SEARCH WARRANTS FOR DIGITAL SPEECH

Effy Folberg[*]

22 YALE J.L. & TECH. 318 (2020)

This Article explores how the Fourth Amendment regulates digital search warrants when the government searches for our conversations. In doing so, it examines the most popular approaches to search warrant regulation: search protocols and use restrictions. These approaches give rise to a previously unexplored trilemma that is created when the Fourth Amendment limits how the government uses data and searches for it. This Digital Disclosure Trilemma means that if the Fourth Amendment is interpreted to limit the scope of useable evidence or how the government conducts a search, such limitations will conflict with the government's Brady obligation to conduct exhaustive searches of data, discovery obligations, and the obligation not to distribute child pornography. These conflicts will either undermine the purpose of the search warrant limitation or cripple police investigations.

Instead, this Article argues for a First Amendment approach to regulate search warrants. Under this approach, the government is required to make an ex ante commitment to describing the content or metadata parameters that the sought speech would meet. But there would be three important limits. First, the Article argues that the foregone conclusion doctrine derived from the Fifth Amendment is a First Amendment doctrine limiting the breadth of a search warrant. Second, any overseized materials would be precluded by a use restriction. Third, the Article argues that the First Amendment provides a constitutional basis for independent search executors to provide for taint teams to solve the Digital Disclosure Trilemma and crimes involving a continuous course of conduct. Finally, the Article explores when digital speech, according to current precedent, is protected by this model, and addresses how a First Amendment theory to the Fourth Amendment could revolutionize litigation over the good-faith exception.

---

[*] Former Staff Attorney, Department of Public Advocacy. This project has benefited from the help and advice of Alex Abdo, Ben Balter, Michael Benza, Heather Gatnarek, Jennifer Stisa Granick, Lewis Katz, Erin Lueker, Cassandra Robertson, Peter Robinson, and Corey Shapiro. Special thanks to Shannon Brooks-English who has provided an immeasurable amount of advice and support. Finally, thanks to my clients for letting me into your lives and giving me the inspiration to share what I have seen. Finally thank you to Shili Shao, Sara Worth, and the rest of the *Yale Journal of Law and Technology* for editorial assistance.

TABLE OF CONTENTS

INTRODUCTION

In *State v. Knoefel*,[1] a Willoughby Hills, Ohio detective obtained a search warrant authorizing police to search several cell phones for "anything in connection with the crimes of Murder and/or Aggravated Murder."[2] Probable cause to search the phones was based upon the following: (1) the phones were found in the bedroom where the murder took place; (2) the suspect had been in the room shortly before the victim was killed; and (3) in the detective's training and experience, it was common for individuals of the suspect's age to use digital devices to communicate.[3] The warrant authorized the search of the phones'

> central processing units, SIM card, screen, processor chips and/or any other storage device, assigned phone number for cell phone device; all stored text messages, images, photographs, emails, recently dialed telephone numbers, both incoming and outgoing calls, address books/contacts lists and any other electronic, digital information, or data stored in electronic form, including read and unread data and/or erased/deleted messages and/or images.[4]

Even though the warrant "authoriz[ed] the police to search the entire contents of the phone" for anything connected to the homicide, the court found "this [breadth] does not mean that the warrant lacks specificity."[5] This level of particularity was satisfactory because "the police did not know who the phones belonged to, the victim was dead, the suspect claimed no memory of the events, and there was no apparent motive for the crime."[6] Even if the search was a "'fishing expedition,'" the court held "it is not, for that reason, violative of the Constitution."[7] At trial, text messages between Knoefel and his wife, the victim, were used to show that their marriage had been deteriorating.[8]

However, the U.S. Supreme Court had found fifty years prior that a search warrant authorizing the police to seize a similar laundry list of documents to search for evidence of a crime was

---

[1] No. 2014-L-088, 2015-Ohio-5207 (Ohio App. 2015).
[2] *Id.* ¶ 126.
[3] *Id.* ¶ 124.
[4] *Id.* ¶ 128.
[5] *Id.*
[6] *Id.* ¶ 130.
[7] *Id.* The court described the defendant's characterization of the search as a fishing expedition as "pejorative," but the court still appears to view a fishing expedition as not violating the Constitution. *Id.*
[8] *Id.* ¶ 21, 29, 131-32.

unconstitutional.[9] In *Stanford v. Texas*, the Court held that a warrant violated the Fourth Amendment's particularity requirement when it authorized the seizure of "books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings, and other written instruments concerning the Communist Party of Texas" to investigate a conspiracy to overthrow the United States government.[10] Upholding such a warrant would be, according to the Court, "false to the terms of the Fourth Amendment, false to its meaning, and false to its history."[11]

The history referenced by the *Stanford* Court was the history of the First and Fourth Amendments.[12] For the *Stanford* Court, because of the historical use of search warrants to suppress speech, warrants must describe the speech sought with "scrupulous exactitude" if the government seeks to seize books "for the ideas which they contain."[13]

In 2015, the *Knoefel* court cited neither *Stanford* nor the First Amendment in upholding the cell phone warrant. *Knoefel* is not an outlier in its silence on the First Amendment implications of digital search warrants. Courts in multiple jurisdictions have upheld similarly broad warrants for speech without mentioning the First Amendment or *Stanford*.[14] Moreover, in the Department of Justice's manual on the legality of digital search warrants, the words "scrupulous exactitude" do not appear, while the phrase "First Amendment" appears almost exclusively in reference to search warrants issued for the work of journalists.[15]

Indeed, scholars and judges have mostly declared the particularity requirement unhelpful in the era of digital search

---

[9] *Stanford v. Texas*, 379 U.S. 476 (1965).
[10] *Id.* at 478-79.
[11] *Id.* at 486.
[12] *Id.* at 481-85.
[13] *Id.* at 485.
[14] *See, e.g.*, United States v. Ulbricht, 858 F.3d 71, 104 (2d Cir. 2017); United States v. Triplett, 684 F.3d 500, 504-05 (5th Cir. 2012); United States v. Richards, 659 F.3d 527, 539 (6th Cir. 2011); People v. Farrsiar, 2015 WL 2329071, at *6 (Mich. App. May 14, 2015); Moore v. State, 160 So. 3d 728, 731 (Miss. Ct. App. 2015); Hedgepath v. Commonwealth, 441 S.W.3d 119, 121-22 (Ky. 2014); People v. Watkins, 994 N.Y.S.2d 816, 818 (N.Y. Sup. Ct. 2014); United States v. Roman, 2014 WL 6765831 (S.D.N.Y. Dec. 1, 2014). For a more extensive list of courts upholding laundry-list warrants, see Adam Gershowitz, *The Post*-Riley *Search Warrant: Search Protocols and Particularity in Cell Phones*, 69 VAND. L. REV. 585, 601-14 (2014).
[15] *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, U.S. DEP'T OF JUSTICE 100-09 (3d. ed. 2009) (explaining Zurcher v. Stanford Daily, 436 U.S. 547 (1978), a case involving a search warrant on a newsroom and the legislative response to *Zurcher*) (hereinafter DOJ Manual). The phrase "First Amendment" appears only one other time in a parenthetical citation discussing searches at the border. *Id.* at 39.

warrants.[16] The Sixth Circuit, in its survey of particularity challenges to digital search warrants, has concluded that "the federal courts have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers."[17] Few court opinions even reference the First Amendment implications of digital search warrants, and those that do tend to summarily analyze the issue.[18] Although scholarship exists on the intersection among the First and Fourth Amendments and digital technology, this literature focuses on why the First Amendment mandates that digital information be protected by the warrant requirement.[19] Now that *Carpenter v. United States*[20] and *Riley v. California*[21] have settled that the government needs a warrant to obtain access to private data on cell phones or sensitive data held by third parties, the next question is whether the intersection between the First and Fourth Amendments can regulate search warrants for digital speech.

After explaining the history of search warrants in Part I, this Article begins to answer this question in Part II by examining the problem of particularity for digital search warrants and the two most prominent theories for limiting the scope of digital search warrants. Because the seizure of digital data requires that the government extract the entire contents of a digital device, the government always *over*-seizes data when it executes a digital search warrant.[22] To counteract this overseizure, scholars and courts have proposed that magistrates use "search protocols," which affect how the

---

[16] *See, e.g.*, Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 EMORY L.J. 49 (2018); Gershowitz, *supra* note 14; Marc C. McAllister, *Rethinking Student Cell Phone Searches*, 121 PENN ST. L. REV. 309, 348-49 (2016); William Clark, Note, *Protecting the Privacies of Digital Life: The Fourth Amendment's Particularity Requirement and Search Protocols For Cell Phone Search Warrants*, 56 B.C. L. REV. 1981 (2016); Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. ONLINE 1 (2011).

