officer compel a journalist to surrender and unlock a smartphone, and are some security measures more durable than others in standing up to a demand that might compromise confidential newsgathering materials? In short, how can mobile journalists most effectively use technology and the law to keep their confidences secure at a time when confrontations with police are increasingly routine and predictable? This Article attempts to answer that question.

Courts overwhelmingly agree that the First Amendment protects the right to record police activity in public spaces. But it is less clear whether and under what circumstances journalists have a constitutionally protected right to resist having their work product searched when they are eyewitnesses to potential criminal activity, such as looting or throwing objects at police. The first generation of "smartphone law" cases has produced diverging results: Some (but not all) judges regard the compelled unlocking of a secured device

[*] Professor and Director of the Joseph L. Brechner Center for Freedom of Information at the University of Florida in Gainesville, Florida. B.A., 1992, Political Science, Georgia State University; J.D. (Order of the Coif), 2000, University of Georgia School of Law.

[**] Philip Sliger is a third-year law student at the University of Florida's Levin College of Law and a research associate at the Brechner Center for Freedom of Information.

as implicating Fifth Amendment safeguards against self-incriminatory testimony, as well as Fourth Amendment guarantees against unreasonable search and seizure. A little-known federal statute, the Privacy Protection Act ("PPA"), provides an additional potential layer of protection—or after-the-fact recourse—for a journalist who is subjected to an intrusive search for unpublished work. However, a recent court interpretation threatens to undermine the reliability of PPA protection when journalists are not just witnesses but also arrestees.

This Article surveys the landscape of constitutional and statutory claims that might apply when a journalist is confronted with a demand to decrypt a smartphone for police inspection. Additionally, this Article examines the pro-and-con arguments for the two primary security methods—alphanumeric passcodes and biometric locks—and how courts have treated those unlocking methods for Fourth and Fifth Amendment purposes. Lastly, this Article concludes that journalists assigned to scenes where clashes between police and protesters are foreseeable should anticipate facing a demand to surrender a phone—or face an arrest—and take precautions, knowing that after-the-fact damages as remedies against police are, after the Supreme Court's recent ruling in Nieves v. Bartlett*, increasingly unreliable.*

TABLE OF CONTENTS

I. INTRODUCTION

The ability to use roadways, parks, and sidewalks to demonstrate against abusive government behavior is deeply ingrained in United States culture and law.[1] When people are angered by perceived government overreaching, they take to the streets to dramatize their dissatisfaction. Simmering discontent over the excessive use of deadly force against Black people exploded into a sustained "Black Lives Matter" protest movement when a white Minneapolis police officer asphyxiated a 46-year-old Black man, George Floyd, during an arrest for a petty offense in May 2020.[2] In cities across the United States and around the world, people took to the streets to protest injustice and advocate for public policy reforms.[3]

---

[1] *See, e.g.*, Thornhill v. Alabama, 310 U.S. 88, 105 (1940) (striking down a statute that criminalized using public sidewalks for picketing and observing the important role of public thoroughfares as vehicles for communicating ideas: "The safeguarding of these means is essential to the securing of an informed and educated public opinion with respect to a matter which is of public concern"); Hague v. Comm. for Indus. Org., 307 U.S. 496, 515 (1939) ("Wherever the title of streets and parks may rest, they have immemorially been held in trust for the use of the public and, time out of mind, have been used for purposes of assembly, communicating thoughts between citizens, and discussing public questions. Such use of the streets and public places has, from ancient times, been a part of the privileges, immunities, rights, and liberties of citizens.").

[2] *See* Alicia Victoria Lozano, *Fury Across U.S. as Protesters Demand Justice for George Floyd's Death*, NBCNEWS (May 30, 2020, 12:11 PM), https://www.nbcnews.com/news/us-news/curfew-set-twin-cities-after-unrest-turns-chaos-during-48-n1218991 [https://perma.cc/CNW7-WKWZ] (reporting that public outrage over Minneapolis police killing of George Floyd, an unarmed Black man, spawned civil unrest in cities throughout the United States, and even abroad).

[3] Larry Buchanan, Quoctrung Bui & Jugal K. Patel, *Black Lives Matter May Be the Largest Movement in U.S. History*, N.Y. TIMES (July 3, 2020), https://www.nytimes.com/interactive/2020/07/03/us/george-floyd-protests-crowd-size.html [https://perma.cc/S5N8-6GG6].

One distinct feature of the recent protest movements is the massive amount of contemporaneous footage that both professional and amateur videographers are sharing online. A civilian with a smartphone captured George Floyd's killing in its entirety,[4] and the subsequent protests and unrest that reverberated across the country were documented by thousands of spectators, often by the participants themselves.[5] Demonstrations of peaceful protest, as well as acts of violence, are now streamed live to viewers at home. Amateur coverage of the events can reach the public hours before mainstream media outlets repackage the content for their audiences. At times, these videos capture lawbreaking activity, such as excessive force by police or vandalism by civilians.[6] Thus, "smartphone journalists" regularly capture footage that could be used as evidence in criminal investigations.[7]

The scenario of a smartphone journalist capturing documentary evidence of criminal activity will likely become more commonplace as participation in social movements increases, both on social media

---

[4] *See* Rachel Treisman, *Darnella Frazier, Teen Who Filmed Floyd's Murder, Praised for Making Verdict Possible*, NPR (Apr. 21, 2021, 11:15 AM), https://www.npr.org/sections/trial-over-killing-of-george-floyd/2021/04/21/989480867/darnella-frazier-teen-who-filmed-floyds-murder-praised-for-making-verdict-possib [https://perma.cc/47VN-4B67].

[5] *See e.g.*, Kellen Browning, *Where Black Lives Matter Protesters Stream Live Every Day: Twitch*, N.Y. TIMES (June 18, 2020), https://www.nytimes.com/2020/06/18/technology/protesters-live-stream-twitch.html [https://perma.cc/TGW2-FCTQ] (describing how protesters and "citizen journalists" created their own channels on the video streaming platform, Twitch, dedicated to daily live feeds of people marching in protest of police violence).

[6] *See* Kimberly Kindy, Shayna Jacobs & David A. Fahrenthold, *In Protests Against Police Brutality, Videos Capture More Alleged Police Brutality*, WASH. POST (June 5, 2020), https://www.washingtonpost.com/national/protests-police-brutality-video/2020/06/05/a9e66568-a768-11ea-b473-04905b1af82b_story.html [https://perma.cc/E9QW-8XY4] (reporting that citizen-shot videos are capturing police using "[b]rutal tactics" to quell unarmed protesters, raising questions about whether officers are being properly trained and regulated).

[7] *See* Heather Kelly & Rachel Lerman, *America Is Awash in Cameras, a Double-Edged Sword for Protesters and Police*, WASH. POST (June 3, 2020), https://www.washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters/ [https://perma.cc/NU27-88RC].

and in the offline world.[8] Law enforcement has considerable interest in obtaining such documentary materials, either to inculpate alleged wrongdoers or to exculpate their own officers.[9] Thus, the ability to resist demands for disclosure of smartphone footage becomes a concern for professional and amateur journalists alike who capture potentially incriminating activities. Under what circumstances may law enforcement compel an individual to unlock a smartphone? Moreover, even if compelled unlocking is permissible, what limits does the law impose on law enforcement's authority to view the smartphone's contents?

News organizations are increasingly urging journalists to protect their data while covering protests. Mindful of the potential for law enforcement to seize journalists' devices, news outlets train their journalists to use various locking methods so that material recorded

---

[8] *See* Buchanan, Bui & Patel, *supra* note 3 (characterizing protests against police violence as "the largest movement in the country's history" with estimates of participation ranging from 15 million people to as many as 26 million people); Sarah Frostenson, *The Women's Marches May Have Been the Largest Demonstration in US History*, VOX (Jan. 31, 2017, 11:11 AM), https://www.vox.com/2017/1/22/14350808/womens-marches-largest-demonstration-us-history-map [https://perma.cc/G397-TEVT] (stating that "scientists think we may have just witnessed the largest day of demonstrations in American history," with 4.2 million people marching in 600-plus U.S. cities in protest of Donald Trump's inauguration as president)*; see also* Brooke Auxier, *Activism on Social Media Varies by Race and Ethnicity, Age, Political Party*, PEW RSCH. CTR. (July 13, 2020), https://www.pewresearch.org/fact-tank/2020/07/13/activism-on-social-media-varies-by-race-and-ethnicity-age-political-party/ [https://perma.cc/XD9W-ACRC] (reporting survey findings that about one-third of social media users say they have used social media in the past month to post a picture to show support for a cause, to look up information about rallies or protests, or to encourage others to take action on issues they care about).

[9] *See* Cindy Von Quednow, *Long Beach Police Seek Evidence of 'Criminal Activity' During Recent Protests Using New Online Portal*, KTLA (June 4, 2020, 5:30 PM), https://ktla.com/news/local-news/long-beach-police-seek-evidence-of-criminal-activity-during-recent-protests-using-new-online-portal/ [https://perma.cc/P7MZ-RN2P] (reporting that a California police department and the FBI created an online portal to solicit smartphone footage from racial unrest that resulted in property damage).

on a confiscated phone is not readily viewable.[10] Case law interpreting the Fourth and Fifth Amendments, and the rarely-litigated Privacy Protection Act of 1980, provides a helpful guide for journalists seeking to secure the data on their smartphones.[11] This case law, however, does not provide perfect clarity on smartphone data protection.[12] Thus, anyone taking to the streets to participate in, or cover, protests should be aware of these legal ambiguities and take practical steps to minimize the need to litigate on uncertain footing.

This Article examines the tension between law enforcement and photojournalists, both professional and amateur, and how that tension has regularly produced conflict over the interest of police in solving crimes and the interest of journalists in maintaining their professional detachment from police to disseminate essential information to the public. This tension is as old as photojournalism. However, new technologies have blurred the lines between journalists and bystanders, creating far more opportunities for conflict and confusion, as police now look to the increasingly tempting shortcut of cellphone video footage to solve crimes. Specifically, this Article considers the not-uncommon scenario of law enforcement officers seeking to unlock a secured smartphone to examine its contents, and evaluates which types of security—numeric passcode or biometric trigger—might give journalists the best chance of being able to control access to their work product.

Part II looks at instances where the interests of police and videographers have come into conflict at scenes of civil unrest and why the legal system recognizes the importance of enabling journalists to resist demands to surrender their unpublished work. In Part III, this Article examines the legal bases on which a journalist might legitimately resist a demand to surrender work product stored on a smartphone. Specifically, Part III discusses the Fifth Amendment and a growing body of diverging judicial interpretations of whether a person suspected of wrongdoing can be

---

[10] *See* Maddy Varner, *How Do I Prepare My Phone for a Protest?*, THE MARKUP (June 4, 2020), https://themarkup.org/ask-the-markup/2020/06/04/how-do-i-prepare-my-phone-for-a-protest [https://perma.cc/M2KB-Q7AT].

[11] *See infra* Parts III, IV, and V.

[12] *See infra* Part VI.

compelled to unlock a phone or surrender the information enabling police to unlock it. Part IV considers the Fourth Amendment arguments that might arise when police search or seize a smartphone and how federal courts—including the Supreme Court in its 2014 *Riley v. California* ruling[13]—are coming to recognize the singularly intrusive nature of a smartphone search.[14] Part V discusses a little-known statutory shield, the federal Privacy Protection Act of 1980, and how that statute can deter and penalize over-eager officers who seek to pry into journalists' phones. Given the state of constitutional and statutory protections against over-intrusive searches, Part VI subsequently analyzes where the law is clear, as well as unclear, on whether law enforcement agents may demand access to footage of protests or other "breaking" on-scene news and how journalists might maximize their chances of protecting the confidential contents of their phones. Finally, Part VII emphasizes the importance of preparing smartphone journalists for the risk of adverse interactions with law enforcement while covering fast-breaking news in the field because—constitutional principles notwithstanding—journalists have struggled to use the legal system to curb overreaching by law enforcement officials.

II. THE CAMERA NEVER BLINKS – BUT SOMETIMES, IT SQUEALS

While journalists have an obvious personal stake in avoiding search, detention, and arrest on the job, the public also benefits from robust protection of news organizations' ability to safely gather information at scenes of civil unrest. This newsgathering includes unpaid "citizen journalists" who, increasingly, are fulfilling the information needs of communities that lack well-supported professional newsrooms. Though not unanimous, there is broad consensus that journalists should have some degree of evidentiary privilege against surrendering their confidential work product to authorities. But for that legal protection to have any practical value, police must be restricted from preemptively seizing journalists'

[13] Riley v. California, 573 U.S. 373 (2014).

[14] *See id.* at 402 (holding that, given the unique privacy concerns at stake in regard to one's smartphone, a search warrant is generally required).

recording devices and inspecting the contents before a judge can even consider whether privilege applies.

A. Public Reliance on Professional and Amateur News Footage

Alongside celebrated professional journalists from *The New York Times*, *The Washington Post*, the Associated Press, and Reuters, the 2021 Pulitzer Prizes for journalism recognized a seventeen-year-old Minnesota teen whose act of videography—capturing the murder of George Floyd at the hands of a Minneapolis police officer—may have been the most impactful act of "citizen journalism" of all time.[15] That the world's most prestigious journalism awards recognized an act of amateur smartphone videography underscores the blurring distinction between "journalist" and "bystander" and how unpaid citizen "watchdogs" can use smartphone technology to perform journalistic functions when news is unfolding.

Mainstream community news organizations have drastically downsized their staffing as advertising and circulation revenues dry up; photojournalism positions have been especially hard-hit.[16] This downsizing has made newsrooms increasingly dependent on "one-man-band" mobile journalists, who record smartphone videos when

---

[15] *See* Elahe Izadi, *Darnella Frazier, the Teen Who Filmed George Floyd's Murder, Awarded a Pulitzer Citation*, WASH. POST (June 11, 2021), https://www.washingtonpost.com/media/2021/06/11/darnella-frazier-pulitzer-george-floyd-witness/ [https://perma.cc/J8SR-MHXS].