[17] United States v. Richards, 659 F.3d 527, 539 (6th Cir. 2011).

[18] *See, e.g.*, State v. Besola, 359 P.3d 799, 803 (Wash. 2015); Porath v. State, 148 S.W.3d 402, 410 (Tex App. 2004); Mink v. Knox, 566 F. Supp. 2d 1217, 1228-29 (D. Colo. 2008); United States v. Clough, 246 F. Supp. 2d 84, 87-88 (D. Maine 2003).

[19] Alex Abdo, *Why Rely on the Fourth Amendment to the Do the Work of the First?*, 127 YALE L.J.F. 444 (2017); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1230-32 (2016); Michael Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 NAT' L SECURITY L. & POL' Y 247 (2016); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611 (2015).

[20] 138 S. Ct. 2206 (2018).

[21] 573 U.S. 373 (2014).

[22] Orin S. Kerr, *Search Warrants in An Era of Digital Evidence*, 75 MISS. L.J. 85, 86-87 (2005) (describing the two-step process wherein government agents must seize more than is permitted by the search warrant and then filter for the sought-after evidence in the second step).

government searches for data on the device, or that trial court judges enforce "use restrictions," which prohibit the government from using overseized evidence at trial.

Part II argues that both approaches overlook their creation of what I call the Digital Disclosure Trilemma. The trilemma is created because once digital evidence comes within the government's custody and control, the government has up to four obligations in handling that data: (1) the order of the search warrant; (2) its *Brady* obligations; (3) its discovery obligations; and (4) its obligation not to distribute child pornography in discovery. If the scope of the search is limited by a search protocol or if overseized data is excluded by a use restriction, a conflict is created with the government's exhaustive *Brady* and discovery obligations to exhaustively search for and disclose information.

Part III explores how a First Amendment-based theory of particularity could instead be used to limit the scope of search warrants for digital data. Based on the history of the First and Fourth Amendments, I argue that warrants that give officers discretion to determine what digital data relates, concerns, or is relevant to a particular offense should be considered impermissible general warrants. For a warrant to be sufficiently particular under *Stanford*, the warrant must describe *ex ante* the data or metadata parameters to be employed by the executing officer. A warrant that fails to meet this particularity standard is too vague to avoid the unconstitutional suppression of protected speech.

To determine how broad the scope of a search warrant should be, the "foregone conclusion" doctrine—which is now used to overcome a Fifth Amendment response to a subpoena—should be employed as a First Amendment doctrine for search warrants. Both *Stanford* and the foregone conclusion doctrine note the constitutional problems with placing discretion to decide what is responsive to the compulsory process with the officer executing a search warrant or the records custodian for a subpoena. Whereas the Fifth Amendment is concerned with an individual being compelled to testify against oneself, the First Amendment is concerned with whether the warrant is pretextual or vague. This Article argues that under the First Amendment, any speech that is seized in excess of the Foregone Conclusion Floor should be excluded from evidence. This could be achieved through elimination of the so-called "plain view" exception or with a use restriction.

Part IV explores some of the applications and limits of the scrupulous exactitude model. First, the Article argues that a government seizes someone's papers "for the ideas which they contain"[23] when the government seeks to obtain evidence to show that a person's thoughts or actions conformed with the content of the

[23] *See supra* note 14.

papers. The basis for this conformity test is derived from *Stanford* itself. As Texas sought to seize Communist literature to show the defendant was participating in a communist overthrow of the government, the conformity test merely universalizes this logic to apply to all speech which the government seeks to show conformity of mind or conduct to the data's contents. Therefore, as a general matter, the Article argues that spoken communications between people should be subject to this standard whereas metadata such as contact lists, or a list of phone applications would not be. Second, as a descriptive matter, the Article predicts that business records will not receive enhanced speech protections from courts, and discusses the theoretical basis and consequences of a business records exemption.

Finally, Part V argues that a model based on the First Amendment is uniquely suited to ensure that unlawfully seized evidence is actually suppressed. Although the exclusionary rule is supposed to suppress unlawfully seized evidence, the Roberts Court's expansion of the good-faith exception to the exclusionary rule has limited its application. Part V explains how a scrupulous exactitude model fits into multiple clearly established exceptions to the good-faith exception. It then concludes by explaining how criminal defense attorneys should be able to leverage the harms to the First Amendment and to individual clients to preclude application of the good-faith exception.

I. SEARCH WARRANTS FOR SPEECH IN A PRE-DIGITAL ERA

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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.[24]

From a textualist perspective, "papers" are a distinct category, the protection of which is both required and distinct from that of "persons, houses . . . and effects." After all, if the protection of our homes was sufficient to protect our papers, then the reference to "papers" would be superfluous.[25] Since the Fourth Amendment prohibits both the unreasonable search and seizure of someone's papers and the place where those papers are stored, papers are doubly

[24] U.S. CONST. amend. IV.

[25] Harmelin v. Michigan, 501 U.S. 957, 978 n.9 (1991) (noting a prohibition against interpreting part of the Constitution as superfluous).

protected. As a practical matter, this double protection has historically required the government to learn of the existence of a paper's contents through independent means in order to obtain a search warrant for that paper.

The two English cases that inspired the creation of the Fourth Amendment, *Wilkes v. Wood* and *Entick v. Carrington*, noted the importance of the double protection of papers.[26] John Wilkes, a member of the British Parliament, was the anonymous publisher of the satirical paper *The North Briton*. In *The North Briton*, Wilkes lampooned the British government's peace treaty concluding the Seven Years' War as being too favorable to the French. For instance, when the terms of the agreement were published, Wilkes, through the *North Briton*, lamented that "[i]t is with the deepest concern, astonishment, and indignation that the *Preliminary articles of Peace* have been received by the public."[27] When the treaty was signed, Wilkes mockingly thanked the British government officials "from sav[ing] *England* from the certain ruin of success."[28]

Because of these repeated criticisms, Lord Halifax launched an investigation into Wilkes, but he did not stop there. He also issued a warrant to seize items regardless of those items' connection to the investigation of the writer of *The North Briton*. Commonly called a general warrant, this warrant authorized the messengers to "seize . . . papers" belonging to those who the State had "a bare suspicion of a libel" by means of "a general warrant, without nam[ing] of the person charged."[29] In total, fifty people, including Wilkes, were arrested and all persons had their papers seized over three days.[30] Wilkes sued the messengers for trespass.

At trial, Wilkes' butler claimed to witness the search, stating that three messengers "rummaged all the papers together they could find, in and about the room" and "fetched a sack and filled it with papers."[31] Another messenger went downstairs and broke open locks and proceeded to seize all the papers inside, and then continued to search every room in the house.[32] In defense, the messengers claimed that they were justified in trespass due to their possession of a warrant. Such a defense caused Chief Judge Pratt to impress upon

---

[26] For scholarly discussion of how these cases influenced the Founders, see Price, *supra* note 19, at 254-58.

[27] John Wilkes, *North Briton No. 28*, *in* 2 THE NORTH BRITON 154 (printed for John Mitchell and James Williams 1764); *see also* Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1199-205 (2016) (providing more examples of Wilkes's criticisms).

[28] John Wilkes, *North Briton No. 31*, *in* 2 THE NORTH BRITON 173, 175; *see also* Donohue, *supra* note 27, at 1201.

[29] Wilkes v. Wood, 98 Eng. Rep 489, 490 (C.B. 1763).

[30] NEIL LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 43-44 (Johns Hopkins 1937).

[31] *Wilkes*, 98 Eng. Rep. at 491.

[32] *Id.*

the jury that "[i]f such a power is truly invested in a Secretary of State, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject."[33] The jury subsequently found for Wilkes and awarded him 1,000 pounds.[34]

Viewed within today's constitutional framework, Wilkes's speech would constitute protected political speech under the First Amendment.[35] For instance, the Court in has declared that "if the First Amendment has any force, it prohibits Congress from fining or jailing citizens, or associations of citizens, for simply engaging in political speech."[36] Consequently, Lord Halifax's warrant raises the question of whether a search warrant can be considered a means of suppressing protected speech.

But at that time, arguing that Wilkes's speech was socially valuable was unlikely to succeed. For instance, even though Lord Camden struck down a general warrant for seditious libels, he explicitly noted his disapproval of these publications. For Lord Camden, these criticisms of the government or "libels" had been punished "with reason" because "these compositions debauch the manners of the people."[37]

Perhaps realizing that a free speech argument would not be successful, Wilkes focused his argument on the intrusion entailed in having one's irrelevant private speech exposed to potential seizure in an unrelated criminal prosecution. Wilkes argued that seizing someone's "most private concerns" was egregious, and that it was incapable of being cured through reparations.[38] He was also concerned that "some papers quite innocent in themselves, might, by the slightest alteration, be converted to criminal action."[39] Thus, the privacy in papers that Wilkes envisioned was in the private papers that the government did not know existed but could potentially use as evidence of a crime.

Two years later, John Entick published a paper known as the *British Monitor*, which derided British elites and government officers in the same manner as Wilkes had.[40] In response to Entick's criticisms, Lord Halifax issued a general warrant. To avoid the issue

---

[33] *Id.* at 498.
[34] *Id.* at 499.
[35] *See, e.g.*, Rankin v. McPherson, 483 U.S. 378 (1978) (holding that the First Amendment permitted an employee to speculate that the perpetrator of an assassination attempt on Ronald Reagan was black based solely upon Reagan's potential cuts to government social welfare programs).
[36] Citizens United v. Fed. Elec. Comm'n, 558 U.S. 310, 349 (2010).
[37] Entick v. Carrington, 19 How. St. Tr. 1129, 1074 (C.P. 1765).
[38] *Wilkes*, 98 Eng. Rep. at 490.
[39] *Id.*
[40] For a description of papers that lead to the warrant in *Entick v. Carrington*, see Donohue, *supra* note 27, at 1196-97.

encountered in *Wilkes*, the warrant was limited to Entick's home, but still authorized the seizure of all of Entick's papers.[41] Lord Camden nevertheless found the warrant unlawful.

In finding for Entick in his suit for trespass, Lord Camden observed that the word "papers" was not limited to libelous papers; instead, the word was "general, and there is nothing in the warrant to confine it; nay, I am able to affirm, that it [was] . . . executed in its utmost latitude [as in *Wilkes v. Wood*]."[42] Lord Camden observed that "the great end, for which men entered into society, was to secure their property."[43] Therefore, any nonconsensual invasion of property constituted a trespass which must be justified.[44] Lord Camden then shifted his focus to personal property by noting that papers are the "owner's goods and chattels[,]" and "though the eye cannot . . . be guilty of a trespass, . . . where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect."[45] To find otherwise "would be subversive of all the comforts of society."[46]

After Lord Camden concluded that there was an absence of legal authority to support the general warrant,[47] he remarked that a cost-benefit analysis favored ruling for Entick. Many of his reasons were specific to the problems of seditious libel. But the most noteworthy one for our purposes was Lord Camden's belief that such searches would cause compulsory self-incrimination, as the contents of the paper could incriminate the possessor.[48]

Lord Camden recognized that two injuries occur when someone's eyes see a private paper during the search of a home. The first injury occurs with the trespass to the area where the papers are stored, and the second occurs when someone sees the papers' contents. Intuitively, recognizing these two injuries helps show that security in the information (the papers) and security in a private location (the place) have been violated. But Lord Camden is never that explicit. Instead, he claims without explanation that such searches would be "subversive of all the comforts of society."

From a First Amendment standpoint, this lack of explanation of is regretful. The theory of chilling effects recognizes that if people know that possessing controversial speech can lead to liability, they will not create, store or associate with such controversial speech. The injury is societal. But if the focus is solely on self-incrimination, the

---

[41] *Id.*
[42] *Entick*, 19 How. St. Tr. at 1065.
[43] *Id.* at 1066.
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.* at 1067-73.
[48] *Id.*

harm experienced is reduced to an evidentiary question at trial, and the societal impacts fall out of the equation.

Boyd v. United States[49] is the result of the Supreme Court losing sight of (or never realizing) the First Amendment implications of *Entick* and *Wilkes*. The case concerned the constitutionality of a federal statute that permitted a U.S. attorney to request that a person produce documents after the U.S. attorney described their contents.[50] If the requesting party refused to produce the papers, the U.S. attorney's allegations of what the papers contained would be construed as an admission.[51] At issue was the request for an invoice concerning a shipment of glass which the government believed was fraudulently created to avoid the payment of customs duties.[52]

Even though the Act only required the production of documents, the Court controversially concluded that the request for the invoice was a search because the production of the invoice "effects the sole object and purpose of [a] search and seizure."[53] The larger question, however, was whether such a search was reasonable. After explaining *Entick's* historical significance to the Constitution,[54] the Court interpreted *Entick* as holding "any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods, is within the condemnation of [*Entick*]. In this regard, the Fourth and Fifth Amendments run almost into each other."[55]

From this framing, *Boyd* concluded that the Fourth and Fifth Amendments worked synergistically. A reasonable search could be determined by looking at the purpose of a search to gather evidence to convict someone. Because searches are "are almost always made for the purpose of compelling a man to give evidence against himself"[56] (e.g., the target of the search warrant is also the suspect), that would be similar to someone giving evidence to incriminate themselves. Because the Constitution forbids self-incrimination, a search for such information must be unreasonable.[57]

This reading of *Entick* missed that court's broader suggestion that protecting "the comforts of society" by outlawing general searches was a societal, rather than individual, problem. However, the *Boyd* Court likely did not consider the First Amendment implications of search warrants for papers because the First

---

[49] 116 U.S. 616 (1886).
[50] *Id.* at 619-20.
[51] *Id.*
[52] *Id.* at 618.
[53] *Id.*
[54] *Id.* For a discussion of the importance of *Entick* and *Wilkes* to the creation of the Fourth Amendment, see generally Price, *supra* note 19.
[55] *Id.* at 630.
[56] *Id.* at 633.
[57] *Id.*

Amendment case law did not exist.[58] The early twentieth century dissents which would eventually become the cornerstones of modern First Amendment jurisprudence had not been written yet.[59]

Despite this (mis)reading of *Entick*, papers under *Boyd* received enormous protection because of the creation of "the mere evidence" rule.[60] This rule provides that the government's right to own property, such as stolen goods, counterfeit money, instrumentalities of the crime, was stronger than the target of the search warrant.[61] However, the government could never have a stronger claim to own an object because it was "mere evidence" of a crime.[62] Consequently, standard police practices today such as collecting a buccal swab of DNA or clothes would be prohibited. Unsurprisingly, the rule would not last.

The collapse of the mere evidence rule occurred while the Court was undergoing a revolution in its understanding of why the Fourth Amendment protected certain items. In *Warden v. Hayden*,[63] the Court overturned the "mere evidence" rule and *Boyd*'s requirement for the government to demonstrate a superior right to title in the property. At issue was whether a search warrant for a home where the police sought to seize clothes as evidence of murder was lawful.[64] Justice Brennan, writing for the majority, declared:

> Searches and seizures may be "unreasonable" within the Fourth Amendment even though the Government asserts a superior property interest at common law. We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts.[65]

Later in that term, the Court decided *Katz v. United States*,[66] which led to the creation of the expectation of privacy test and

---

[58] *See* Tim Wu, *Is the First Amendment Obsolete?*, 117 MICH. L. REV. 547, 551-52 (2018) (noting that the First Amendment remained dormant until the 1920s).
[59] *Id.*
[60] Gouled v. United States, 255 U.S. 298, 309 (1921) (holding that the government "may not be used as a means of gaining access to a man's house or office and papers solely for the purpose of making search to secure evidence to be used against him in a criminal or penal proceeding.").
[61] *Id.*
[62] *Id.*
[63] 387 U.S. 294 (1967).
[64] *Id.* at 296.
[65] *Id.* at 304.
[66] 389 U.S. 347 (1967).

further distancing from property concepts.[67]

Perhaps the disastrous holding in *Boyd* blinded the Court from what *Boyd* did well: protect the privacy of written documents. Although the Court would briefly embrace heightened protections for search warrants for First Amendment-protected material, this case law has remained largely dormant after the Warren Court.[68] Instead, the Burger and Rehnquist Courts would significantly reduce the protection of papers. The Court would find in *United States v. Miller*[69] and *Smith v. Maryland*[70] that the fact a person had conveyed information to a third party—financial information in *Miller* and a phone number in *Smith*—demonstrated that there was no reasonable expectation of privacy in that information. Consequently, most papers, if they were ever shared with anyone, lost all Fourth Amendment protection. Privacy became equated with secrecy. It is not a surprise that this state of Fourth Amendment doctrine has engendered enormous criticism from jurists and commentators.[71]

In sum, the history of the Fourth Amendment shows that the Court has never had a cohesive framework for regulating searches for informational privacy. And the lack of such a framework is more of an accident than the result of intentional planning. When *Boyd* was decided, the Court lacked any coherent concept of the First Amendment. The mere evidence rule may have stifled the collection of evidence, but an unappreciated benefit was its strong protections for privately recorded information. Once the Court realized the faults of *Boyd*, the Court replaced the mere evidence rule with the expectation of privacy test and the third-party doctrine. These doctrines significantly limited privacy protections for papers. As police are now interested in the modern-day equivalent of papers (text messages, emails, etc.),[72] Fourth Amendment doctrine is unprepared to regulate search warrants for digital speech.