[16] *See* Monica Anderson, *At Newspapers, Photographers Feel the Brunt of Job Cuts*, PEW RSCH. CTR. (Nov. 11, 2013), https://www.pewresearch.org/fact-tank/2013/11/11/at-newspapers-photographers-feel-the-brunt-of-job-cuts/ [https://perma.cc/9EF8-WGB6] (reporting that photography jobs in U.S. newsrooms dropped 43% between 2000 and 2012, outpacing the rate of erosion of other fast-disappearing journalism jobs). The *Chicago Sun-Times* and the *New York Daily News* are among the major metropolitan daily publications that eliminated substantially all of their full-time photography jobs in recent years. Tom Burton, *NY Daily News Eliminates Photographers' Jobs in Massive Layoffs*, NAT'L PRESS PHOTOGRAPHERS ASS'N (July 25, 2018), https://nppa.org/news/ny-daily-news-eliminates-photo-staff [https://perma.cc/2BFU-LL2W]; Mark Memmott, *'Chicago Sun-Times' Fires Its Photographers*, NPR.ORG (May 30, 2013, 1:48 PM), https://www.npr.org/sections/thetwo-way/2013/05/30/187292393/chicago-sun-times-fires-its-photographers [https://perma.cc/3S88-DSDX].

reporting from the field.[17] Additionally, short-staffed newsrooms are more reliant on video contributed by eyewitnesses or reshared from non-journalists' social media pages.[18] The increasing quality and user-friendliness of smartphone cameras enable a relative novice to shoot images that, if not a substitute for the craftsmanship of well-trained photojournalists, are at least a serviceable standby.[19]

The ubiquity of high-quality smartphones has also increased the opportunity for confrontations with law enforcement officers at scenes of newsworthy events. Instead of having to deal with one or two news photographers carrying conspicuous camera equipment and who are readily recognizable as journalists, police now must assume that any bystander can photograph, record, or livestream to a potentially limitless online audience. As one commentator has observed:

> Police face potential bombardment from videographers because recording devices are cheaper and handier than ever. Due to the proliferation of inexpensive recording technology, police encounters in public are more commonly captured on portable media that can be

---

[17] *See* Robert Corn-Revere, *Protecting the Tools of Modern Journalism*, 30 COMMC'NS L. 9, 9 (2014) ("Media outlets increasingly issue reporters smartphones to take photographs and to record other story elements.").

[18] For an especially vivid illustration, see Otto v. Hearst Commc'ns, Inc., 345 F. Supp. 3d 412 (S.D.N.Y. 2018). In *Otto*, a bank executive attending a wedding at the Trump National Golf Club in New Jersey snapped an iPhone photo of then-President Donald Trump unexpectedly popping into the reception to congratulate the bride and groom. *Id.* at 420. He shared the photo with several other guests, one of whom posted the photo to a personal Instagram account, where professional news outlets, including the website for *Esquire* magazine, discovered the post and—without obtaining permission from the creator—copied and republished the picture online. *Id.* at 421. The amateur photographer sued *Esquire* owner *Hearst* for copyright infringement, and a federal district court found for the photographer, holding that the appropriation did not qualify for the defense of fair use. *Id.* at 433. The district court awarded the photographer minimal damages of $750. Clerk's Judgment, Otto v. Hearst Commc'ns., Inc., No. 1:17-cv-04712-GHW (S.D.N.Y. Jan. 23, 2020).

[19] *See* Terry Sullivan, *A Beginner's Guide to Taking Great Video on Your Phone*, N.Y. TIMES (Apr. 17, 2018), https://www.nytimes.com/2018/04/17/smarter-living/beginners-guide-phone-video.html [https://perma.cc/GJ5M-TQTT] (observing that improvements in smartphone technology have enabled even professional filmmakers to use smartphones in place of traditional video cameras).

> disseminated almost instantly, allowing the public to constantly scrutinize and form opinions about the police.[20]

The presence of such pervasive scrutiny is, perhaps understandably, threatening to some officers, who fear that videos will be mischaracterized or deceptively edited. Until recently, officers enjoyed the advantage of having the only video of most confrontations with civilians, plus the intrinsic "benefit of the doubt" that their testimony carried weight when a situation involved merely the uncorroborated word of a civilian witness against that of an officer.[21]

The heightened tension between law enforcement and smartphone journalists has manifested in arrests, beatings, and the destruction or seizure of recording equipment. In Baltimore, for instance, police confiscated a smartphone and deleted its video contents merely because a bystander recorded the arrest of a fellow attendee at a horserace to the chagrin of the arresting officers.[22] In Philadelphia, a college student photographing police making a traffic stop in his neighborhood as part of a class photojournalism assignment was thrown to the ground and handcuffed.[23] The college student and his girlfriend, who tried to come to his aid, were charged with obstruction and disorderly conduct.[24] In jurisdictions across the

---

[20] David Murphy, Comment, *"V.I.P." Videographer Intimidation Protection: How the Government Should Protect Citizens Who Videotape the Police*, 43 SETON HALL L. REV. 319, 327 (2013).

[21] *See id.* at 330 (stating that, before the widespread availability of home video cameras and, later, smartphones, "[p]olice previously enjoyed a monopoly over the ability to record public confrontations using cameras in cruisers and recording equipment attached to officers").

[22] *See* Derek Valcourt, *Landmark Settlement Reached in Preakness Arrest Case; New Police Policy Spells Out Recording Rights*, CBS LOCAL (Mar. 12, 2014, 5:40 PM), https://baltimore.cbslocal.com/2014/03/12/landmark-settlement-reached-in-preakness-arrest-case/ [https://perma.cc/H74T-KT5Z] (reporting that, after nearly four years of litigation, the City of Baltimore agreed to pay a six-figure settlement plus attorney fees to the videographer, as well as clarify police department policies to protect the right to record officers).

[23] Dan Reimold, *Temple Student Sues Over Arrest for Photojournalism Class Assignment*, USA TODAY (Mar. 16, 2014, 7:43 PM), https://www.usatoday.com/story/college/2014/03/16/temple-student-sues-over-arrest-for-photojournalism-class-assignment/37439061/ [https://perma.cc/S45L-RMYV].

[24] *Id.*

country, the American Civil Liberties Union ("ACLU") has filed lawsuits accusing police of similar excesses, attesting to the regularity of confrontations with "citizen journalists" for filming police activity.[25]

Advances in facial recognition technology, as well as a growing archive of surveillance videos against which to match faces, make smartphone video an even more useful tool for investigating crimes.[26] For example, after rioters loyal to outgoing President Donald Trump stormed the U.S. Capitol on January 6, 2021, in an attempt to stop Congress from certifying the results of the 2020 presidential election, investigators used bystander-shot video to track down and arrest scores of suspected participants in the mayhem.[27]

Of course, no law exists to stop police from viewing footage publicly shared to YouTube, Instagram, or any other video-sharing platform. Once an image is posted to social media, the law

---

[25] *See* Beth Burger, *ACLU of Ohio Sues Columbus Police After Hilltop Man Arrested for Recording SWAT Officers*, COLUMBUS DISPATCH (Jan. 12, 2021, 2:30 PM), https://www.dispatch.com/story/news/2021/01/11/aclu-sues-columbus-police-after-man-arrested-recording-officers/6630973002/ [https://perma.cc/9NXQ-26KZ] (reporting that a bystander alleged a SWAT team arrested him for filming a SWAT team raid of a neighbor's house from his own front porch); *Lawsuit Alleges Police Seized Cellphone Without Warrant*, ASSOCIATED PRESS (Mar. 13, 2020), https://apnews.com/article/fa8a33d6fc823d532ba94ad0e24a4d48 [https://perma.cc/3AER-ZKCF] (reporting that a bystander alleged the police arrested him for shooting a smartphone video of officers responding to a fight outside of a convenience store); Kim Zetter, *ACLU Sues Police for Seizing Man's Phone After Recording Alleged Misconduct*, WIRED (Sept. 7, 2012, 3:02 PM), https://www.wired.com/2012/09/man-sues-police-over-phone/ [https://perma.cc/8M9Q-G3X9] (describing a lawsuit that alleged the police grabbed an eyewitness' smartphone and stole its memory card because the eyewitness was filming officers beating a suspect).

[26] *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1119–24 (2021) (explaining how police use face identification technology to match a suspect's face against other available images, and how commercially available technology is making it easier, even for small police departments, to use facial recognition).

[27] Craig Timberg, Drew Harwell & Spencer S. Hsu, *Police Let Most Capitol Rioters Walk Away. But Cellphone Data and Videos Could Now Lead To More Arrests.*, WASH. POST (Jan. 8, 2021, 5:37 PM), https://www.washingtonpost.com/technology/2021/01/08/trump-mob-tech-arrests/ [https://perma.cc/7TUJ-EKWY].

recognizes that there is no "expectation of privacy" in content willfully shared to the public; thus, viewing the image does not constitute a "search" triggering constitutional safeguards.[28] But, when police insist on viewing or—even more invasively—taking possession of unpublished videos of newsworthy events, both constitutional and statutory safeguards may be triggered.

B. Why Confidentiality Matters

Society has long recognized that the public benefits when journalists are free to gather and report news without undue governmental interference. For this reason, the legal system sometimes puts journalists in a preferred position that recognizes their role as the eyes and ears of the general public.[29] Nearly every state recognizes some degree of evidentiary privilege, entitling journalists to refuse demands to surrender confidential information in connection with legal proceedings where ordinary citizens would be compelled to comply.[30] As with other evidentiary privileges, these "shield laws" are built around recognizing that the public has a profound interest in the flow of truthful and timely information to

---

[28] *See, e.g.*, Chaney v. Fayette Cnty. Pub. Sch. Dist., 977 F. Supp. 2d 1308, 1317 (N.D. Ga. 2013) (finding that a student whose Facebook photos were humiliatingly displayed at a school assembly had no constitutional claim because society would not recognize a reasonable expectation of privacy for photos voluntarily posted to a publicly viewable social media page).

[29] *See* Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 572–73 (1980) ("Instead of acquiring information about trials by firsthand observation or by word of mouth from those who attended, people now acquire it chiefly through the print and electronic media. In a sense, this validates the media claim of functioning as surrogates for the public."). Justice Lewis F. Powell Jr. made this point in his dissent in *Saxbe v. Wash. Post Co.*, in which he argued for recognizing a First Amendment right for journalists to gain access to interviews with prison inmates: "An informed public depends on accurate and effective reporting by the news media. No individual can obtain for himself the information needed for the intelligent discharge of his political responsibilities. For most citizens the prospect of personal familiarity with newsworthy events is hopelessly unrealistic. In seeking out the news the press therefore acts as an agent of the public at large." 417 U.S. 843, 863 (1974) (Powell, J., dissenting).

[30] *See* Christina Koningisor, *The De Facto Reporter's Privilege*, 127 YALE L.J. 1176, 1202 (2018) (explaining that every state (except Wyoming) recognizes some degree of journalist's privilege by way of statute, common law, or constitutional interpretation).

journalists. Therefore, public interest can override the normal expectation that witnesses must cooperate in providing testimony and any physical evidence in their possession.[31] Highlighting this principle, law professor Christina Koningisor asserted that "the most common justification for the reporter's privilege today is that revealing confidential information would cause reporters' sources to dry up. This, in turn, would stem the flow of information to the press—and by extension—to the public."[32] Professor Koningisor's assertion is representative of a 1981 holding from the D.C. Circuit Court of Appeals, whereby the Court drew a direct link between the journalist's ability to protect his confidential source and the public's access to candid information.[33] Ruling in favor of a journalist whose testimony was sought in a civil lawsuit over leaked government documents identifying suspected organized crime figures, the court reasoned:

> Without an unfettered press, citizens would be far less able to make informed political, social, and economic choices. But the press' function as a vital source of information is weakened whenever the ability of journalists to gather news is impaired. Compelling a reporter to disclose the identity of a source may significantly interfere with this news gathering ability; journalists frequently depend on informants to gather news, and confidentiality is often essential to establishing a relationship with an informant.[34]

Although generally referred to as a "reporter's" privilege, the benefit of this privilege more directly flows to the source of the photo or video. In fact, one state, Wisconsin, has explicitly denominated its statute as a whistleblower protection law rather than

---

[31] *See* David Abramowicz, *Calculating the Public Interest in Protecting Journalists' Confidential Sources*, 108 COLUM. L. REV. 1949, 1954 (2008) ("[P]roponents argue that the ability to promise confidentiality facilitates newsgathering. Such newsgathering can serve the public interest, such as when unnamed sources blow the whistle on government or corporate corruption."); *see also id.* at 1955 (discussing an additional rationale for why conscripting journalists as frequent witnesses for the government could compromise their independence).

[32] Koningisor, *supra* note 30, at 1180.

[33] *Id.*

[34] Zerilli v. Smith, 656 F.2d 705, 711 (D.C. Cir. 1981).

a journalist protection law.[35] While journalists theoretically can be fined—or, in extreme cases, jailed—for refusing to cooperate with demands for evidence,[36] such sanctions are infrequent.[37] Instead, the true "skin in the game" belongs to the person who provided the information to the journalist: the person who could be in jeopardy of being fired or criminally prosecuted for leaking the information.[38]

Considerable debate exists concerning the proper scope of the privilege: who should be covered, what material should be subject to withholding, and in which types of proceedings the privilege should apply.[39] For more than a century, courts have recognized the

---

[35] *See* Erik Ugland, *The Reporter's Privilege Goes Incognito in Wisconsin*, MARQ. L. SCH. FAC. BLOG (May 31, 2010), https://law.marquette.edu/facultyblog/2010/05/the-reporters-privilege-goes-incognito-in-wisconsin/ [https://perma.cc/LBN6-M2BH] ("[S]upporters of the new law have deliberately flown it under the radar and have presented [it] more as a boon for citizen-watchdogs than reporters.").

[36] *See* Markus E. Apelis, *Fit to Print? Consequences of Implementing a Federal Reporter's Privilege*, 58 CASE W. RSRV. L. REV. 1369, 1370 (2008) (stating that more than twenty U.S. journalists were known to have been jailed between 1972 and 2008 for defying judicial directives to disclose confidential material, including Joshua Wolf, a California videographer and blogger, who was held on contempt charges for 226 days for refusing to furnish video of a protest sought by federal law enforcement agents as part of a grand jury investigation).

[37] In a 2003 report, the nonprofit Reporters Committee for Freedom of the Press stated that, over the preceding ten years, only five reporters had been jailed anywhere in the United States for refusing to give evidence in court. *New York Times Reporters Refuse to Answer Questions About Sources*, REPS. COMM. FOR FREEDOM OF THE PRESS (Dec. 19, 2003), https://www.rcfp.org/new-york-times-reporters-refuse-answer-questions-about-sources/ [https://perma.cc/M7CY-73MX].

[38] *See* Note, *The Rights of Sources – The Critical Element in the Clash Over Reporter's Privilege*, 88 YALE L.J. 1202, 1203–04 (1979) ("A source's interests . . . are qualitatively different and far more compelling than those of a reporter."); *see also id.* at 1210–12 (opining that compelled disclosure of a journalist's unnamed source implicates the speaker's constitutional right of freedom of association, as well as freedom of speech).

[39] *See* Mary-Rose Papandrea, *Citizen Journalism and the Reporter's Privilege*, 91 MINN. L. REV. 515, 549 (2007) (describing the "disagreement among the states regarding whether shield laws should protect the identity of both nonconfidential sources and confidential sources; whether the privilege should extend to newsgathering materials; and whether publication is required before the

existence of some common-law protection for the confidentiality of newsgathering, though the breadth and durability of protection have varied.[40] While the First Amendment offers some protection for the act of gathering news, the Supreme Court has neither specified the metes-and-bounds of that protection nor determined what level of showing a government agency must make to override the protection.[41] In general, the Supreme Court has resisted recognizing any special legal status for professional newsgatherers above and beyond the legal rights of ordinary citizen bystanders.[42]

The Supreme Court's limited engagement with the concept of a journalist's privilege in *Branzburg v. Hayes*[43] left First Amendment law in a state of uncertainty.[44] In *Branzburg*, a closely divided

---

protection can be invoked" among other variations regarding the scope of coverage); *see also id.* at 566–67 (describing states' varying interpretations as to what amount of journalistic employment is necessary to qualify a person to take advantage of the reporter's privilege).

[40] *See* Koningisor, *supra* note 30, at 1213–14 (tracing the evolution of the common-law privilege to gather information in early twentieth century case law).

[41] *See* Nicholas J. Jacques, *Information Gathering in the Era of Mobile Technology: Towards a Liberal Right to Record*, 102 CORNELL L. REV. 783, 785 (2017) ("The Supreme Court and lower courts have developed this First Amendment right to gather information in a patchwork of cases over the past forty years, but the Court has never explained its exact origins or rationale.") (citation omitted).

[42] *See* Pell v. Procunier, 417 U.S. 817, 834 (1974) (rejecting the proposition that the press has a First Amendment right of access to enter prisons to conduct interviews: "The Constitution does not . . . require government to accord the press special access to information not shared by members of the public generally"); *see also* Genevra Kay Loveland, *Newsgathering: Second-Class Right Among First Amendment Freedoms*, 53 TEX. L. REV. 1440, 1445–46 (1975) (citing *Pell* as among the rulings that "dimmed for the foreseeable future the press' hope of convincing the Court that the first amendment grants to the press, as a representative of the public, a special right of access to information of public concern").

[43] 408 U.S. 665 (1972).

[44] *Id.*; *see also* Sonja R. West, *Concurring in Part & Concurring in the Confusion*, 104 MICH. L REV. 1951, 1953–54 (2006) (using the *Branzburg* case, in which no rationale attracted a majority and Justice Lewis Powell's concurrence provided the decisive fifth vote, to illustrate how partial versus full concurrences have caused interpretive difficulties); Robert T. Sherwin, *"Source" of Protection: The Status of the Reporter's Privilege in Texas and a Call to Arms for the State's*

Supreme Court ruled that there was no First Amendment-based privilege, which would have entitled journalists to refuse to answer questions about their work if subpoenaed to testify in a criminal investigation before a grand jury.[45] The decisive fifth vote came from Justice Lewis F. Powell Jr., whose concurring opinion suggested that the First Amendment might supply a privilege against testifying in settings other than a criminal grand jury probe, where the need for information is uniquely urgent.[46] When combined with the votes of the four dissenters, Powell's concurrence can be read as recognizing a constitutionally-based privilege on, as Powell wrote, "a case-by-case basis."[47]

In the aftermath of *Branzburg*, most federal courts have concluded that the Constitution affords some degree of protection enabling journalists to keep confidences, emanating from the First Amendment right to gather information.[48] For instance, just a few years after *Branzburg*, the D.C. Circuit Court of Appeals declined to follow the Supreme Court's narrow precedent when the demand for disclosure of a journalist's confidential source came in a civil lawsuit; the public interest in disclosure was less compelling than in a criminal grand jury investigation.[49] The D.C. Circuit wrote:

> Compelling a reporter to disclose the identity of a confidential source raises obvious First Amendment problems. The First Amendment guarantees a free press primarily because of the important role it can play

---

Legislators and Journalists, 32 TEX. TECH. L. REV. 137, 147–48 (2000) (suggesting that Powell's concurrence plus the dissenting votes constitute a majority for some "qualified" level of constitutionally-based reporter's privilege, but caveating: "It is unclear whether this interpretation is accurate; the Supreme Court has not since directly readdressed the issue, leaving lower courts with the difficult task of deciphering *Branzburg's* meaning").

[45] *See Branzburg*, 408 U.S. at 693 ("[T]he evidence fails to demonstrate that there would be a significant constriction of the flow of news to the public if this Court reaffirms the prior common-law and constitutional rule regarding the testimonial obligations of newsmen.").

[46] *See id.* at 709–10 (Powell, J., concurring).

[47] *Id.* at 710. Powell's brief, three-paragraph opinion was unilluminating even to his fellow justices, one of whom called it "enigmatic." *See id.* at 725 (Stewart, J., dissenting).

[48] *See* Abramowicz, *supra* note 31, at 1957 (observing that "nearly every federal circuit recognizes some degree of journalist's privilege").

[49] Zerilli v. Smith, 656 F.2d 705, 707, 711–12 (D.C. Cir. 1981).

> as a vital source of public information . . . . Without an unfettered press, citizens would be far less able to make informed political, social, and economic choices. But the press' function as a vital source of information is weakened whenever the ability of journalists to gather news is impaired. Compelling a reporter to disclose the identity of a source may significantly interfere with this news gathering ability; journalists frequently depend on informants to gather news, and confidentiality is often essential to establishing a relationship with an informant.[50]

When a dispute involves a physical search for confidential information rather than (as in *Branzburg*) a demand for testimony, courts do not generally consider the First Amendment to provide special protection against being searched, leaving the Fourth Amendment to carry the load.[51] The lack of consensus as to whether, and to what extent, a constitutionally-based right exists to refuse to divulge unpublished newsgathering work product means that journalists, and those who share confidences with journalists, are heavily reliant on state privilege statutes.

Privilege statutes, however, largely predate the development of ubiquitous handheld video cameras and online file-sharing. Therefore, courts have been asked to adapt decades-old notions of "journalism" for the social media era, with varying outcomes.[52] In 2011, a state court judge initially denied the benefit of privilege to a technology blog that did not fit the literal description of an eligible

---

[50] *Id.* at 710–11 (internal quotes and citations omitted).

[51] *See* Alex Abdo, *Why Rely on the Fourth Amendment to Do the Work of the First?*, 127 YALE L.J.F. 444, 451–53 (2017) (opining that courts should recognize a First Amendment-based privilege protecting the privacy of confidential information where disclosure might chill the flow of information but observing that courts have thus far failed to do so, leaving the Fourth Amendment as the only recourse).

[52] *See* Jason A. Martin & Anthony L. Fargo, *Rebooting Shield Laws: Updating Journalist's Privilege to Reflect the Realities of Digital Newsgathering*, 24 U. FLA. J.L. & PUB. POL'Y 47, 65 (2013) (observing that, as of 2013, only "a handful" of privilege statutes had been updated to add references to the Internet or online publishing); William E. Lee, *Citizen-Critics, Citizen Journalists, and the Perils of Defining the Press*, 48 GA. L. REV. 757, 776–78 (2014) (contrasting analyses applied by courts in Oregon, where a blogger was deemed insufficiently journalistic to qualify for the reporter's privilege, versus courts in New Jersey, where a blogger was deemed to qualify as a journalist despite flouting some traditional professional norms).

"news medium" under the Illinois reporter shield law but ultimately reconsidered and reversed its decision.[53] More recently, a trial court, applying Nevada's half-century-old shield law, ruled that a blogger was not entitled to claim protection against disclosure of confidential sources.[54] The Nevada Supreme Court did, however, overturn the decision, saying that online newspapers were entitled to the protection of their sources.[55] In general, the law has increasingly accepted that the reporter's privilege should apply functionally, based on whether the seeker of the privilege shows a pattern of having regularly engaged in gathering and disseminating news, regardless of format or professional status.[56] The legal system is thus evolving to recognize that people gathering images who are not full-time-salaried journalists nevertheless make valuable contributions to the flow of newsworthy information.

States also have different understandings about how much material journalists may defensibly withhold and under what circumstances journalists may withhold such material.[57] The

---

[53] *See* Martin & Fargo, *supra* note 51, at 48–49 (describing a lawsuit involving website TechnoBuffalo, which was hit with a demand to disclose the source of a news tip alleged to have revealed trade secrets about a forthcoming Motorola smartphone model).

[54] *See* Marcella Corona, *Nevada Judge Rules Online Journalist Must Reveal Sources, Not Protected by Media Shield Law*, RENO GAZETTE-JOURNAL (Mar. 7, 2019, 11:50 AM), https://www.rgj.com/story/news/2019/03/07/nevada-judge-rules-online-sites-not-protected-media-shield-law/3091926002/ [https://perma.cc/4Z3T-T5J7] (describing backlash over the trial court's ruling, which based denial of the recognition of the right to protect gathered information on evidence that the publication did not appear in "print" and that the blogger was not a dues-paying member of the state press association at the time the disputed news articles were published).

[55] *See* Toll v. Wilson, 453 P.3d 1215, 1219 (Nev. 2019) (stating that "just because a newspaper can exist online, . . . does not mean it ceases to be a newspaper").

[56] *See* Martin & Fargo, *supra* note 51, at 85, 93 (commenting that courts have extended protection to bloggers when their "output substantively resemble[s] [that of more] traditional news media," but courts have denied coverage to purported journalists who are unable to show a pattern of previous journalistic output).

[57] *See, e.g.*, Kitzmiller v. Dover Area Sch. Dist., 379 F. Supp. 2d 680, 686–89 (M.D. Pa. 2005) (recognizing that reporters could be compelled to testify about what they witnessed at a school board meeting that was viewable to the public but

privilege may be "absolute" (i.e., no circumstances allow for an override of the privilege) or "qualified" (i.e., a judge can compel disclosure if the proponent makes an overriding showing of need).[58] Moreover, the privilege may apply only to information gathered under a promise of confidentiality, or the privilege may apply more broadly to any unpublished journalistic work product.[59] When the dispute involves footage shot at a public event, the scope of the privilege statute can be decisive; images of protesters are rarely obtained under a promise of anonymity, as opposed to recordings of interviews with individuals, which may well have been.[60]

Just as the reporter's privilege benefits those who confidentially furnish information to the press (often insisting on anonymity out of fear of retaliatory workplace consequences), the ability to secure a journalist's smartphone protects those whose communications with journalists might otherwise be exposed by a search. Reviewing the contents of a journalist's phone could compromise a confidential source's communications directly (e.g., conversations or copies of leaked documents that are stored on the phone) or indirectly (e.g., the confidential source appears in the journalist's address book and has corresponded with the journalist). Because third-party interests are so directly implicated—indeed, the risk to the source may be significantly greater than any peril to the journalist—a smartphone search is not entirely analogous to the more traditional types of

---

could not be compelled to surrender their notes or unpublished work product). *See also* Bartlett v. Superior Court *ex rel*. County of Pima, 722 P.2d 346, 350 (Ariz. Ct. App. 1986) (interpreting narrowly Arizona's reporter's privilege statute to apply to material gathered only under a promise of confidentiality: "[T]he claim of privilege depends, in the first instance, upon the existence of a confidential relationship such that compliance with a subpoena would either result in disclosure of confidential information or sources or would seriously interfere with the news gathering and editorial process").

[58] *See* Koningisor, *supra* note 30, at 1203, 1203 n.148 (explaining that privilege may be regarded as absolute or qualified, and providing illustrative contrasting statutes).

[59] *See id.* at 1203–04 nn.149–50, 154 (offering examples of shield laws that differ in their protection of nonconfidential information).

[60] *See, e.g.*, *Kitzmiller*, 379 F. Supp. 2d at 686–89; *see also Bartlett*, 722 P.2d at 350 (drawing a decisive contrast between information received in confidence from an interviewee, which is protected by privilege, versus a video recording of a non-confidential event, which raises none of the same concerns).

searches around which search-and-seizure legal principles have evolved (for instance, a drunk-driving breathalyzer or blood test).[61]

C. From Journalist to Jailbird

Whether because journalists are either purposefully targeted by police for gathering news or are merely caught in the net alongside demonstrators, journalists not infrequently find themselves facing arrest and/or prosecution as a result of documenting scenes of civil unrest. During the nationwide wave of racial justice protests triggered by the killing of George Floyd, the U.S. Press Freedom Tracker, a nonprofit organization, recorded more than 600 instances of law enforcement officers "arresting, detaining, or engaging in acts of physical aggression against journalists."[62]

The scale of the George Floyd protests was unpresedented, but the peril to journalists was not; when crowds of people confront police, journalists frequently find themselves in the legal crosshairs. For example, at least ninety journalists were arrested in twelve different cities during the "Occupy Wall Street" economic justice protests of 2011, which originated in New York but spawned look-alike "Occupy" encampments in public spaces from coast to coast.[63] While in Ferguson, Missouri covering demonstrations following the fatal police shooting of Black teenager Michael Brown in 2014, *Washington Post* reporter Wesley Lowery and *Huffington Post* reporter Ryan Reilly were arrested simply for failing to immediately leave a McDonald's restaurant when ordered by police.[64] During the

---

[61] *See* Aaron Chase, *Secure the Smartphone, Secure the Future: Biometrics, Boyd, a Warrant Denial and the Fourth and Fifth Amendments*, 17 HASTINGS RACE & POVERTY L.J. 577, 587 (2020) (explaining that courts have generally declined to protect against compelled disclosure of *data* that is accessible to third parties, such as a phone carrier's log of the phone numbers that a smartphone owner dialed, but have been more protective when the disclosure involves the *content* of conversations as opposed to data).

[62] *See* Sonja R. West, *The Majoritarian Press Clause*, 2020 U. CHI. LEGAL F. 311, 324 (2020).

[63] Corn-Revere, *supra* note 17, at 10.

[64] Angela Rulffes, *The First Amendment in Times of Crisis: An Analysis of Free Press Issues in Ferguson, Missouri*, 68 SYRACUSE L. REV. 607, 613–14 (2018). St. Louis County authorities did not file criminal charges until nearly a year after

same Ferguson events, Gerald "Trey" Yingst, a college student working as a journalist for the website News2Share, was arrested and charged with unlawful assembly, failure to obey a lawful order, and interfering with the duties of a police officer while standing on a public sidewalk shooting news video during a protest.[65]

When protests erupted surrounding Donald Trump's January 2017 presidential inauguration, the Washington, D.C. Police arrested six journalists covering the unrest; the charges included rioting, which is a felony carrying a potential ten-year prison sentence.[66] One of the journalists, freelance writer Aaron Cantú, who was under a cloud of felony charges for nearly eighteen months until federal prosecutors dismissed the case, claimed that federal law enforcement officers extracted data from potentially hundreds of arrestees' confiscated phones but were unable to crack his phone ("thanks to strong encryption").[67] Alexi Wood, a San Antonio-based photojournalist, could have faced up to seventy years in prison after being arrested while livestreaming scenes of the Trump inaugural protests on his smartphone.[68] His incitement case went all the way

---

the arrests, dropping them only when, nine months later, the journalists entered into an agreement not to sue. *Id.* at 630.