---

[67] For a discussion of how the Court distanced itself from property concepts, see Orin Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67 (2013).

[68] *See infra* Part III.A

[69] 425 U.S. 435 (1976).

[70] 442 U.S. 735 (1979).

[71] Carpenter v. United States, 138 S. Ct. 2206, 2236 (2018) (Gorsuch, J., dissenting).

[72] *See id.* at 2222 (suggesting that in dicta that emails are a modern-day equivalent of papers); United States v. Warshak, 631 F.3d 266, 283-88 (6th Cir. 2010) (holding a search warrant was required based in part on analogy to physical letters).

II. SEARCH WARRANTS FOR SPEECH IN THE NEW DIGITAL WORLD

A. Digital Search Warrants Have Created an Unregulated View into Everyone's Lives

A client whom I will refer to as Todd had his first interaction with law enforcement when police were dispatched in response to a domestic violence report concerning him and his girlfriend, both eighteen years old. After interviewing the two, the police obtained a search warrant for Todd's cell phone in order to search for evidence of domestic violence. During the search, the police found old, self-produced, sexually explicit images of Todd and his girlfriend. Based on the photos' creation dates, police determined that Todd and his girlfriend were minors when the photos were taken. Todd was charged with possession of child pornography. The charges were eventually dismissed, but an important question remains as to whether the Fourth Amendment should have precluded that charge in the first place.

In a pre-digital era, in order to enter Todd's home to search for evidence of domestic violence in Todd's papers, the government would have needed probable cause from an independent source to believe that such papers existed in the home. Once that probable cause was obtained, they would be permitted to seize only the relevant papers and, once found, the government would need to leave. However, as Todd's case shows, mere possession of a cell phone implies that one communicates using the digital device and that the relevant information is stored on the cell phone. Consequently, the nature of a search for a cell phone has eroded the double protection of papers once enjoyed at common law.[73]

Compounded with the erosion of the double protection of papers is the judiciary's acquiescence to the reasonable overseizure of information as a necessary consequence of executing digital search warrants[74] By this account, in order to obtain digital evidence, the government must overseize information to search through later for admissible evidence.[75] The problem is how to determine what has been properly seized or overseized and whether the police can use overseized evidence in criminal cases.

Section II.A.1 explains the erosion of the double protection of papers for digital search warrants. It argues that the nature of digital

---

[73] Kyllo v United States, 533 U.S. 27, 34 (2001) (holding that technology cannot be usurp the "minimum expectation" of privacy enjoyed at the Founding).

[74] *See, e.g.*, United States v. Richards, 659 F.3d 527, 537-38 (2011) (describing the need to sort through intermingled documents on a computer).

[75] For a good explanation of why overseizing evidence is a necessity of modern digital searches, see State v. Mansor, 421 P.3d 323, 331-34 (Or. 2018).

devices has increased the circumstances in which the government can obtain a warrant for communications. These circumstances either lead to individuals suppressing their speech or, alternatively, taking the risk of exposure of private information because they believe such risks are necessary to participate in society. Section II.A.2 argues that the Court's acceptance of the overseizure of digital data has created uncertainty among practitioners around how to define what data is overseized and whether the government can use that overseized data as evidence.

1. The Erosion of the Double Protection of Papers Weakens Privacy in Private Communications

To understand how private communications were protected by the Fourth Amendment in the pre-digital era, consider sending a letter through the U.S. Postal Service. The individual would write it in a home or office and drive to the post office. That post office would deliver the letter to another post office, which would then send it out for delivery. Once the mail arrived at the recipient's address, there would be no guarantee that the recipient would not move, consume, or destroy the contents of the package. From a privacy perspective, the random timing of various events and the short time window in which a particular letter could exist in a particular place make snail mail a secure method of communication. Although the government could compromise the U.S. Postal Service or the home, the Supreme Court has protected both of those sites by requiring warrants for homes or letters in transit.[76]

However, the security of email or text messages from government surveillance is weaker because of the nature of digital technology. Today, an email client, social media platform, or text messaging app are both the means by which we communicate and the storage facility for those communications. Further, digital devices have increased our storage capacities to prevent us from having to choose what to save or what to delete. But the convenience of *not* having to make this decision means that knowing the timing window of when something was delivered is less important. Consequently, so long as the government has probable cause to believe that someone has committed a crime, the ubiquity and utility of a digital device will usually also create a belief that evidence of a crime exists on the device.

The ease by which the government can obtain probable cause to search our communications represents an erosion of the double protection of papers. This erosion has three components. First, the ease by which the government can obtain a warrant for digital

[76] The text of the Fourth Amendment protects the home. For letters, see *Ex parte* Jackson, 96 U.S. 727 (1887).

devices means it will have greater access to our communications. Second, because text messaging can substitute for ephemeral communications (e.g., face-to-face conversations), more private conversations will be retained, and for longer. And finally, digital communication has supplanted more secure forms of communication such as sending a letter in the mail.

Indeed, *Knoefel* demonstrates how the erosion of the double protection of papers harms privacy. There, the government had undertaken a homicide investigation where the police "had no apparent motive" for the killing. Consequently, the government obtained a warrant to go on a "fishing expedition" to search for evidence on a suspect's digital device.[77] Once the search was conducted, text message conversations between the suspect and victim revealed that a faltering marriage could have been this suspect's motive for the killing.[78]

In response to a *Knoefel*-style warrant, citizens have two options to protect their speech from government surveillance. One solution for the citizenry is to suppress its speech and stop creating a record of "problematic" speech. Alternatively, people may speak freely because they view the decision to suppress their speech as a false choice given the necessity of digital communications. Under this latter view, citizens have to merely hope their communications do not become subject of a government investigation.

The harm stemming from the suppression of speech is more easily understood. If people are afraid that their speech will be used against them in court, they will be deterred from private and frank conversations on a wide range of subjects.[79] Because speech can be valuable evidence as to someone's mental state, individuals could theoretically have to self-censor on such a wide range of topics that it would be practically impossible to avoid creating evidence.

The false choice creates two distinct harms: the knowledge that someone else knows of their private speech and the potential threat that someone may circulate their private speech. The harm arising from knowledge of speech derives from the target's uncertainty of whether the searcher has discovered a secret on their digital device. The target then has a choice of whether to assume certain secrets have been located, not been located or live without knowing one way or the other. The knowledge that the searcher knows some secrets could alter the future behavior of the target of the search warrant depending upon the disposition of the target.

The harms from circulation are more easily understood: targets of search warrants are harmed by the knowledge that other people

---

[77] State v. Knoefel, No. 2014-L-088, 2015-Ohio-5207, ¶130 (Ohio. App. 2015).
[78] *Id.* ¶ 131-32.
[79] Price, *supra* note 19, at 283-84 (arguing electronic communications should receive protection of a warrant for this reason).

know their secrets and that the information's circulation cannot be contained. The Supreme Court has recognized such harm in the context of child pornography. In concluding distributing child pornography was not protected speech, the Court reasoned that child pornography acts "a permanent record of the children's participation and the harm to the child is exacerbated by their circulation."[80] The court's reasoning as to the harms of circulation applies to more than just child pornography; any secret disclosed, threatened to be disclosed, or capable of being disclosed is subject to this same potential harm.

Second, once the individual becomes aware of the specific speech that has been seized (e.g., by having a conversation with a defense attorney or prosecutor), the target next faces the choice of whether to seek to prevent the information's disclosure at trial. This means that victims or defendants whose cell phones are searched may seek non-trial resolutions such as plea bargains for reasons unrelated to the strength of the cases. Or, witnesses may forgo testifying to a nuanced view of a topic for fear of being impeached.

The question posed by the erosion of the double protection of papers is not whether privacy should be invaded. Few would defend the view that individual privacy should never be invaded in lawsuits. Rather, the question is how much information the government (or even a defense attorney) needs *ex ante* to obtain compulsory legal process. If we think that digital content, particularly text message or emails, often contains intimate private speech, it is worth observing that the probable cause standard is not as protective as it might seem in the abstract.