[65] *See* Michael Calderone, *Trey Yingst, Journalist Arrested In Ferguson, Wins Settlement From St. Louis County*, HUFFINGTON POST (Aug. 3, 2015, 11:50 AM), https://www.huffpost.com/entry/trey-yingst-journalist-arrested-in-ferguson-wins-settlement-from-st-louis-county_n_55b7f4bfe4b0224d88345c7d [https://perma.cc/L79V-MMBG] (reporting that charges were dropped, and an $8,500 settlement was paid to resolve Yingst's civil lawsuit against St. Louis County challenging the legal basis for his arrest).

[66] Rulffes, *supra* note 63, at 631.

[67] Aaron Cantú, *The Feds Tried to Lock Up a Journalist for Life for Reporting on Inauguration Protests. This Is His True Story of Conspiracy in Trump's America*, INDY WEEK (Aug. 1, 2018, 7:00 AM), https://indyweek.com/news/feds-tried-lock-journalist-life-reporting-inauguration-protests.-true-story-conspiracy-trump-s-america./ [https://perma.cc/MX8D-ATVU].

[68] Alex Zilensky, *SA Photojournalist Alexei Wood Found Not Guilty on All 7 Inauguration Day Charges*, SAN ANTONIO CURRENT (Dec. 21, 2017, 11:47 AM), https://www.sacurrent.com/the-daily/archives/2017/12/21/sa-photojournalist-alexei-wood-found-not-guilty-on-all-7-inauguration-day-charges [https://perma.cc/UCL4-YY4U].

to trial; however, the case resulted in a December 2017 not-guilty verdict on all counts.[69]

Even though journalists seldom end up being convicted of a crime arising out of newsgathering,[70] simply being arrested carries real costs. An arrest interrupts journalists' ability to continue producing coverage, obligates the journalists or their employers to pay for legal defense, and inflicts a chilling effect, inhibiting future coverage.[71]

The charges brought against journalists frequently amount to insignificant "nuisance" charges that prosecutors typically drop, such as jaywalking.[72] But police have an arsenal of rather vague and easily violated criminal codes at their disposal, including the catch-all charge of disorderly conduct, which can be violated in some jurisdictions simply by using loud profanities in a public place.[73]

---

[69] *Id.*

[70] *See* Lee Levine, Nathan E. Siegel & Jeanette Melendez Bead, *Handcuffing the Press: First Amendment Limitations on the Reach of Criminal Statutes as Applied to the Media*, 55 N.Y.L. SCH. L. REV. 1015, 1030 (2011) (citations omitted) (observing that prosecutors seldom proceed with cases against journalists except for "the rare circumstance where they directly committed an unlawful physical act, such as removing a piece of debris from the wreckage of a sabotaged aircraft, 'stealing documents,' or engaging in 'private wiretapping'").

[71] *See* Murphy, *supra* note 20, at 337; *see also* Index Newspapers v. City of Portland, 480 F. Supp. 3d 1120, 1131–34, 1143 (D. Or. 2020) (discussing journalists who were shot with non-lethal munitions, gassed, pepper-sprayed, and otherwise targeted by police while covering racial unrest in Portland, Oregon and subsequently testified that they refrained from going back to demonstration sites without protective gear, or cut their coverage short and left early, out of fear of arrest or violence by the police).

[72] *See* Rulffes, *supra* note 63, at 612 (recounting arrests of journalists during the Occupy Wall Street movement: "Journalists who were arrested were charged with violations that included disorderly conduct and unlawful assembly").

[73] *See generally* Alexandra Baruch Bachman, *WTF? First Amendment Implications of Policing Profanity*, 17 FIRST AMEND. L. REV. 65, 80–84 (2018) (examining state statutes and concluding that some broadly criminalize "boisterous" or similarly nonviolent behavior that invites misapplication against pure speech); *see also* Note*, The Demise of the Chaplinsky Fighting Words Doctrine: An Argument for Its Interment*, 106 HARV. L. REV. 1129, 1144 (1993) (critiquing the breadth of statutes that criminalize speech constituting a "breach of the peace" and commenting that "a disorderly conduct arrest often serves as

That arsenal is augmented by state eavesdropping and wiretapping statutes that police may construe as making it a crime to record a conversation without the consent of all participants,[74] even though such arrests are on dubious constitutional grounding.[75] As demonstrated above, the possibility that a journalist assigned to a scene of civil unrest may be drawn into the conflict as an arrestee is not at all farfetched; therefore, it is prudent to anticipate the information-security issues that might arise if police turn their sights from protesters to the press.

D. Locking Eyes: How Biometric Security Works

The fact that smartphones contain all manner of intimate details about people's lives is well-recognized; indeed, people regard a phone search as being comparably intrusive to a search of their own bodies—with good reason.[76] With an unlocked phone, the holder

---

punishment in and of itself rather than as the first step in the criminal process, thus marginalizing judicial review's capacity to mitigate the penalty imposed on a speaker"). For a colorful example, see generally State v. Robinson, 82 P.3d 27, 28–29 (Mont. 2003) (holding that a speaker could constitutionally be prosecuted under a "breach of the peace" statute for directing insults "f**king pig" and "f**k off a**hole" at a police officer, because the insults were "fighting words" unprotected by the First Amendment).

[74] This scenario is what happened in the case of *Glik v. Cunniffe*, 655 F.3d 78, 80 (1st Cir. 2011), in which Boston police arrested a bystander for videotaping a struggle during an arrest on a public thoroughfare on the Boston Commons, claiming that the taping constituted wiretapping in violation of Massachusetts criminal law—a charge that was ultimately found to be unsustainable under the First Amendment.

[75] *See id.* at 85 (concluding 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"); *see also* Ashley Billam, *The Public's Evolution from News Reader to News Gatherer: An Analysis of the First Amendment Right to Videorecord Police*, 66 U. KAN. L. REV. 149, 150 (2017) (collecting cases and observing that "[m]ost of the courts presented with the question have found that the First Amendment protects the public's right to videorecord police").

[76] *See* Matthew B. Kugler, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1166–67 (2014) (reporting results of a survey of 300 Americans about privacy concerns associated with border crossings: "The results show that people see the

can read the owner's text messages, gain access to the owner's email and social media accounts, view the owner's photographs and videos, and even see which websites the owner has visited.[77] For these reasons, devices routinely come equipped with safety features that prevent unauthorized access to their contents with additional security options available for installation.[78]

The two most common types of phone locks require either the entry of an alphanumeric passcode or the use of a biometric indicator, such as a fingerprint, a scan of the owner's face, or a reading of the owner's iris.[79] Consumers have found biometric security temptingly convenient and reassuring because numeric codes can be forgotten, hacked, or, if written down, stolen or copied by unauthorized people.[80]

---

intrusiveness of electronic-device searches as comparable to that of strip searches and body cavity searches, which have generally been held to require elevated suspicion. Electronic searches are the most revealing of sensitive information and are only slightly less embarrassing than the most intimate searches of the body" (emphasis omitted)).

[77] *See id.* at 1185 (observing that smartphones "contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails . . . . highly revealing and embarrassing information").

[78] *See* Heather Kelly, *Fingerprints and Face Scans Are the Future of Smartphones. These Holdouts Refuse to Use Them.*, WASH. POST (Nov. 15, 2019), https://www.washingtonpost.com/technology/2019/11/15/fingerprints-face-scans-are-future-smartphones-these-holdouts-refuse-use-them/ [https://perma.cc/FF98-JAU6] (describing how smartphone manufacturers Apple and Samsung offer standard security features that require a facial or iris scan to unlock the device, despite some customers' discomfort with sharing biometric data); *see also* Michael Grothaus, *Use These 11 Critical iPhone Privacy and Security Settings Right Now*, FAST CO. (Feb. 18, 2020), https://www.fastcompany.com/90254589/use-these-11-critical-iphone-privacy-and-security-settings-right-now [https://perma.cc/9NDX-44LY] (describing optional tools users can install to make their phones and digital accounts more secure).

[79] Carissa A. Uresk, *Compelling Suspects to Unlock Their Phones: Recommendations for Prosecutors and Law Enforcement*, 46 BYU L. REV. 601, 609 (2021).

[80] *See* Ariel N. Redfern, *Face It – The Convenience of a Biometric Password May Mean Forfeiting Your Fifth Amendment Rights*, 125 PENN ST. L. REV. 597, 603 (2021) ("Rather than having to remember or type a lengthy password, biometric passwords offer the convenience and speed of short passwords while

Besides the locking device on the initial screen, smartphones have increasingly been designed with an additional layer of encryption protection, so that data is stored on the device as a digitally scrambled garble—unreadable even to a person who might be able to bypass the initial login-screen security.[81] But technology is rapidly overtaking even that additional safeguard. Police reportedly have begun using a commercially available tool, GrayKey, that can defeat the encryption that comes with the operating system on today's Apple iPhones so that the iPhone's encrypted contents are readable when the login security is overcome.[82] Nevertheless, for most government agencies, breaking into a locked phone is "impractical for three reasons: (1) it is expensive, (2) it takes time, and (3) the technology is constantly changing."[83] Therefore, police still have every incentive to try to convince—or compel—the owner to unlock the device on the spot.

---

providing enhanced security. Accordingly, technology experts widely agree that biometric passwords are superior to their alphanumeric counterparts."); *see also* Adam Herrera, *Biometric Passwords and the Fifth Amendment: How Technology Has Outgrown the Right to Be Free From Self-Incrimination*, 66 UCLA L. REV. 778, 784 (2019) (explaining that biometric passwords are more secure than alphanumeric codes, as the default of a four-numeral passcode "can be hacked through brute force in just seven minutes"). On the other hand, a letter-number combination has one security advantage over biometrics: A combination can easily be changed if it falls into the hands of hackers, while a person's face or fingerprints cannot be changed if they are duplicated. *See* Vindu Goel, *That Fingerprint Sensor on Your Phone Is Not as Safe as You Think*, N.Y. TIMES (Apr. 10, 2017), https://www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html [https://perma.cc/AG6Z-GTRX] (citing research findings that "smartphones can easily be fooled by fake fingerprints digitally composed of many common features found in human prints").

[81] *See* Uresk, *supra* note 78, at 604–05 (explaining that when the text stored on a smartphone is encrypted, reading the text requires a complex decryption key that is considered to be impervious to cracking; without the key, the text will appear as unintelligible characters).

[82] Joseph Cox, *Cops Around the Country Can Now Unlock iPhones, Records Show*, VICE: MOTHERBOARD (Apr. 12, 2018, 12:52 PM), https://www.vice.com/en/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police [https://perma.cc/M93K-N38K].

[83] Uresk, *supra* note 78, at 611–12.

III. THE FIFTH AMENDMENT AND THE MEANING OF "TESTIMONY"

Law enforcement officers may be motivated to seize recording devices for one of two purposes: to prevent the videographer from recording what is happening or to use the recordings as evidence. These two purposes implicate different legal and constitutional doctrines. If the purpose of the seizure is to prevent the filming from taking place, then the First Amendment may provide relief for the device owner: six of the Nation's twelve geographic Circuits have stated that the act of filming police in public spaces with the intent to disseminate the footage publicly is protected by the First Amendment, and thus, police act unconstitutionally if they interdict the filming or arrest the videographer.[84] But, if police are not seeking to prevent filming or destroy images for the purpose of preventing publication but are instead confiscating smartphones for the purpose of gathering evidence, a different legal analysis likely applies. This Article focuses on the latter scenario, starting with the possible Fifth Amendment defenses that might entitle a videographer to refuse a demand to unlock a phone and make its recordings accessible.

In situations where the possessor of sought-after documentary materials is not a criminal suspect, the Fifth Amendment will not be an availing defense against compelled production of an unlocked phone.[85] However, in the often-chaotic setting of public demonstrations, law enforcement does not always carefully

---

[84] *See* Fields v. City of Philadelphia, 862 F.3d 353, 355 (3d Cir. 2017); Turner v. Lieutenant Driver, 848 F.3d 678, 690 (5th Cir. 2017); ACLU v. Alvarez, 679 F.3d 583 (7th Cir. 2012); Glik v. Cunniffe, 655 F.3d 78, 85 (1st Cir. 2011); Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000); Fordyce v. City of Seattle, 55 F.3d 436, 440 (9th Cir. 1995). More recently, the First Circuit extended its *Glik* ruling to cover not just openly recording police, but also clandestinely recording them. Project Veritas Action Fund v. Rollins, 982 F.3d 813, 833 (1st Cir. 2020). In a pre-smartphone case that could have relevance to contemporary confrontations over protest coverage, a federal district court found that the act of seizing a TV news crew's camera equipment and film constituted a forbidden "prior restraint," violating bedrock First Amendment doctrine. Channel 10, Inc. v. Gunnarson, 337 F. Supp. 634, 637 (D. Minn. 1972).

[85] *See* U.S. CONST. amend. V.

differentiate between "a suspect" and "an observer."[86] Journalists are often arrested alongside demonstrators on charges such as trespass, disorderly conduct, obstruction, and failure to disperse.[87] If journalists themselves face charges and are confronted with a demand for evidence, their first line of defense against compelled production of an unlocked phone is the Fifth Amendment's provision against self-incrimination.[88] The underlying principle of this self-incrimination privilege is to require the government to produce evidence against an individual through "the independent labor of its officers, not by the simple, cruel expedient of forcing it from his own lips."[89] To qualify for the Fifth Amendment privilege, a communication must be testimonial, incriminating, and compelled.[90] The primary issue regarding government-compelled production of a passcode or biometric key is whether the act of production is "testimonial" in nature.[91]

To be considered testimonial, an accused's act "must itself, explicitly or implicitly, relate a factual assertion or disclose information."[92] The Supreme Court has said that even the act of selecting documents to comport with the demands of a subpoena can qualify as testimonial, because that process communicates that the person targeted by the subpoena is in possession of responsive and

---

[86] *See* Sara Rafsky, *At Occupy Protests, U.S. Journalists Arrested, Assaulted*, COMM. TO PROTECT JOURNALISTS (Nov. 11, 2011, 3:01 PM), https://cpj.org/2011/11/at-occupy-protests-us-journalists-arrested-assault/ [https://perma.cc/5XFE-DPGG] (chronicling instances during a nationwide wave of economic-justice protests "in which reporters and photographers were cuffed and booked as police rounded up groups of protestors demonstrating in allegedly unauthorized places").

[87] REPORTERS COMM. FOR FREEDOM OF THE PRESS, *Police, Protesters, and the Press*, 2 (June 2020), https://www.rcfp.org/wp-content/uploads/2020/06/Police-Protesters-Press-2020.pdf [https://perma.cc/RZA2-8SHD].

[88] U.S. CONST. amend. V.

[89] Estelle v. Smith, 451 U.S. 454, 462 (1981).

[90] Hiibel v. Sixth Jud. Dist. Ct. of Nev., 542 U.S. 177, 189 (2004).

[91] *See* Erin M. Sales, *The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free From Self-Incrimination*, 69 U. MIAMI L. REV. 193, 239 (2014) (concluding that the use of biometric authentication likely forfeits Fifth Amendment protection if confronted with a demand to unlock the phone because "an analysis of physical characteristics" will not qualify as "testimonial").

[92] Doe v. United States, 487 U.S. 201, 210 (1988).

authentic documents—comparable, in the Court's view, to forcing a homeowner to recite the combination to a wall safe.[93] One court recently illustrated the distinction between a testimonial and non-testimonial act: A person may not be compelled to acknowledge the existence of an incriminating tattoo or describe its appearance, but a person may be compelled to display the tattoo in court for the jury because the latter is conduct and not testimony.[94] By this standard, the compelled production of an alphanumeric passcode is testimonial, as the production requires a statement of fact and reveals the contents of the speaker's mind.[95] This perspective is the overwhelming consensus of the courts that have directly confronted the issue of the nature of a smartphone passcode.[96]

One exception to compelled production being "testimonial" is when the government can prove that the testimonial aspect of the production is a "foregone conclusion."[97] For example, where a suspect has already voluntarily entered the passcode in the presence of law enforcement, "the testimonial value of compelling the passcode's production a second time is negligible," and the

---

[93] United States v. Hubbell, 530 U.S. 27, 36 (2000).

[94] State v. Pittman, 479 P.3d 1028, 1039 (Or. 2021) (en banc).

[95] *See* Herrera, *supra* note 79, at 799 (collecting cases and concluding that "disclosing a smartphone password – numeric or alphanumeric – is a testimonial communication which falls under the protection of the Self-Incrimination Clause").

[96] *See* State v. Johnson, 576 S.W.3d 205, 225 (Mo. Ct. App. 2019) ("In jurisdictions that have addressed this issue, the majority of cases have determined that this act of production is, in fact, a testimonial act."); *accord* State v. Valdez, 482 P.3d 861, 875 (Utah Ct. App. 2021); Pollard v. State, 287 So. 3d 649, 657 (Fla. Dist. Ct. App. 2019); State v. Trant, No. CUMCDCR201502389, 2015 WL 7575496, at *2 (D. Me. Oct. 27, 2015); Sec. & Exch. Comm'n v. Huang, No. 15-269, 2015 WL 5611644, at *1 (E.D. Pa. Sept. 23, 2015); Commonwealth v. Baust, No. CR14–1439, 2014 WL 10355635, at *3 (Va. Cir. Ct. Oct. 28, 2014). In a rare deviation from the consensus, a Florida appellate court decided that the act of divulging a passcode was *not* testimonial, in part driven by the policy consideration that using a fingerprint to unlock the same device would also not be testimonial, and the appellate court "[was] not inclined to believe that the Fifth Amendment should provide greater protection to individuals who passcode protect their iPhones with letter and number combinations than to individuals who use their fingerprint as the passcode." State v. Stahl, 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016).

[97] *Pollard*, 287 So. 3d at 653, 656.

"foregone conclusion" exception would permit compelled production.[98] Thus, compelled production of a passcode is permissible when doing so communicates no new information to the government.[99]

However, even when the government can prove that the suspect knows the passcode, some courts are hesitant to apply the "foregone conclusion" exception to the compelled production of an unlocked smartphone unless the government can show even more. In *Eunjoo Seo v. State*, the Supreme Court of Indiana held that the government needed to show that the defendant knew the password, that the data files existed on the device, and that the defendant possessed those files.[100] According to the court, this additional information implicitly conveyed to the police that the defendant's compelled production of the passcode was a foregone conclusion.[101] Thus, although "the communicative aspects of the production [fell] within the Fifth Amendment's protection," the government overcame that protection because the government showed that the government already knew the defendant possessed and could access the smartphone.[102] The court in *Eunjoo Seo* was concerned with extending the "foregone conclusion" exception, reasoning that compelled production of an unlocked smartphone, unlike the production of specific documents, "gives the government access to everything on the device, not just those files it can identify with 'reasonable particularity.'"[103] As such, the court cautioned against extending the foregone conclusion exception in a way that would give the government such unfettered access.[104]

Less than two months later, however, the New Jersey Supreme Court permitted the compelled production of an alphanumeric

---

[98] *Id.*

[99] *Id.*; *see also Pittman*, 479 P.3d at 1046 (holding that a warrant can validly compel unlocking of suspect's password-protected smartphone only if law enforcement already knows the "testimonial aspects of the act" of unlocking and if the suspect is given immunity from the use of those testimonial acts as evidence).

[100] Eunjoo Seo v. State, 148 N.E.3d 952, 958 (Ind. 2020).

[101] *Id.* at 956.

[102] *Id.* at 957–58.

[103] *Id.* at 960.

[104] *Id.*

passcode under the "foregone conclusion" exception.[105] The court found that the State's demonstration of the passcode's existence, the suspect's previous possession and operation of the smartphone, and the passcode's self-authenticating nature, made the production of the unlocked smartphone an issue of surrender, not testimony.[106] The court took issue with the analysis in *Eunjoo Seo*, asserting that the *Eunjoo Seo* court introduced "Fourth Amendment privacy principles into a Fifth Amendment inquiry" by focusing its analysis on the content to which the government gains access rather than the act of production itself.[107]

The law is even less clear regarding the government's ability to compel production of a biometric key (e.g., a finger-press or facial recognition) for the purposes of unlocking a suspect's smartphone. Most modern smartphones permit the use of both alphanumeric passcodes and biometric keys for encryption; however, not all courts treat these two security features the same for Fifth Amendment purposes. In the limited case law interpreting this issue, two prevailing philosophies have emerged.

The first philosophy is that a biometric key is functionally the same as a passcode, and therefore, if a passcode is testimonial, so too is a biometric key.[108] In *United States v. Wright*,[109] a federal district court in Nevada reasoned that, by producing a biometric key that unlocks a smartphone, a suspect is essentially testifying that the suspect has unlocked the phone before (at least at a minimum, to set up the biometric capabilities) and has "some level of control over the phone" and its contents.[110] Courts that subscribe to this

---

[105] State v. Andrews, 234 A.3d 1254, 1275 (N.J. 2020).

[106] *Id.*

[107] *Id.* at 17*; see also* State v. Johnson, 576 S.W.3d 205, 227 (Mo. Ct. App. 2019) (collecting cases that have taken varying views of what it means for disclosure to be a "foregone conclusion" and concluding that the focus must be on the state's knowledge of the information that the state is attempting to compel—that is, the passcode itself—rather than the state's knowledge of the contents of any particular file on the device).

[108] United States v. Wright, 431 F. Supp. 3d 1175, 1187 (D. Nev. 2020).

[109] *Id.* at 1175.

[110] *Id.* at 1187.

philosophy find production of a biometric key to be a testimonial act privileged by the Fifth Amendment.[111]

The alternative, second philosophy in case law, and the predominant view currently, rejects the idea that a biometric key is testimonial simply by serving the same purpose as a passcode, reasoning that their "functional equivalency" does not amount to a "legal equivalency."[112] In July 2020, a federal district court in Kentucky found that, because a biometric key could be produced "without any mental impressions, communication, or admission of mens rea from the target," such a compelled act could not be testimonial.[113] Thus, the court determined that a compelled physical act, which requires no revelation of information stored in a person's mind, is not testimonial.[114] Courts that subscribe to this point of view have determined that compelled production of a biometric feature to unlock a smartphone is no different than other compelled physical acts that have been upheld as non-testimonial, such as undergoing blood tests, providing handwriting and voice exemplars, or trying on a garment.[115]

---

[111] *See e.g.*, *In re* Residence in Oakland, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019) (finding that the compelled production of biometric key was testimonial in the context of a warrant application seeking to unlock a device); *In re* Application for Search Warrant, 236 F. Supp. 3d 1066, 1067 (N.D. Ill. 2017) (finding that the compelled production of a fingerprint to unlock a smartphone was testimonial where accessing the smartphone via that fingerprint would communicate that the defendant exercised significant control over the phone and its contents).

[112] *In re* Search Warrant No. 5165, 470 F. Supp. 3d 715, 734 (E.D. Ky. 2020); *see also* Redfern, *supra* note 80, at 600 ("The majority of courts that have addressed the constitutional issue posed by biometric passwords have determined that the Fifth Amendment does not protect individuals against compelled biometric decryption.").

[113] *In re* Search Warrant No. 5165*,* 470 F. Supp. 3d at 729.

[114] *Id.* at 730.

[115] *See e.g.*, State v. Diamond, 905 N.W.2d 870, 877 (Minn. 2018) (holding that a finger-press on a smartphone screen cannot be considered "testimonial" for Fifth Amendment purposes because a defendant does not have to engage in any mental processes to trigger the unlocking, and indeed, a defendant could even be unconscious); *In re* Search Warrant Application for Cellular Telephone v. Barrera, 415 F. Supp. 3d 832, 833 (N.D. Ill. 2019) (finding that compelling production of a biometric feature is no different than other compelled physical

The Eastern District of Kentucky further emphasized that even when the production of a biometric feature is both compelled and incriminating, the production of the biometric feature is not necessarily testimonial.[116] The court recognized that the use of biometrics might lead to incriminating evidence but ultimately held that the State did not violate the Fifth Amendment because the State would still be required to locate the incriminating evidence and prove its authenticity.[117] Since multiple individuals may have access to a device, and since files may exist on a device without an individual's knowledge or intent, "the government may still have to prove possession of the contents of the device as well as the *mens rea* connected to [the alleged] crimes."[118] Thus, the compelled production of "an immutable physical characteristic" to access a smartphone would not be testimonial where the State would still need to authenticate any incriminating evidence revealed by the act of production.[119]

In summary, unless the government can prove that an individual knows a device's passcode, the government's compelling of a suspect to produce a passcode is widely believed to violate the Fifth Amendment's privilege against self-incrimination.[120] However, some courts have inferred knowledge of a passcode from a suspect's mere possession and operation of a passcode-protected phone.[121] For this reason, a videographer should avoid entering a passcode into a phone within view of law enforcement agents, as at least some courts will consider that act to render the re-disclosure of the

---

acts that have been upheld as non-testimonial); *In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 527 (D.D.C. 2018) (finding the compelled production of a biometric feature are akin to other compelled uses of physical characteristics that courts have found non-testimonial even when the produced information would be used for investigatory rather than identification purposes).

[116] *In re* Search Warrant No. 5165, 470 F. Supp. 3d at 729.

[117] *Id.* at 734.

[118] *Id.*

[119] *Id.*; *see also Barrera*, 415 F. Supp. 3d at 833 (finding that a defendant's ability to unlock a phone was not dispositive of guilt since phones can be programmed to accommodate multiple users; therefore, the compelled production is not testimonial or incriminating in and of itself).

[120] Pollard v. State, 287 So. 3d 649, 653 (Fla. Dist. Ct. App. 2019).

[121] State v. Andrews, 234 A.3d 1254, 1275 (N.J. 2020).

passcode a "foregone conclusion," eliminating the constitutional protection of the smartphone's contents.

In contrast with numeric or alphanumeric passcodes, a majority of courts hearing the issue have found that a biometric key is not testimonial and therefore not privileged under the Fifth Amendment.[122] The distinction is best illustrated by a Virginia trial court's ruling in the afore-cited *Baust* case, where police ordered the suspect in an assault case to unlock his phone so that the police could see whether a video of the attack existed on the device, as believed by the assault victim.[123] The phone could be unlocked either by way of an alphanumeric passcode or by a fingerprint; the defendant invoked the Fifth Amendment as to both methods, but the court found that only the passcode, and not the fingerprint, qualified as testimonial, implicating the defendant's Fifth Amendment rights.[124] The Supreme Court has yet to speak to the issue, so trial courts provide much of the available authority. Currently, an individual is afforded more predictable and consistent Fifth Amendment protection by encrypting their phone with an alphanumeric passcode than with a biometric key.

Despite the current thrust of case law, policy interests may eventually give way to a different outcome—and with good reason. In the case of *In re Search Warrant No. 5165*,[125] a district court lamented being without authoritative guidance "in the unmapped territory where old law and new technology intersect" and recognized that emerging law would need to play "catch up" with technology.[126] Reaching a similar conclusion, a district court for the District of Columbia acknowledged that, as a lower court, its duty to faithfully interpret and apply Supreme Court precedent outweighed the important privacy interests at stake.[127]

---

[122] *In re* Search Warrant No. 5165, 470 F. Supp. 3d at 729.

[123] Commonwealth v. Baust, No. CR14–1439, 2014 WL 10355635, at *1 (Va. Cir. Ct. Oct. 28, 2014); *see supra* note 96.

[124] *See id.* at *4 ("In this case, the Defendant cannot be compelled to produce his passcode to access his smartphone, but he can be compelled to produce his fingerprint to do the same.").

[125] *In re* Search Warrant No. 5165, 470 F. Supp. 3d 715 (E.D. Ky. 2020).

[126] *Id.* at 735.

[127] *In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 540 (D.D.C. 2018).

In its 2014 decision in *Riley v. California*,[128] the Supreme Court may have signaled its position if presented with the issue of compelled production of a passcode or biometric feature to access the contents of a smartphone. In *Riley*, Chief Justice John Roberts emphasized that the capacity of modern cellphones to hold "the privacies of life" made their search and seizure uniquely intrusive and thus required a warrant.[129] This recognition of the immense capacity for smartphones to store intimate data could prompt the Supreme Court to find that production of a passcode or biometric feature for the purposes of unlocking a smartphone is a testimonial act—and therefore privileged by the Fifth Amendment. As one commentator has argued, smartphones are now "an extension of the self," so that the privacy considerations implicated by a search are even more profound than in traditional searches of physical spaces around which constitutional doctrine developed: "It is no longer workable to separate the action of decryption from the person, especially considering the person is now the means of decryption."[130]

IV. THE FOURTH AMENDMENT: WHAT IS WARRANTED?

Even when compelled production of an unlocked smartphone is permissible, the Fourth Amendment provides an additional layer of protection against government search and seizure. The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[131] The "touchstone of the Fourth Amendment is 'reasonableness,'" and—except for a few recognized categories of exigent situations—reasonableness normally requires law enforcement agencies to obtain a search warrant from a neutral magistrate after demonstrating probable cause to believe that the

[128] Riley v. California, 573 U.S. 373 (2014).
[129] *Id.* at 403.
[130] Redfern, *supra* note 80, at 627–28.
[131] U.S. CONST. amend. IV.

place to be searched contains evidence of a crime.[132] When a search warrant sufficiently states probable cause for the search and seizure of an electronic device, law enforcement may either access the device if the device is unlocked or attempt brute force efforts to gain entry into the device.[133] However, the critical inquiry in this context is under what circumstances law enforcement agents can compel individuals to produce a passcode or biometric feature to gain access to a device.