2. The Reasonable Overseizure of Information Eliminates the Traditional Limitations of a Warrant

Courts' acquiescence to the overseizure of digital information has also eroded other important limitations on digital search warrants. For instance, when officers during the search of a home discover new evidence of a crime, the "plain view" exception governs whether that new evidence can be seized. Under the plain view exception, if the government, during a lawful execution of a search warrant, discovers an item whose criminality is immediately apparent, the government can seize that item.[81]

Because searches for data involve a search for intangible items, digital searchers are ill-equipped to handle a plain view exception made for the physical world. As digital evidence may be found anywhere on a device, the plain view exception risks making a warrant's limitations illusory. This reality caused Paul Ohm to

[80] New York v. Ferber, 458 U.S. 747, 759 (1982).
[81] Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971).

declare that "[c]omputer search warrants are the closest things to general warrants we have confronted in the history of the Republic."[82]

This overseizure problem, as with the erosion of the double protection of papers, impacts more than criminal defendants: crime victims also suffer. For instance, as a practitioner I came across a case in which the government forensically analyzed the victim's phone and turned over the entire forensic report to the defense counsel. The defense attorney then used the contact list and text messages to contact witnesses to confirm unflattering details about the victim. The prosecutor found out when the friends told the victim, who complained to the prosecutor. And in one of my homicide cases, the government sought social media records belonging to the deceased to look for communications between him and my client. Instead, we obtained detailed records of the deceased planning robberies with his friends and threatening to kill other people.

Overseizure impacts victims, witnesses, suspects, defendants, the innocent, and the guilty, who all have something to hide. They may not need to hide the same thing, and what they seek to hide may or may not be relevant to a criminal trial. But these small vignettes demonstrate two harms that stem from overseizure. First, overseized data provides litigants with new leads, and can be used to find additional information that they likely could not have obtained without access to the data. Second, once the litigant gains access to oveseized data, anything found is now fair game for use by litigants.

3. Warrants Provide Only Minimal Protections for the Private Speech

In *Riley v. California*,[83] the Court bluntly told police to "get a warrant" if they wanted to search a cell phone. But the Court did not specify what that warrant should look like. As I have shown, warrants currently offer a false promise of protecting privacy in the digital age. The standard for obtaining probable cause is much weaker than it is for traditional privacy cases. And the pre-digital particularity requirement and plain view exception are ill-equipped to administer digital search warrants. Consequently, the warrant requirement for digital devices in many cases offers an illusion of protection for private information.

[82] Ohm, *supra* note 16, at 11.
[83] 573 U.S. 373, 403 (2014).

B. Search Protocols Create an Unsolvable Digital Disclosure Trilemma

The most popular solution for addressing the problems with digital search warrants is the use of search protocols.[84] Although there is no agreed upon definition of what constitutes a search protocol, search protocols attempt to protect privacy by adding restrictions on *how* the government can search for digital data. For instance, if the government is searching for an image, the government may be required to look for the image using extensions or file headers which are associated with image files (e.g., JPEG), MD-5 hash function values,[85] or special forensic tools that can isolate images found within other files. As the needs of an investigation will differ, the acceptability of a search protocol in a warrant varies according to the circumstances.

Ideally, if a search protocol is successful, it will limit the government's exposure to data that is not clearly relevant to the charges. If the government is never exposed to irrelevant digital data, it will not be able to assert the plain view exception. Further, the search protocol acts as a mitigation procedure to counterbalance the increased frequency by which officers can obtain warrants to search a digital device. If a search protocol is impractical because suspect records permeate the device, search protocol advocates argue that the plain view exception should be eliminated.[86]

1. *Comprehensive Drug Testing* Jumpstarted the Movement for Search Protocols

The adoption of search protocols began in earnest in 2008 with *United States v. Comprehensive Drug Testing*.[87] There, the federal government sought multiple search warrants for digital records which the government believed would contain evidence that ten Major League Baseball players had tested positive for steroids.[88] Under Ninth Circuit precedent, the search warrants had screening procedures whereby agents not involved in the case would segregate

---

[84] Brief of Amici Curiae ACLU and ACLU of West Virginia at 16-26, United States v. Cobb, 19-4172 (4th Cir. July 15, 2019) [hereinafter ACLU Brief].

[85] Hash values are a unique digital signature that exists for every file that can be observed without opening the file itself. These signatures are often used in child pornography investigations. The hash values of images on the target digital device are compared to hash values of known images of child pornography.

[86] ACLU Brief, *supra* note 84, at 24.

[87] 513 F.3d 1085 (9th Cir. 2008), *reh'd en banc* 579 F.3d 989 (9th Cir. 2009) (hereinafter CDT I), *amended by* 621 F.3d 1162 (9th Cir. 2010). *Comprehensive Drug Testing* has a complicated procedural history where the Ninth Circuit issued three sets of opinions. As the procedural history is less important for our purposes, I will primarily focus on the first *en banc* opinion, issued in 2009.

[88] *Id.* at 1089.

responsive data from nonresponsive data and hand only the responsive data over to investigators.[89]

The government, however, ignored these segregation procedures and stumbled across a directory on a computer that contained the results of drug tests for hundreds of baseball players as well as athletes in other sports.[90] Once the district court judges discovered what had occurred, they were furious.[91] The government argued that the records outside the scope of the warrant fell within the plain view exception and could be seized.[92] The district court judges rejected the government's argument. The government appealed all three orders to the Ninth Circuit.[93]

The *en banc* panel affirmed the district courts' orders, and issued some "guidance" to magistrate judges to prevent the abuses in *Comprehensive Drug Testing* from occurring again. Specifically, the Ninth Circuit suggested that in future digital searches: (1) magistrate judges should insist on the government's waiver of the plain view exception; (2) segregation of data must be done by the third-party and nonresponsive data must not be disclosed to the government; (3) warrants and subpoenas must disclose the actual risk of destruction of evidence; (4) the government's search protocol must be designed to only discover the evidence sought; and (5) the government must destroy or return nonresponsive data to the recipient. Upon the government's motion to be heard before the full court of appeals, the Ninth Circuit reissued its majority opinion with the guidance section moved to a concurring opinion by Judge Kozinski.[94]

Despite this change from binding to persuasive authority, magistrates began to issue search protocols or similar regulations.[95] Scholars engaged in a vigorous debate over the constitutionality and desirability of these protocols.[96] Most of the debate has centered on whether current constitutional doctrine permits these protocols or whether the nature of digital search warrants calls for a change in Fourth Amendment doctrine. Those in the pro-protocol camp maintain that nothing in current constitutional doctrine prohibits

---

[89] *See* 579 F.3d at 993-94, 997 (noting both judges had procedures put in place to segregate intermingled data).
[90] *Id.* at 996.
[91] *See, e.g.*, CDT I, 579 F.3d at 994 ("All three judges below expressed grave dissatisfaction with the government's handling of the investigation, some going so far as to accuse the government of manipulation and misrepresentation.").
[92] *Id.* at 997-98.
[93] *Id.*
[94] United States v. Comprehensive Drug Testing, 621 F.3d 1162 (9th Cir. 2010).
[95] For a list of these various decisions, see Berman, *supra* note 16, at 86-92 and accompanying footnotes.
[96] *Compare* sources cited *supra* note 16 (arguing for search protocols), *with* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Search and Seizure*, 96 VA. L. REV. 1241 (2010) (arguing against search protocols).

search protocols, and that regardless, the Court should recognize that digital information is different and create new rules for digital searches.[97] Kerr has argued that search protocols are precluded by current doctrine and are otherwise impractical to implement because data can be manipulated to avoid detection by the protocol.[98] Search protocol advocates' focus on the Fourth Amendment privacy implications has caused an underappreciation of how search protocols interact with the criminal justice system as a whole.