The taking of a fingerprint constitutes a search under the Fourth Amendment.[134] In *Hayes v. Florida*, the Supreme Court set forth criteria to justify obtaining fingerprints from an individual, requiring that (1) the government had reasonable suspicion that the suspect committed a crime, (2) the government reasonably believed that fingerprinting would establish or negate the suspect's connection with that crime, and (3) the procedure was carried out with dispatch.[135] Several courts have applied this standard in determining whether the government may compel the use of an individual's biometric features to unlock a device during the execution of a search warrant.[136]

While taking a fingerprint is considered a search under the Fourth Amendment, the Fourth Amendment status of a facial scan remains an open question. If scanning facial features is not considered a search, then no warrant is required.[137] This conclusion is logical since a person's outward appearance, particularly when attending a protest or other form of public gathering, can freely be

---

[132] Emmanuel Abraham Perea Jimenez, *The Fourth Amendment Limits of Facial Recognition at the Border*, 70 DUKE L.J. 1837, 1856 (2021) (quoting Riley v. California, 573 U.S. 373, 381 (2014)).

[133] *In re* Search Warrant No. 5165, 470 F. Supp. 3d 715, 725 (E.D. Ky. 2020).

[134] Hayes v. Florida, 470 U.S. 811, 816–17 (1985).

[135] *Id.* at 817.

[136] *See In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 526 (D.D.C. 2018); *see, e.g.*, *In re* Search Warrant No. 5165, 470 F. Supp. 3d at 725 (applying the three-pronged standard from *Hayes* to determine the legality of a biometric request during a search warrant).

[137] For simplicity, and in the absence of a conclusive consensus on the status of facial scanning, the remainder of this Article refers to fingerprinting and facial scanning collectively as the compelled production of biometric features, on the assumption that Fourth Amendment safeguards will apply.

observed by anyone—including police—without intruding on any reasonable expectation of privacy.[138] But this inference does not necessarily extend to ordering a smartphone owner to hand over a phone and hold still while the phone is held up to the owner's face for unlocking. Courts have taken a somewhat more nuanced approach to the "expectation of privacy in public" (or lack thereof) since the Supreme Court's *Carpenter v. United States* decision.[139] In *Carpenter*, the Supreme Court held that the "pings" on cellphone towers, which can be used to piece together a smartphone user's movements, implicate constitutionally protected privacy interests.[140] Thus, the act of exposing one's face to a crowd of demonstrators does not logically translate to the conclusion that the expectation of privacy is waived for purposes of the Fourth Amendment's search and seizure doctrine.

Even if police must obtain a search warrant, and the warrant is authorized, compelling a smartphone owner to unlock the device

---

[138] *See* Elizabeth Snyder, *"Faceprints" and the Fourth Amendment: How the FBI Uses Facial Recognition Technology to Conduct Unlawful Searches*, 68 SYRACUSE L. REV. 255, 261 (2018) ("The limited number of courts that have considered the applicability of Fourth Amendment protections to photographs have largely declined to find a search where a camera captures that which an individual publishes to the public."). Snyder argues that, although Fourth Amendment precedent is "bleak" for convincing a court that a search to run a person's lawfully-obtained photo through a database for matching to a suspected criminal is unlawful, there *should* be a recognized privacy interest in that transaction because exposing one's face for purposes of a photo does not necessarily imply anticipation of—much less consent to—the biometric analysis of that photo by the government. *See id.* at 260–63.

[139] *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[140] *Id.* at 2216–17; *see, e.g.*, Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 341 (4th Cir. 2021) (en banc) (citing *Carpenter* for the proposition that the reasonable expectation of privacy can be violated by "prolonged tracking that can reveal intimate details through habits and patterns" and holding that plaintiffs were entitled to a preliminary injunction against police aerial surveillance program); *see also* Matthew Doktor, *Facial Recognition and the Fourth Amendment in the Wake of* Carpenter v. United States, 89 U. CIN. L. REV. 552, 568 (2021) (arguing that, just as with the cellphone locational data at issue in *Carpenter*, "facial recognition scans of biometric data intrude into a sphere of privacy that merits protection through the Fourth Amendment's warrant requirement").

may occur only in the manner authorized by the search warrant.[141] In *United States v. Maffei*, a prosecutor compelled a defendant to convey the alphanumeric passcode of his phone; however, the warrant provided only the authority to compel production of a biometric key.[142] The court found that obtaining the defendant's passcode rather than a biometric key, constituted materially different conduct and, as such, found that the prosecutor's conduct exceeded the scope of the warrant.[143]

The government need not state with specificity the exact devices the government seeks to compel a suspect to unlock.[144] In *In re Search of [Redacted] Washington, D.C.*,[145] a warrant sought access to "any digital device which [was] capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant . . . ."[146] The court held that, so long as the government has a "reasonable suspicion that the individual's biometric features will unlock the device," the suspect may be compelled to produce a biometric feature for that device.[147] Thus, the government may compel production of a biometric key to unlock any device found on the premises that could reasonably be connected to that individual and the alleged criminal offense, as long as the procedure is carried out promptly and only against the individual subject to the warrant.[148]

The subject of the search warrant need not be a suspect of the crime for the Fourth Amendment to attach.[149] In *Zurcher*, police

---

[141] United States v. Maffei, No. 18–SW–0122 (GMH), 2019 WL 1864712, at *5 (N.D. Cal. Apr. 25, 2019).

[142] *Id.* at *4.

[143] *Id.* at *5.

[144] *In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 526 (D.D.C. 2018).

[145] 317 F. Supp. 3d 523 (D.D.C. 2018).

[146] *Id.* at 526.

[147] *Id.* at 533.

[148] *Id.*; *see also In re* Search Warrant No. 5165, 470 F. Supp. 3d 715, 725 (E.D. Ky. 2020) (finding that the government may compel an individual's biometrics if there exists reasonable suspicion that (1) the individual has committed a criminal act for which the warrant authorizes an evidentiary search, *and* (2) the individual's biometric features will unlock the device).

[149] Zurcher v. Stanford Daily, 436 U.S. 547, 559 (1978).

executed a search warrant of the *Stanford Daily*, an undergraduate student newspaper, under the suspicion that the newspaper possessed photographs documenting violence against police during a demonstration.[150] The newspaper filed a civil action, claiming that the search warrant deprived the journalists of their constitutional rights.[151] When the case made it to the Supreme Court, the Court agreed that the Fourth Amendment applied to the newsroom search but ultimately found no constitutional violation in the search because the search was "reasonable."[152] The reasonableness of the search warrant turned on whether there was reason to believe that evidence might be located on an individual's property (and there was reason to believe the *Stanford Daily* had evidence "on" its newsroom), not whether the individual being searched was criminally liable.[153]

However, the government may not broadly compel production from any or all individuals present on the premises that is the subject of a search warrant.[154] In *In re Application for Search Warrant*, the government sought authority to compel any individual present at the premises at the time of the search to provide biometrics onto any Apple device.[155] The court denied the search warrant application because the warrant was "neither limited to a particular person nor a particular device."[156] However, the court did determine that, in some instances, the government may temporarily detain individuals not subject to a warrant if the individuals are occupants of the premises being searched, but this authority did not extend to individuals who were merely present but not otherwise connected to the premises.[157]

To complicate the analysis, the Supreme Court has given police considerable latitude to conduct what is known as a "search incident

---

[150] *See id.* at 551.
[151] *Id.* at 552.
[152] *See id.* at 567–68.
[153] *Id.* at 555–56.
[154] *See e.g.*, *In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1067 (N.D. Ill. 2017).
[155] *Id.* at 1067.
[156] *Id.* at 1068.
[157] *See id.* at 1069–70.

to arrest" without a warrant. In *Chimel v. California*,[158] the Supreme Court gave its clearest guidance on the "search incident to arrest" doctrine and its limits, holding that, in the course of making a lawful arrest, police may conduct a warrantless search of the arrestee's person and any areas within the arrestee's reach or immediate control.[159] The Supreme Court's recognition of a workaround to the warrant requirement pursuant to the Fourth Amendment rested on two justifications: (1) the arrestee might grab and use a weapon, or (2) the arrestee might destroy evidence of a crime.[160] The "weapon" rationale plainly has no application to seizing and searching a journalist's phone, but police might argue that the "destruction" rationale does apply, if the journalist is being arrested and accused of a crime.

Finally, and notably, the ability to unlock a phone does not necessarily imply that police may freely review all of the phone's contents. Police may search only in places where the evidence they are authorized to seek might reasonably be found.[161] For instance, in the physical rather than digital world, a warrant authorizing police to search a house for a homeowner's shotgun would not authorize the opening of letters in the homeowner's mailbox.[162] In the context of a journalist's smartphone, an authorized search for video footage of people damaging property would not license police to also read

---

[158] 395 U.S. 752 (1969).

[159] *Id.* at 762–63.

[160] *See id.*

[161] *See, e.g.*, United States v. Pritchard, 745 F.2d 1112, 1122 (7th Cir. 1984) ("[A] search for small electronic devices justifies entry into containers in which they would fit and might reasonably be found.").

[162] *See* Terry v. Ohio, 392 U.S. 1, 18–19 (1968) ("[A] search which is reasonable at its inception may violate the Fourth Amendment by virtue of its intolerable intensity and scope . . . . The scope of the search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible.") (citations omitted); United States v. Foster, 100 F.3d 846, 850–51 (10th Cir. 1996) (holding that a warrant empowering police to search a home and barn for illegal drugs and firearms did not also authorize them to confiscate everything else of value on the premises, including the homeowner's lawnmower, television sets, clock radio, and other household items, on a mere suspicion that some of the items might have been stolen).

the journalist's emails.[163] Unlocking a secured smartphone, then, is not an all-or-nothing proposition, as an otherwise lawful search can ripen into a Fourth Amendment violation if the search exceeds its permissible scope.

In summary, the government can compel production of a biometric key from individuals that the government reasonably suspects either committed, or possess evidence of, the criminal act that is the subject matter of the warrant.[164] The compelled production may be carried out on devices subject to the warrant that the government has reasonable suspicion to believe the individual's biometric features will unlock.[165] The procedure must be carried out "with dispatch and in the immediate vicinity of the premises to be searched."[166] Additionally, the government may compel an individual to unlock a phone only in the manner authorized by the search warrant.[167] Thus, anyone in possession of sought-after documentary materials, who is not the subject of a search warrant, is under no obligation to produce an unlocked device for law enforcement.

V. THE PRIVACY PROTECTION ACT AND THE "NEWSROOM" IN AMERICA'S POCKET

While the privileges afforded by the Fourth and Fifth Amendments extend to all citizens, the Privacy Protection Act of 1980[168] ("PPA") may provide an additional layer of protection for journalists and others gathering information to inform the public. Congress enacted the PPA as a direct response to the Supreme Court's resolution in the aforementioned *Zurcher* case, in which the

---

[163] *See* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) (recognizing that the Fourth Amendment applies to a police search of the contents of an email account because the accountholder has a reasonable expectation of privacy in emails, notwithstanding the fact that the account can be accessed by the company that issued the email account).

[164] *See In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 533 (D.D.C. 2018).

[165] *Id.*

[166] *Id.*

[167] *See* United States v. Maffei, No. 18–SW–0122 (GMH), 2019 WL 1864712, at *5 (N.D. Cal. Apr. 25, 2019).

[168] 42 U.S.C. § 2000aa (1980).

Justices found no actionable constitutional violation when police raided a college newspaper's office pursuant to a judicially-issued search warrant, whereby the police confiscated cameras to search for unpublished photos.[169] Thus, while the direct inspiration for the PPA stemmed from the search of a newsroom, and the Act is sometimes colloquially referred to as a "newsroom search law,"[170] the application of its broad protections could readily extend to the memory card of a journalist's smartphone.

In short, the PPA prohibits a government officer or employee from seizing any unpublished work product or documentary materials possessed by an individual who intends to disseminate the material to the public.[171] While such materials may be obtained by lawful means, "such as [by] grand jury subpoenas and voluntary requests," these lawful means provide an individual the opportunity to immediately object and possibly assert legally recognized grounds for refusing to comply, such as privilege.[172] A surprise raid of a newsroom—or the snatch of a smartphone from a journalist's hand—provides no such opportunity.

The PPA's text provides a somewhat greater degree of protection for "work product" materials as opposed to non-work-product "documentary materials."[173] For purposes of a smartphone

---

[169] Elizabeth B. Uzelac, *Reviving the Privacy Protection Act of 1980*, 107 NW. U. L. REV. 1437, 1442–43 (2013).

[170] *See, e.g.*, Declan McCullagh & Greg Sandoval, *Journalist Shield Law May Not Halt iPhone Probe*, CNET.COM (Apr. 27, 2010, 10:43 AM), https://www.cnet.com/news/journalist-shield-law-may-not-halt-iphone-probe/ [https://perma.cc/89H8-8A75] (referring to the PPA as a "federal newsroom search law" in the context of a police investigation into how journalists obtained a prototype iPhone before its public release).

[171] 42 U.S.C. § 2000aa(a)–(b).

[172] Sennett v. United States, 778 F. Supp. 2d 655, 662 (E.D. Va. 2011), *aff'd*, 667 F.3d 531 (4th Cir. 2012); *see also* Bryan R. Kelly, *#PrivacyProtection: How the United States Can Get Its Head Out of the Sand and Into the Clouds to Secure Fourth Amendment Protections for Cloud Journalists*, 55 WASHBURN L.J. 669, 690 (2016) (explaining that the PPA "creates a substantial protection for journalists by ensuring their day in court before the government may seize any materials").

[173] *See* Uzelac, *supra* note 169, at 1445 (explaining that additional statutory exceptions allow search or seizure when materials do not qualify as "work product").

search, the bulk of materials for which a police officer might search (such as photos and videos, or recordings of audio interviews) should qualify as work product.

For the PPA to apply, government officials must have reason to believe that the targeted individual has "a purpose to disseminate" the seized materials "to the public."[174] "[W]earing press credentials, . . . carrying a video camera, and identif[ying] [one]self as 'media'" are sufficient to put government officials on notice of such an intent.[175] Importantly, protection under the PPA turns on the individual's intent to disseminate the materials to the public and not on whether the individual is a professional journalist.[176] Further, while the government must be on notice of the targeted individual's intent to disseminate, "the PPA does not require" an individual to make "an express statement of intent" to that effect.[177]

Notably, courts have recognized some exceptions to the privileges afforded by the PPA. The "suspect exception" permits the seizure of work product or documentary materials when police have "probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate."[178] Thus, this exception overrides the protection afforded to an individual's work product and documentary materials under the PPA.[179] In *Sennett v. United States*, law enforcement officers searched Sennett's residence and seized hard drives, computers, cameras, and memory cards that Sennett asserted were professional work product.[180] The court found that the "suspect

---

[174] 42 U.S.C. § 2000aa(a).

[175] Benjamin v. Peterson, No. 12–220, 2013 WL 3097271, at *6 (D. Minn. June 18, 2013).

[176] Basler v. Barron, No. H–15–2254, 2017 WL 477573, at *12 (S.D. Tex. Feb. 6, 2017); *see also* Uzelac, *supra* note 169, at 1439 ("Since 1980, the pool of those potentially covered by the Act has increased dramatically as a result of changes in the information industry . . . . [G]iven the dramatic expansion of digital publishing and home computer usage, the Act might now in fact protect any person who publishes online.").

[177] Garcia v. Montgomery Cnty., 145 F. Supp. 3d 492, 524 (D. Md. 2015).

[178] 42 U.S.C. § 2000aa(a)(1), (b)(1).

[179] *See* Sennett v. United States, 778 F. Supp. 2d 655, 656 (E.D. Va. 2011), *aff'd*, 667 F.3d 531 (4th Cir. 2012).

[180] *See id.* at 658–59.

exception" applied because there was probable cause to believe that Sennett had vandalized the Four Seasons Hotel, and the subsequent search of the suspect's apartment related to that investigation.[181] Sennett claimed to have been documenting the unrest that unfolded at the hotel as a professional photojournalist.[182] However, the court found that the fact that Sennett arrived at the hotel "within seconds of the vandals," wore clothing and a backpack similar to that of the vandals, and fled the hotel along with the vandals, collectively amounted to a reasonable suspicion that Sennett was a member of the vandal group.[183] As such, the court found that Sennett's claim of being present only as a photojournalist merely provided "[t]he possibility of an innocent explanation [that did] not vitiate properly established probable cause."[184] In sum, because the court found probable cause that Sennett participated in the vandalism, and because the seized property related to that offense, Sennett's PPA claim was barred by the "suspect exception."[185]

Illustrating the differing protections for journalistic work product versus non-work-product, an additional statutory exemption permits the seizure of documentary materials (though not deemed "work product") when the advance warning of a subpoena "would result in the destruction, alteration, or concealment of such materials."[186] This exception permits police to confiscate documentary evidence, even from people who would otherwise

---

[181] *See id.*

[182] *See id.* at 663.

[183] *Id.* at 663–64.

[184] *Id.* at 665 (quoting United States v. Booker, 612 F.3d 596, 601 (7th Cir. 2010)).

[185] *Id.* at 667. In another recent application of the "suspect" exemption, a federal district court dismissed a PPA claim brought by the operator of a parody Facebook page whose home was searched by the police department that was the target of his mockery. *See* Novak v. City of Parma, No. 1:17-CV-2148, 2021 WL 720458, at *1, *17 (N.D. Ohio Feb. 24, 2021). Whether a social media page qualifies for the protection under the PPA was not at issue; the issue was whether police could claim the benefit of the "suspect" exemption because they had a judicially issued warrant to arrest the critic for violating an Ohio statute, making it a crime to interfere with the operations of a law enforcement agency. *See id*. at *6, *17. The court found that the exemption applied. *See id.* at *17.

[186] 42 U.S.C. § 2000aa(b)(3).

qualify for PPA protection, without a warrant or hearing.[187] In *Berglund v. City of Maplewood*, plaintiffs Berglund and Zick, hosts of a public-access television show, attended a local banquet with the intent of videotaping the event for a broadcast.[188] An altercation ensued involving the plaintiffs, which resulted in Berglund being charged with disorderly conduct and obstruction.[189] Berglund had operated the video camera throughout the altercation.[190] After Berglund's arrest, police seized the camera from Zick and confiscated the videotape without a warrant.[191] Citing the "'destruction of evidence' exception," the court found that "an objectively reasonable officer would have reason to believe that Zick . . . would erase or tamper with the videotape that provided evidence of Berglund's conduct."[192] As such, the "destruction of evidence" exception permitted the warrantless seizure of the incriminating documentary material.[193]

The PPA includes two additional exceptions. The "emergency exception" permits seizure of work product and documentary materials when law enforcement has a reason to believe that immediate seizure "is necessary to prevent the death of, or serious bodily injury to, a human being."[194] The final exception permits seizure of documentary materials when the targeted individual has failed to produce materials in compliance with a subpoena and where any further delay in the investigation or trial would "threaten the interests of justice."[195] When the government seeks a search warrant under this exception, however, a journalist must be afforded an "opportunity to submit an affidavit setting forth the basis for any contention that the materials sought are not subject to seizure."[196]

---

[187] *See* Berglund v. City of Maplewood, 173 F. Supp. 2d 935, 944 (D. Minn. 2001), *aff'd sub nom.* Zick v. City of Maplewood, 50 F. App'x 805 (8th Cir. 2002).
[188] *Id.* at 940.
[189] *Id.* at 940–41.
[190] *Id.* at 941.
[191] *Id.*
[192] *Berglund*, 173 F. Supp. 2d at 949.
[193] *Id.* at 949.
[194] 42 U.S.C. § 2000aa(a)(2), (b)(2).
[195] *Id.* § 2000aa(b)(4)(B).
[196] *Id.* § 2000aa(c).

Two murky areas of the PPA are worth noting, both relating to the government accidentally obtaining otherwise-PPA-protected materials. The first is when the government incidentally seizes PPA-protected materials that are commingled with criminal evidence.[197] For example, in *Guest v. Leis*, the user of an electronic bulletin board system ("EBBS") sued the government after the government confiscated and searched his computer server in an obscenity investigation, asserting that the seizure of certain electronic files violated the PPA.[198] The court found no liability under the PPA since the "protected materials [were] commingled on a criminal suspect's computer with criminal evidence that [was] unprotected by the act."[199] The court stressed, however, that the government may not search any protected materials that the government incidentally seizes.[200]

The second murky area is when the government incidentally seizes PPA-protected materials from an individual who is not suspected of a crime to which those materials relate.[201] In *Steve Jackson Games, Inc. v. U.S. Secret Service*, Jackson operated an EBBS for the purpose of publishing articles and information about

---

[197] Guest v. Leis, 255 F.3d 325, 342 (6th Cir. 2001).

[198] *Id.*

[199] *Id.*

[200] *Id.* Although the *Guest* case ended with a decision in favor of the law enforcement agency, the case is noteworthy for recognizing standing for people who were not themselves publishers but who had furnished material to a publisher for purposes of dissemination. *See id.* at 341 (noting that the PPA is not limited to publishers but rather furnishes a cause of action to "[a] person aggrieved by a search for or seizure of materials" covered by the Act). The *Guest* ruling suggests that a person who is, for instance, a source who gives an interview to a journalist should be able to bring a claim over an unlawful search or seizure of the records of that interview, even if the journalist chooses not to bring a claim. This determination overrides the normal presumption that a person relinquishes any reasonable expectation of privacy and loses the ability to bring a constitutional challenge to a search, by voluntarily sharing information with third parties. *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

[201] *See* Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432 (W.D. Tex. 1993).

his company's products.[202] Jackson's computer was seized during an investigation into a separate EBBS operated by one of his employees.[203] At no point was Jackson suspected of any criminal wrongdoing.[204] The government agents who seized the property claimed to be unaware of Jackson's publisher status and were thus unaware that seizing the computer might violate the PPA.[205] The court concluded that the government's retention of the computer, after learning of Jackson's publisher status, amounted to a violation of the PPA.[206] Importantly, the court seemed to leave open the idea that the government could have avoided liability under the PPA by making copies of all the materials seized and returning the hardware to Jackson upon learning of his publisher status.[207] The court's suggested workaround would greatly undermine the heightened protections afforded to work product of those who are not suspects of criminal wrongdoing, though there is so far no indication that other courts are adopting this workaround.

The PPA closes significant gaps in constitutional law that would otherwise leave journalists' work product vulnerable to examination and use by law enforcement in ways that might harm confidential sources.[208] While police sometimes seek to inspect, and even destroy, the contents of smartphones on the scene where news is happening,[209] police also sometimes confiscate phones for later

---

[202] *Id.* at 434.
[203] *Id.* at 436.
[204] *Id.* at 435.
[205] *Id.* at 436.
[206] *Id.* at 441.
[207] *Id.*
[208] *See* Uzelac, *supra* note 169, at 1459 (noting that the Fourth and Fifth Amendments offer little protection if one's documents are in the possession of third parties).
[209] *See* Kiara Alfonseca, *Philadelphia Officer Investigated for Allegedly Deleting Suspect's Cellphone Video of Arrest*, ABC NEWS (June 10, 2021), https://abcnews.go.com/US/philadelphia-officer-investigated-allegedly-deleting-suspects-cell-phone/story?id=78195441 [https://perma.cc/Z4JN-7W46] (reporting on the internal investigation of a police officer seen on body-cam video apparently deleting the recording of a traffic stop from the motorist's cellphone); Angie Jackson, *Can Police Order Citizens to Delete Video of Officers? Experts Weigh in*, MLIVE (Apr. 12, 2016), https://www.mlive.com/news/grand-

examination. In the latter scenario, absent the PPA, a journalist's newsgathering materials would be vulnerable to compromise if—as is increasingly the case—police succeed in cracking the phone's security without the owner's cooperation, bypassing the constitutional protections that would have enabled the owner to refuse to unlock it.[210] If, however, police obey the strictures of the PPA, then police will not confiscate journalists' phones or attempt to look at the content of phones without the benefit of a court proceeding.

In summary, the PPA protects work product and documentary materials produced in anticipation of public dissemination from seizure by government officials.[211] The PPA applies if government officials reasonably believe the seized materials were possessed by an individual intending to distribute information to the public.[212] The PPA does not apply when police have probable cause to believe that the person possessing the sought-after materials has committed the criminal offense to which the materials relate.[213] Nor does the PPA apply when notice of a subpoena would result in the destruction, alteration, or concealment of the material.[214]

---

rapids/2016/04/can_police_order_citizens_to_d.html [https://perma.cc/GZV6-87BQ] (reporting on a lawsuit over a 2014 arrest in Grand Rapids, Michigan, in which bystanders filming the suspect's struggle with police were ordered to delete their images "for the safety of the undercover officers"); Timothy B. Lee, *Journalist Recovers Video of His Arrest After Police Deleted It*, ARS TECHNICA (Feb. 6, 2012), https://arstechnica.com/tech-policy/2012/02/journalist-recovers-video-of-his-arrest-after-police-deleted-it/ [https://perma.cc/5SSE-X6C5] (describing how, after being arrested while covering "Occupy Wall Street" protests in Miami, Florida, a photojournalist found that several videos were erased from his camera memory while the camera was in police custody).

[210] *See* Lily Hay Newman, *How Law Enforcement Gets Around Your Smartphone's Encryption*, WIRED (Jan. 13, 2021, 1:01 PM), https://www.wired.com/story/smartphone-encryption-law-enforcement-tools/ [https://perma.cc/BDD6-XQ7E] (reporting that "new research indicates governments already have methods and tools that, for better or worse, let them access locked smartphones thanks to weaknesses in the security schemes of Android and iOS").

[211] 42 U.S.C. § 2000aa(a)–(b).

[212] *Id.*

[213] *Id.* § 2000aa(a)(1), (b)(1).

[214] *Id.* § 2000aa(b)(3).

VI. THE IMPLICATIONS FOR SMARTPHONE NEWSGATHERING

Those who document protests where clashes with police are foreseeable (either as professional journalists or as citizen observers) should anticipate demands for the handing over of their devices by police and be prepared to respond. With regard to the Fifth Amendment's privilege against self-incrimination, an alphanumeric passcode is more consistently protected from compelled production by law enforcement than a biometric key, and both of these lock methods are far superior in terms of receiving protection than a device with no encryption. With regard to the Fourth Amendment, an individual is not required to produce a biometric feature to unlock a device unless the individual is the subject of a search warrant or is an occupant of the premises being searched. Even if the government identifies an individual as the subject of a warrant, oftentimes government agents must identify in their warrant application the individual's specific finger or biometric feature that is to be applied to the device.[215]

While anyone "taking to the streets" enjoys the privileges afforded by the Fourth and Fifth Amendments, it is less clear who might enjoy additional protection under the seldom-litigated PPA. The PPA protects work product, not people. Specifically, the PPA protects work product possessed by someone with the purpose of disseminating "a newspaper, book, broadcast, *or other similar form of public communication*" to the public.[216] While the language of the PPA predates Twitter, Facebook, YouTube, and Reddit, these platforms arguably represent similar forms of public communication, rendering work product and documentary materials destined for these platforms protected under the PPA. For those who can show a history of using the platform in a way comparable to a news blog (for instance, a person who maintains a Facebook page about community news events), their work product would likely be

---

[215] *In re* Search Warrant Application for [redacted text], 279 F. Supp. 3d 800, 803–04 (N.D. Ill. 2017); *see also In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 536 (D.D.C. 2018) (finding that the procedure proposed by the government for collection of the subject's biometric features requires the government to identify the exact finger to apply to the sensor).

[216] 42 U.S.C. § 2000aa(a) (emphasis added).

protected.[217] So, ostensibly, any civilian who records the events of a protest with the purpose of posting the recording on a platform open to the public could qualify for protection under the PPA, affording the civilian the opportunity to object to any government effort to obtain the documentary material.

A case before the U.S. District Court for the Middle District of Georgia recently tested the outer limits of this protection.[218] In *Dunn v. City of Fort Valley*, Dunn was a self-described citizen-journalist who composed and distributed news-like videos on his YouTube channel, which had more than 8,000 followers.[219] While Dunn was recording inside a municipal building, a law enforcement officer seized Dunn's video camera without his consent and arrested him.[220] The court found no probable cause for Dunn's arrest and thus found his PPA claim sufficient to survive a motion to dismiss.[221]

If 8,000 followers on YouTube is sufficient for an individual's documentary material to qualify for protection under the PPA, then thousands of the citizen-journalists documenting the events in Minneapolis, Portland, Chicago, and other cities across the United States should be afforded similar protection for their work product. The argument for this broad interpretation of the PPA to extend beyond professional journalists becomes even stronger where, as is often the case, law enforcement officials themselves are the focus of the filming, as courts are increasingly recognizing a compelling public interest in monitoring police doing official business in publicly viewable places.[222]

---

[217] *See, e.g.*, Simon Romero, *La Gordiloca: The Swearing Muckraker Upending Border Journalism*, N.Y. TIMES (Mar. 10, 2019), https://www.nytimes.com/2019/03/10/us/gordiloca-laredo-priscilla-villarreal.html [https://perma.cc/JAW6-QGUP] (describing an amateur watchdog journalist's popular Facebook feed, which provides citizens of Laredo, Texas, with coverage of police news, comparable to what a community newspaper might offer).