1. Search Protocols Create a Digital Disclosure Trilemma

Once a prosecutor obtains any item with respect to a criminal case, it has disclosure obligations concerning discovery, child pornography, and *Brady* material. Under *Brady v. Maryland*,[99] the government must disclose any material evidence within its possession that is favorable to the defense.[100] This obligation applies (to some evidence) without regard to the request of the defense[101] and includes evidence that would impeach a witness.[102] Most importantly, for our purposes, "the individual prosecutor has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police."[103]

Although the Constitution does not prohibit the government from discarding exculpatory evidence in good faith,[104] complaints from defense attorneys and judges have been concerned with the opposite problem of the government's indefinite retention of data.[105] For instance, in *United States v. Ganias*,[106] the federal government obtained a search warrant for the defendants' computers as part of an investigation into unlawful activity by corporate entities for which Ganias was not a suspect.[107] But after those files were seized, the government became suspicious that Ganias had committed tax evasion.[108] Three years later, the government obtained a subsequent

---

[97] *See generally* Berman, *supra* note 16, at 82-94; Clark, *supra* note 16, at 2008-18; Gershowitz, *supra* note 14, at 614-38; Ohm, *supra* note 16.
[98] Kerr, *supra* note 96.
[99] 373 U.S. 83 (1963).
[100] *Id.*
[101] United States v. Agurs, 427 U.S. 97 (1976).
[102] United States v. Bagley, 473 U.S. 667 (1985).
[103] Kyles v. Whitley, 514 U.S. 419, 437 (1995); *see also* Youngblood v. West Virginia, 547 U.S. 867, 869-70 (2006) (per curiam); Banks v. Dretke, 540 U.S. 668, 693 (2004).
[104] Arizona v. Youngblood, 488 U.S. 51, 58 (2000).
[105] United States v. Comprehensive Drug Testing, 579 F.3d 989 (9th Cir. 2009) (en banc), *overruled by* 621 F.3d 1162 (9th Cir. 2010) (en banc).
[106] 755 F.3d 125 (2d Cir. 2014), *reheard en banc* 824 F. 3d 199 (2d Cir. 2016).
[107] *Ganias*, 824 F.3d at 201 ("Nothing in the record suggests that Ganias himself was suspected of any crimes at that time.").
[108] *Ganias*, 755 F.3d at 129.

search warrant on this data which it already had in its possession.[109]

Consequently, if the government must learn of all exculpatory information within its possession and the government is not discarding material that is outside the scope of the warrant, current *Brady* doctrine requires the government to search both the relevant and irrelevant material for exculpatory evidence. Because the government believes that everything seized pursuant to the original warrant can fall within the plain view exception, no conflict between the government's *Brady* and commands under the search warrant exists. But if the government is wrong about its plain view argument, the overseizure and retention of digital information creates a conflict between the search protocol and the government's *Brady* obligation. A similar problem occurs with the government's discovery regime, depending on the jurisdiction. For instance, in some states, the government's discovery obligation is broad enough to encompass any tangible item (including electronically stored information) that "may be material to the preparation of the defense."[110]

One solution is for the government to always disclose the full contents of a forensic file to the defense without looking at the contents of the full digital file. Under this view, the government could comply with *Brady* and still limit its search. Putting aside concerns over whether this "discovery dump" complies with *Brady*,[111] such a position is barred by discovery restrictions on the disclosure of child pornography in discovery.[112] Prosecutors can comply with this statute only if every file disclosed does not contain child pornography. Consequently, a government agent must look at what is being disclosed to comply with federal law.[113]

---

[109] *Id.* at 130.

[110] *See, e.g.*, KY. R. CRIM. P. 7.24(2) (West 2019).

[111] *See, e.g.*, United States v. Kirk Tang Yuk, 885 F.3d 57, 86 (2d Cir. 2018) ("Some courts have reasonably suggested that burying exculpatory material within a production of a voluminous, undifferentiated open case file might violate the government's obligations.").

[112] 18 U.S.C. §3509(m) (2018).

[113] Some may object that machine learning algorithms can identify child pornography without an agent reviewing the files. *See* Abhishek Gangwar et. al., *Pornography and Child Sexual Abuse Detection in Image and Video: A Comparative Evaluation*, 8 INT'L CONF. ON IMAGING FOR CRIM. DETECTION & PREVENTION 37, 41 (2017) (concluding that the best machine learning algorithm can detect child pornography with accuracy of 87.56% without "fine-tuning" the algorithm). Given the potential false negative error rate, it is unclear whether these solutions will be satisfactory. 18 U.S.C. §3509(m)(1) (2018) states that child pornography "shall remain" with the government or the court as opposed to requiring the government to make reasonable efforts to prevent disclosure. Because of the policy objective and public pressure to prevent distribution errors, prosecutors will likely self-impose (and judges will require) strict compliance with these statutes despite their administrative cost. Machine learning algorithms likely cannot meet this standard.

Together, these rules create what I call a Digital Disclosure Trilemma. As restrictions on the government's ability to search digital files increase, conflicts with its obligations to produce *Brady* material and limit disclosure of child pornography emerge. Search protocols, however, are designed exclusively to search for incriminating evidence. In controlling the manner in which the search is executed, these protocols attempt to avoid application of the plain view exception by preventing the government from ever seeing the incriminating data. But the narrow focus on the Fourth Amendment implications of overseizure leave search protocols unprepared to solve the Digital Disclosure Trilemma.

2. Search Protocols Cannot Solve the Digital Disclosure Trilemma

Doctrine cannot be modified to solve the Digital Disclosure Trilemma without undermining *Brady* or the purpose of the search protocol. First, as a practical matter, the search protocols used to find incriminating evidence are likely different than search protocols used to find exculpatory evidence. To solve this issue, doctrinally, search protocols would need to place limitations on *Brady*'s reach. However, such a limitation permits a prosecutor to either undermine *Brady*'s purpose or use *Brady* obligations pretextually to undermine the search protocol in the warrant.

As to the practical matter, the protocol used to search for *Brady* material will often be quite different from the protocol used to search for incriminating evidence. The government might be interested in communications between the victim and suspect on the suspect's phone, but communications between the suspect and critical prosecution witness may exist elsewhere on the phone and in a completely different timeframe. Messages that attack a key witnesses' character for truthfulness could theoretically be anywhere on the phone, particularly if the suspect and witness shared common friends who have no relationship to the suspected crime at issue. As many crimes occur between people who know one another, this issue will frequently arise.

Advocates for search protocols could avoid the trilemma by arguing that *Brady* does not apply to overseized information. Under this framework, the "universe" of materials that cabin the scope of *Brady* material is limited to materials that are responsive to the search warrant. Therefore, if the government obtained a search warrant for conversations between Jim and Joe between January and June of a particular year, *Brady* would only require disclosure of exculpatory conversations between Jim and Joe. Conversations with parties outside the scope of probable cause would amount to a hard limit on the contours of the government's *Brady* obligation.

The problem with this view is that the universe of seizeable

material under a search warrant can be smaller than the scope of *Brady* material. For instance, the government may only have probable cause to seize communications between the victim and the suspect in an assault case. But the *Brady* material that may exist on a cell phone could encompass statements made to third parties about the victim or suspect's state of mind, location information, and even character traits such as violence or peacefulness. Under this hypothetical limitation, the government would have to discard potentially exculpatory information it found during its search of the device. Such information may have to be excluded even if the government had reason to know it might exist on the device.

This limitation therefore incentivizes the government to create search protocols to avoid *Brady* material in certain instances. Say, for instance, that the government wants to search someone's Facebook account for conversations that a suspect had with the government's confidential informant (CI). The government could reasonably create a search protocol focused on communications between known user IDs of the suspect and the CI within a specific timeframe. However, what about possible conversations that the suspect had with others *about* the CI? The government may be less interested in these conversations if it knows that the CI is unscrupulous.

Further, excluding overseized information from *Brady* could, ironically, exact a high cost for defendants in the name of privacy. If evidence that could exonerate a defendant is part of the overseized information, the defendant may not obtain access to this information to his benefit. This may increase the risk of wrongful conviction or overincarceration.

Even when search warrants are issued for criminal defendants' digital devices, criminal defendants would want the government to search for *Brady* material even on their private digital devices. Private criminal defense attorneys and public defenders (as well as prosecutors) only have so much time to sift through digital information. If prosecutors were excused from searching for exculpatory evidence, the burden of finding it would shift to the defense attorney. The reality, particularly at the state level, is that defense attorneys do not have time to search through all of the data that comes within a digital search warrant. Eliminating *Brady* obligations for overseized digital information would cut off any post-conviction relief for a defendant for a *Brady* violation.

Moreover, depending on the discovery regime, a criminal defense attorney may not know that certain evidence is exculpatory until trial. Because prosecutors tend to have easier access to victims, investigators, and other state agencies, there will be some instances in which only the prosecutor is aware that exculpatory information exists. Clients are also imperfect means of finding exculpatory

evidence because they do not know the rules of evidence and, at the beginning of the attorney-client relationship, they often have idiosyncratic views of what is exculpatory or incriminating evidence.

Finally, determining how *Brady* should interact with overseized material is further complicated by theory-dependent *Brady* material. Suppose that a murder suspect communicated to someone, "I did not kill Mark, but I know who did."[114] The statement is likely discoverable as an oral incriminating statement by a defendant[115] (due to the suspect admitting knowledge of the killing) or *Brady* material (due to the denial of responsibility). If such a statement, however, is disclosed under the government's *Brady* obligation, can the government use this information as further probable cause to expand its search protocol? If the answer is no, then the government's *Brady* obligation's interaction with the exclusionary rule is harsh. However, if the answer is yes, we should expect prosecutors to become *Brady* zealots looking for anything and everything that *possibly* could be exculpatory to conduct extensive searches and overseizures of evidence.