[218] *See* Dunn v. City of Fort Valley, 464 F. Supp. 3d 1347, 1354 (M.D. Ga. 2020).

[219] *Id.* at 1354–55.

[220] *Id.* at 1355–56.

[221] *Id.* at 1368.

[222] *See supra* note 83 and accompanying text.

Whether litigation under the PPA will increase as a result of recent events, and whether courts will be willing to construe the statute more broadly than the Middle District of Georgia, remain to be seen. Nevertheless, individuals chronicling protests can take steps to reduce the likelihood that documentary materials captured on their phones will be seized by law enforcement. While there is no requirement to affirmatively state one's intention to disseminate material publicly, making such intention clear puts law enforcement on notice, as required to trigger the protection of the PPA. Further, an individual who documents the criminal conduct of others should seek to differentiate from the wrongdoers in both behavior and appearance so as to minimize opportunities for the government to establish probable cause. Finally, if a person possesses documentary materials that relate to a crime for which the person is not a suspect, the person should make all efforts to indicate an intent to retain and preserve those materials until presented with a court order to turn the materials over. Taking these steps can help journalists protect their documentary material from unlawful search and seizure and can serve the interests of justice in an age when smartphones are documenting more potentially criminal activities than ever before.

VII. CONCLUSION

The public manifestly benefits when photographers and videographers can discharge their role of eyewitness to unfolding history. Not only do visual images make news coverage more credible, but visual images also make news coverage more accessible by increasing the ability of news stories to be shared, reaching large audiences through social media.[223] In the absence of independent news coverage by civilian reporters, government agencies increasingly use online channels to distribute their own images, which can be selectively edited to portray a deceptively

[223] *See* Dianna Gunn, *Most Shared Content Studied: The Post Formats That Get Shared the Most on Social Media*, REVIVE SOC.: SOC. MEDIA MKTG. (Jan. 29, 2020), https://revive.social/most-shared-content/ [https://perma.cc/8DEV-M5MG] (citing studies showing that videos receive 135% more reach on Facebook than still photographs and that posts with photos get three times more interaction from Facebook users than text alone).

favorable picture.[224] A federal judge asserted a similar concern in the context of the arrests and harassment of journalists covering demonstrations against police violence in Portland: "Without journalists and legal observers, there is only the government's side of the story to explain why a 'riot' was declared and the public streets were 'closed' and whether law enforcement acted properly in effectuating that order."[225]

Journalists should take precautions to secure their work product against search and seizure since the incentives for police officers to overstep their boundaries and make retaliatory arrests and/or destroy footage are increasingly lopsided. Officers are heavily insulated against civil liability for wrongful arrests—a product of the widely reviled doctrine of "qualified immunity."[226] For example, in 2010, the Third Circuit dismissed First Amendment claims against Pennsylvania officers who arrested an automobile passenger on wiretapping charges for videorecording the driver's conversation with police during a traffic stop.[227] The court found that qualified immunity shielded the officers against damages because, although

---

[224] *See* West, *supra* note 61, at 311–12 (describing how, during the Trump Administration, federal immigration authorities barred photojournalists and videographers from detention centers at the Mexico border that were overcrowded and unsanitary, instead distributing government-curated photos of detained children cheerfully playing with toys and attending classes).

[225] Index Newspapers LLC v. City of Portland, 474 F. Supp. 3d 1113, 1123 (D. Or. 2020).

[226] *See* Lawrence Hurley & Andrew Chung, *Before the Court: A United Front Takes Aim at Qualified Immunity*, REUTERS (May 8, 2020, 12:00 GMT), https://www.reuters.com/investigates/special-report/usa-police-immunity-opposition/ [https://perma.cc/Q485-ZHK9] (describing eclectic array of amici from across the ideological spectrum urging the Supreme Court to narrow qualified immunity, which enables government employees to escape liability for violating the Constitution if there is no prior binding legal precedent involving near-identical factual circumstances); *see also* Joanna C. Schwartz, *Suing Police for Abuse Is Nearly Impossible. The Supreme Court Can Fix That*, WASH. POST: POSTEVERYTHING (June 3, 2020), https://www.washingtonpost.com/outlook/2020/06/03/police-abuse-misconduct-supreme-court-immunity/ [https://perma.cc/Z428-S795] (decrying an "absurd" level of "hairsplitting" in qualified immunity cases that enable police to get away with unjustified use of force if no other officer has been successfully sued for factually identical misconduct).

[227] Kelly v. Borough of Carlisle, 622 F.3d 248, 251–52 (3d Cir. 2010).

federal case law generally established a First Amendment right to record police, none of the prior cases took place in the factually identical context of a traffic stop.[228] As one commentator observed, while citizens theoretically have the right under the civil rights statute, 42 U.S.C. § 1983, to seek damages against public employees who commit constitutional violations, the remedy has proven only minimally effective:

> [I]t is unworkable for videographers because the burden for establishing a municipality's liability is too heavy, qualified immunity shields offending officers, and courts do not provide adequate damages when officers violate constitutional rights . . . . Although § 1983 was promulgated to address citizens' grievances for violations of their constitutional rights, in the context of citizens filming police, it fails to remedy anything, which results in no deterrence for police officers and no protection for videographers.[229]

Holding officers accountable for ill-motivated arrests became even more difficult with the Supreme Court's 2019 ruling in *Nieves v. Bartlett*,[230] in which the Court found that police cannot be held liable under the First Amendment for a speech-punitive arrest unless the arrestee carries the burden of proving the absence of probable cause.[231] Just months after the Court decided *Nieves*, the Eighth Circuit relied on the ruling to dismiss a First Amendment claim by Tom Johnson, a former Minnesota Vikings football player, arising out of a confrontation with police outside of a nightclub.[232] Police arrested Johnson for, *inter alia*, disorderly conduct and obstructing legal process after he refused to stop filming an officer that Johnson

---

[228] *Id.* at 262–63.

[229] *See* Murphy, *supra* note 20, at 350.

[230] Nieves v. Bartlett, 139 S.Ct. 1715 (2019).

[231] *See id.* at 1724–25; *see also* Michael G. Mills, *The Death of Retaliatory Arrest Claims: The Supreme Court's Attempt to Kill Retaliatory Arrest Claims in* Nieves v. Bartlett, 105 CORNELL L. REV. 2059, 2078–79 (2020) (explaining that, as a result of the heightened burden established in *Nieves*, claims of retaliatory arrest in violation of the First Amendment are now superfluous because the same lack of probable cause would also be required to establish a Fourth Amendment claim of wrongful arrest).

[232] Johnson v. McCarver, 942 F.3d 405, 409–11 (8th Cir. 2019).

accused of manhandling him in the nightclub.[233] A district court in New York likewise relied on *Nieves* in dismissing First Amendment claims by a photojournalist who was arrested for standing in the street while covering protests against then-presidential-candidate Donald Trump.[234] Despite siding with the government, the judge lamented that the facts smacked of selective enforcement and "rais[ed] the specter of a police officer singling out a member of the media in retaliation for his First Amendment activity."[235] Although officers could be liable for damages if sued under the PPA, the opportunity to destroy incriminating footage may seem worth the risk for an officer who was caught on camera using excessive force—an act that, in and of itself, might result in legal or career jeopardy.[236] Even recourse by way of a PPA lawsuit is increasingly uncertain; at least one federal court has applied the *Nieves* standard beyond its First Amendment context, holding that the existence of "reasonably arguable" probable cause to make an arrest defeats a

---

[233] *Id.* at 408. The former football player, Tom Johnson, who was tried on the criminal charges and acquitted, was allowed to proceed on his Fourth Amendment claim alleging excessive use of force because his evidence showed that an officer slapped the smartphone out of his hand and then shocked him twice with a stun-gun although Johnson was sitting peacefully outside the nightclub. *Id.* at 411–12.

[234] Nigro v. City of New York, No. 19-CV-2369, 2020 WL 5503539, at *3 (S.D.N.Y. Sept. 11, 2020).

[235] *Id.* at *7.

[236] *See, e.g.*, Fleming Smith, *Columbia Police Officer Fired After Using Racial Slur During Five Points Dispute*, POST & COURIER (Aug. 21, 2020), https://www.postandcourier.com/news/columbia-police-officer-fired-after-using-racial-slur-during-five-points-dispute/article_e78717ec-ebe6-11ea-aef2-3b8d063937ee.html [https://perma.cc/NBY6-AGF9] (reporting that a South Carolina police officer lost his job after he was caught on a bystander's video (posted to social media) using a racial slur toward bar patrons while clearing the bar to comport with COVID-19 safety regulations); Minyvonne Burke, *Georgia Officer Fired After Video Shows Him Using Stun Gun on Woman During Arrest*, NBC NEWS (Aug. 22, 2020), https://www.nbcnews.com/news/us-news/georgia-officer-fired-after-video-shows-him-using-stun-gun-n1237773 [https://perma.cc/6A6A-GSKV] (reporting that a suburban Atlanta police department fired an officer caught on cellphone video, which went viral on the Tik Tok video platform, cursing at a woman and shocking her with a stun-gun).

journalist's statutory claim for unlawful search and seizure under the PPA as well.[237]

The disciplinary system for law enforcement provides no more of a dependable check on police than the civil justice system.[238] Officers generally escape punishment, even when caught using force against unarmed civilians without apparent justification—as was the case in the 2020 police killing of George Floyd that spurred a national movement for racial justice and police accountability.[239] Derek Chauvin, the Minneapolis officer convicted of murdering Floyd, had accumulated at least eighteen previous citizen complaints, including several complaints alleging the unjustified use of force resembling his lethal interaction with George Floyd.[240] Yet, Chauvin only twice received disciplinary consequences and never lost his job or certification as a police officer.[241] In recent

---

[237] Am. News & Info. Serv., Inc. v. Gore, 778 F. App'x. 429, 431 (9th Cir. 2019) (unpublished).

[238] *See* Rachel Moran, *Ending the Internal Affairs Farce*, 64 BUFF. L. REV. 837, 844 (2016) (characterizing police internal affairs processes as "an irresponsible and, frankly, farcical method of responding to misconduct claims").

[239] Mollie Simon, *Few Cops We Found Using Force on George Floyd Protesters Are Known to Have Faced Discipline*, PROPUBLICA (June 17, 2021), https://www.propublica.org/article/few-cops-we-found-using-force-on-george-floyd-protesters-are-known-to-have-faced-discipline [https://perma.cc/VW7N-RHAF] (reporting results of a survey of dozens of law enforcement agencies that showed, despite hundreds of documented instances of police tear-gassing or otherwise using force to suppress nonviolent and nonthreatening protests during 2020, only 10 officers have been documented as facing any discipline).

[240] *See* Jamiles Lartey & Abbie VanSickle, *"That Could Have Been Me": The People Derek Chauvin Choked Before George Floyd*, MARSHALL PROJ. (Feb. 2, 2021), https://www.themarshallproject.org/2021/02/02/that-could-have-been-me-the-people-derek-chauvin-choked-before-george-floyd [https://perma.cc/UHL5-UFVL] (reporting that Chauvin was the subject of twenty-two complaints or internal affairs investigations over his nineteen-year career with the Minneapolis Police Department, including multiple complaints lodged by people who—like George Floyd—were pinned to the ground in ways that constricted their breathing).

[241] *See* Dakin Andone, Hollie Silverman & Melissa Alonso, *The Minneapolis Police Officer Who Knelt on George Floyd's Neck Had 18 Previous Complaints Against Him, Police Department Says*, CNN (May 29, 2020), https://www.cnn.com/2020/05/28/us/minneapolis-officer-complaints-george-

years, police so often have arrested, beaten, and gassed journalists at protests (either indiscriminately lumping the journalists in with demonstrators or selectively targeting the journalists simply for being journalists) that news organizations have been forced to take the extraordinary step of suing for injunctive relief against continued abuses, doing so successfully in both Minneapolis[242] and Portland.[243] Neither internal nor external checks appear especially effective in preventing ill-disposed officers from misusing their authority to suppress media coverage.

For all of these reasons, journalists recording scenes of civil unrest—where confrontations between civilians and law enforcement officers are foreseeable—cannot confidently assume that police will respect their constitutional right to gather the news. Accordingly, journalists should consider precautions to safeguard their digital communications (for example, by logging out of social media accounts or messaging apps not currently being used) on the assumption that their smartphones might be seized. Both the *Nieves* ruling and the statutory exceptions to the PPA provide incentives for officers to look for ways to charge journalists with crimes. Anyone

---

floyd/index.html [https://perma.cc/6W2Y-L4ZW] (quoting Minneapolis police authorities who said Chauvin had been named in eighteen prior complaints, only two of which resulted in disciplinary action).

[242] *See* Goyette v. City of Minneapolis, 338 F.R.D. 109 (D. Minn. 2021) (entering a temporary restraining order against Minneapolis police accused of shooting journalists with rubber bullets and disregarding an exemption for newsgathering in the governor's curfew order, which interfered with journalists' ability to cover protests following George Floyd's killing).

[243] *See* Index Newspapers LLC v. City of Portland, 480 F. Supp. 3d 1120 (D. Or. 2020), *aff'd*, 977 F.3d 817 (9th Cir. 2020) (granting a preliminary injunction against federal law enforcement agencies, enjoining arresting, searching, using force against, or otherwise interfering with journalists and legal observers lawfully conducting business at the scene of racial justice protests, after finding that agents continued to intentionally target journalists in defiance of an earlier temporary restraining order); *see also* Woodstock v. City of Portland, No. 3:20-cv-1035, 2020 WL 3621179 (D. Or. July 2, 2020) (granting a similarly worded temporary restraining order against city and state law enforcement personnel in Portland, based on testimony that police repeatedly threatened journalists with arrest if the journalists remained on scene of the demonstrations, did arrest three journalists even after knowing they were members of the media, and shoved an ACLU lawyer wearing conspicuous attire identifying her as a legal observer).

planning to document and share images of protest would be well-advised to anticipate being arrested—or, at the very least, confronted with a demand to surrender a smartphone—and take measures to secure their work product against being searched, seized, or destroyed.