3. Defendants Will Rarely Get Relief Under a Search Protocol Regime

The second reason to reject search protocols as a lasting solution is that they fail to give criminal defendants relief and therefore deter illegal police conduct. Search protocols may be helpful when the defendant has an opportunity to be heard prior to the search warrant's execution—such as when the social media provider contests the warrant,[116] or if the case is high profile enough to cause impact litigators to intervene.[117] Most criminal defendants, however, will not be so lucky.

Instead, their cases will involve circumstances in which a warrant is being challenged post hoc. The criminal defendant will always be placed in a situation where no protocol or a poorly created protocol is used. Consequently, they will be forced to argue that the government should have used a particular search protocol *that just*

---

[114] These facts are roughly the fact pattern presented in Escobedo v. Illinois, 378 U.S. 478, 483 (1964), where the suspect's first incriminating statement, was "I didn't shoot Manuel, you did it."

[115] KY. R. CRIM. P. 7.24(1) (West 2019).

[116] In re 381 Search Warrants Directed to Facebook, 78 N.E.3d 141 (N.Y. Ct. App. 2017).

[117] In the Matter of Search of Information Associated with Facebook Accounts DisruptJ20, Laceymauley, and Legbacarrefour that is Stored at Premises Controlled by Facebook, Inc., Special Proceeding Nos. 17 CSW 658, 659-60, https://www.acludc.org/sites/default/files/field_documents/11-9-2017_dc_superior_ct_order.pdf [https://perma.cc/3TL4-L63A].

happens to exclude all incriminating evidence. The government will predictably argue that the search protocol it used was proper because it located the incriminating evidence. The risk of defense attorneys using hindsight to create alternative search protocols is omnipresent in every motion. Courts are sure to take note, and give relief sparingly.

Even if there are judges who wish to enforce narrow search protocols post hoc, there is little way for these defendants to obtain relief due to the good-faith exception. In *United States v. Leon*,[118] the Court found that even if there were a Fourth Amendment violation, the exclusionary rule would not apply if the violation was committed in good faith. In such a circumstance, excluding the evidence would not serve the purpose of the exclusionary rule, which was limited to deterring police misconduct.[119] The Court held that the good-faith exception would not apply when (1) the magistrate "abandoned his detached and neutral role"; (2) the affiant was "dishonest or reckless in preparing their affidavit"; (3) the affidavit was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) the warrant was "so facially deficient—for example in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid."[120] Recently, the Court has hinted that a fifth exception exists if it is shown that a pattern of widespread or systemic misconduct exists.[121]

Although *Leon* concerned an officer's mistake in concluding that the affidavit had sufficiently pled facts for the officer to believe the informant to be credible, the good-faith exception has metastasized to excuse grossly incompetent conduct by officers. For instance, the Southern District of Ohio in *United States v. Whitt*[122] found that a search warrant for a Facebook profile lacked probable cause because the affidavit "fail[ed] to . . . establish[] information known to the agent making it likely that 'specific' evidence is likely to reside in Whitt's particular Facebook account."[123] It nevertheless did not exclude the evidence from the profile because "Sixth Circuit jurisprudence on searching the Facebook account of a suspect is less [developed]" and "[i]t appears that the officer believed, in good faith, that her detailed paragraphs regarding the suspect's connection to the underlying crime . . . [were] enough to establish probable cause."[124] Therefore, "[e]ven if hindsight shows that the requisite

[118] 468 U.S. 897 (1984).
[119] *Id.* at 919-20.
[120] *Id.* at 923, 926.
[121] Utah v. Strieff, 136 S. Ct. 2056, 2064 (2016); Herring v. United States, 555 U.S. 135, 146-47 (2009).
[122] 2018 WL 447586 (S.D. Oh. Jan. 17, 2018).
[123] *Id.* at *4.
[124] *Id.*

nexus was lacking . . . it was not unreasonable for law enforcement to rely on the warrant . . . ."[125]

Of course, what is unstated in *Whitt* is why the officer thought the nexus requirement was unnecessary for a search of a social media profile considering every other warrant requires the government to establish such a nexus.[126] But *Whitt* is not an outlier. Ever since the Supreme Court held in *Davis v. United States*[127] that the good-faith exception applied to an officer's reliance on then-binding judicial decisions, courts have been requiring defendants to show an officer acted in bad faith.[128] There, the Court found the "absence of police culpability doom[ed] Davis' claim." [129] According to the Court, "the harsh sanction of exclusion [applies] only when [misconduct is] deliberate enough to yield meaningfu[l] deterrence, and culpable enough to be worth the price paid by the justice system."[130] Consequently, because the conduct alleged by the defendant "did not violate Davis's Fourth Amendment rights deliberately, recklessly, or with gross negligence," and was not "'recurring or systemic negligence,'" the good-faith exception precluded relief.[131]

As search protocols attempt to erect new restrictions on the government's authority to search digital devices, we should expect that the defendants whose cases establish the rule will be denied relief under the good-faith exception. (This occurs in most new appellate Fourth Amendment cases.) [132] But because the appropriateness of search protocols is context-based, there is a significant concern that the good-faith exception will always preclude relief to criminal defendants because the government will always be able to distinguish a previous case from the current case. If evidence is never excluded, the government is never deterred. The data bears out this argument: since *Comprehensive Drug Testing*, the best victory for search protocols has been that courts are allowed to impose them.[133] No court, however, has required their use.

---

[125] *Id.*
[126] *Id.* at *1 (quoting Ellison v. Balinski, 625 F.3d 953, 958 (6th Cir. 2010)).
[127] 564 U.S. 229 (2011).
[128] *See, e.g.*, United States v. Blake, 868 F.3d 960, 974-75 (11th Cir. 2017); United States v. Ganias, 824 F.3d 199, 221 (2d Cir. 2016) (en banc).
[129] *Davis*, 564 U.S. at 240.
[130] *Id.* (internal quotation marks and citation omitted).
[131] *Id.*
[132] *See, e.g.*, United States v. Rodriguez, 799 F.3d 1222 (8th Cir. 2015) (applying good-faith exception to uphold search of defendant's car after the Supreme Court found a Fourth Amendment violation occurred).
[133] *See, e.g.*, In re Search Warrant, 71 A.3d 1158 (Vt. 2012) (upholding magistrate judges' discretion to regulate how digital search warrants are executed).

C. Use Restrictions Will Rarely Be Used or Will Create a Digital Disclosure Trilemma

Orin Kerr has proposed a second model to accomplish the objectives of search protocols, which he has labeled a use restriction.[134] Kerr accepts that the overseizure of information is reasonable because of the need to access to responsive evidence within the search warrant.[135] However, "[a]gents . . . cannot receive a windfall from the overseizure. Kerr argues that courts should block the windfall by restoring the traditional limits on the seizure power to what was described in the warrant."[136] Therefore, "[s]ubsequent use of the nonresponsive data for reasons unrelated to carrying out the warrant renders the ongoing seizure of the nonresponsive data constitutionally unreasonable."[137]

The use restriction model has two main weaknesses. First, prosecutors will attempt to expand the warrant's scope as much as possible to avoid application of the use restriction.[138] These efforts would likely succeed, at least in state courts, because warrants are so broad already. Second, if the particularity requirement is narrowed, then the use restriction model will, like the search protocol model, create a Digital Disclosure Trilemma.

1. Use Restrictions Incentivize Creating Overly Broad Search Warrants to Limit Application of the Use Restriction

Because the use restriction model creates a hard exclusionary rule for overseized information, we should expect prosecutors and police to write search warrants as broadly as possible. Judges would then be pressed to decide whether to exclude incriminating evidence or to acquiesce to the broad scope of the warrant. Considering that the particularity requirements for many search warrants, especially in state courts, are already very broad, a use restriction will likely only exclude evidence in the most extreme cases.

First, prosecutors can evade the use restriction by means of

---

[134] The origins of the use restriction model originate from Professor Harold Krent. *See* Harold Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49 (1995).

[135] Orin Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH. L. REV. 1, 7 (2015).

[136] *Id.* at 26.

[137] *Id.* at 26-27.

[138] Kerr does have a theory for how digital search warrants should be sufficiently particular. For Kerr, the search warrants should describe all of the data that will copied from the device and separately describe the information that the government is allowed to seize from the copied data. However, as Kerr notes, courts have not followed his recommendation, and instead "somewhat sloppily blend the two stages together." I concur with Kerr's two-step approach. The discussion of particularity here is concerned with the second step only.

subject matter overlap between "responsive" and "nonresponsive" information. Under Kerr's use restriction model, the government's use of evidence is not restricted by its *ex ante* anticipated purpose;[139] rather, whatever the warrant authorizes the seizure of can be used as evidence of any crime whatsoever. Such breadth permits the government to expand the scope of the search warrant beyond evidence of the suspected crime.

For instance, consider the case involving my client Todd.[140] In that case, the government sought evidence of communications that would support a domestic violence charge and happened to find old, self-produced, sexually explicit images of Todd and his girlfriend that would support charges for possession of child pornography. This is precisely the circumstance that the use restriction model seeks to prevent.

However, a savvy prosecutor could argue that in order to prove the crime of domestic violence, the government must first establish that the victim and suspect were in an intimate relationship, and that this image helps to prove that element.[141] This argument should win if the warrant authorizes the government to search for "evidence of domestic violence." It should lose, however, if the government were authorized to search for text messages sent shortly before and after the crime.

Todd's is not an isolated case. Prosecutors investigating evidence of drug trafficking might want to seize a defendant's statements regarding their spending habits or plans. If prosecutors search a murder suspect's phone for evidence of a murder and discover evidence of gang activity, the government is sure to find a way to try to link that evidence to their case. Ultimately, subject-matter crossover is susceptible to the government coming up with post hoc rationalizations of how the seized evidence is responsive to the warrant.

Second, the use restriction model is limited by a court's post hoc construction of the warrant. Consider the case of *State v. Mansor*,[142] where the Oregon Supreme Court adopted the use restriction model. In *Mansor*, the defendant called 911 because his child had stopped breathing.[143] During his interview with the police, Mansor indicated that he had used his computer fifteen minutes before police arrived to search online for what to do.[144] A hospital examination and interview of the child revealed evidence of child abuse, and consequently, the government sought a warrant to search the

---

[139] Kerr, *supra* note 135, at 35.
[140] *See supra* Section II.A.
[141] *See, e.g.*, KY. REV. STAT. 403.720, 508.030, 508.032 (West 2019) (defining domestic violence under Kentucky law).
[142] 421 P.3d 323 (Or. 2018).
[143] *Id.* at 327.
[144] *Id.*

defendant's home including "two laptop computers" and "two desktop computers."[145] Although the internet history within the fifteen minutes included evidence consistent with a father worried about his child's wellbeing, search history *outside* the fifteen-minute window revealed several incriminating Google searches, such as a search for "afraid of abusing my baby," followed by "how do I deal with a screaming baby?"[146]

The Oregon Supreme Court adopted Kerr's use restriction model and suppressed all evidence outside the fifteen minutes of internet history within the affidavit.[147] This time constraint, as Professor Kerr noted, was a post hoc construction by the Oregon Supreme Court, and the police probably "didn't expect courts to read the warrant as narrowly as the Oregon Supreme Court did."[148] To Kerr, the warrant was poorly drafted, yet he believed the police probably had sufficient evidence for "a much broader warrant allowing a search through the computer for any evidence of child abuse."[149]

Regardless of whether Kerr's analysis is correct, I would add that some courts faced with an identical warrant have found that the warrant authorized the government to search for all evidence of a crime at issue.[150] Recall that it was the *lack* of government knowledge about the underlying crime in *Knoefel* that justified a more extensive search for the Ohio appellate court.[151] Consequently, as it stands, we should expect case law under the use restriction model to become highly dependent on how appellate judges interpret the scope of the warrant post hoc. Defendants, prosecutors, and police deserve better predictability for when a warrant is valid.

Third, without a clear particularity framework, the use restriction model cannot draw distinctions between information that is or is not responsive to the search warrant. Is evidence that could be used to impeach a defendant or witness responsive to the search warrant? Should responsiveness simply adopt the broad definition of relevancy found in Federal Rule of Evidence 401?[152] If so, does the evidence have to directly support the existence of an element of the crime, or can it help support the existence of *other evidence* which helps establish the existence of an element of the crime? What about character evidence of bad acts that goes to someone's state of

---

[145] *Id.* at 327-28.
[146] *Id.* at 329-30.
[147] *Id.* at 343-45.
[148] Orin Kerr, *Oregon Supreme Court Adopts Use Restriction on Nonresponsive Data for Computer Warrants*, VOLOKH CONSPIRACY, https://reason.com/2018/06/29/oregon-supreme-court-adopts-use-restrict [https://perma.cc/785J-UP6B].
[149] *Id.*
[150] *See supra* note 14 and accompanying text.
[151] State v. Knoefel, 2014-L-088, 2015-Ohio-5207, ¶130 (Ohio App. 2015).
[152] FED. R. EVID. 401 defines evidence as relevant if it has any tendency to make a fact of consequence to the case more or less probable.

mind, or evidence that could be used to rebut a defense? In the state courts where I have practiced or consulted on cases, I have simply found that evidence is within the scope of the warrant so long as prosecutors can articulate a rational basis for how that information could be admissible evidence.

Finally, the above criticisms of use restrictions work synergistically. Todd's case is the perfect example of such a cruel synergy. Because the old photographs were subject to both subject-matter crossover and a post hoc timeframe construction, the government was able to seize a photo it had no knowledge of and no intention of collecting. The use restriction model, when combined with a weak particularity requirement, will serve only to exclude evidence that lacks any post hoc rational relationship to the warrant.

2. *Even if Courts Adopt a Strong Particularity Requirement, Use Restrictions Cannot Administer the Digital Disclosure Trilemma*

The weak particularity requirement as seen in *Knoefel* is not necessarily inevitable. Courts could require stronger particularity requirements to prevent post hoc creations of a link to evidence. However, when the use restriction model is paired with a stronger particularity requirement, the model still cannot address the Digital Disclosure Trilemma. As the strength of the particularity requirement increases, conflicts will emerge between the use restriction model and the government's *Brady* obligation.

For instance, Kerr has recognized the problem of successive search warrants for data after the initial search warrant. He does not "have strong views on whether the ongoing seizure approach should be limited to prohibiting the use of nonresponsive files or whether it should be extended to blocking second warrants for nonresponsive data more broadly."[153] Nevertheless, Kerr offers two visions of the use restriction doctrine: one in which there is a complete bar on search warrants for nonresponsive data from an initial search warrant, and a weaker version where successive search warrants are permissible, provided there is independent probable cause to support such a search.[154]

If there is a complete bar on successive warrants, the Digital Disclosure Trilemma could cripple multiple investigations into an individual. Suppose the government is investigating a suspect in homicide, but during the investigation, the suspect is arrested on domestic violence charges. The government wants to do a search warrant on the suspect's phone for evidence related to the domestic violence charge, but currently lacks probable cause for the

[153] Kerr, *supra* note 135, at 31.
[154] *Id.* at 33.

homicide. If there is a complete bar on successive warrants, the government's homicide investigation could be crippled if the homicide charges are "nonresponsive" to the domestic violence charge.

If the weaker version of the use restriction is adopted, however, the government's *Brady* obligation will eliminate or significantly weaken its ability to obtain successive search warrants. A successive search warrant is needed when the scope of the search warrant is narrower than the universe of the incriminating evidence on the device. In such a situation, a successive search warrant could permit the government to seize additional evidence based on independent probable cause. However, in practice, the government's *Brady* obligation would prevent that from occurring. Because the government must determine whether exculpatory information exists, it must search the entire device for *Brady* evidence to comply with its obligation. If the government uncovers information outside the scope of the search warrant during its search for *Brady* material, it will prevent the government from establishing the independent probable cause needed to obtain a successive search warrant.[155]

Courts could elect to modify the *Brady* doctrine for digital search warrants. However, this again raises the issue of equal access to quests for truth. If we are willing to give the government unfettered access to search for incriminating evidence against the defendant, there is no reason why the search for exonerating evidence should be limited. Instead, both the defense and prosecutorial interests in truth should be equally balanced against the privacy interest at issue.

III. A FIRST AMENDMENT THEORY OF DIGITAL SEARCH WARRANTS

As explained in Part II, search protocols regulate the administration of a warrant by controlling the executing officer's access to information. Use restrictions regulate prosecutors by creating a constitutional motion *in limine* prohibiting the use of "overseized" information at trial. A First Amendment-based theory of digital search warrants would combine the best of these models by regulating both police and prosecutors. This Article offers three reasons why this model is superior.

First, when the government is searching for speech believed to provide evidence of a crime, the First Amendment demands a heightened particularity standard, requiring prosecutors to describe *ex ante* the speech sought. A description of the types of documents

[155] Proactive investigations, which are seen more at the federal level, might be an important exception to this statement. Still, digital devices searched incident to arrest will always encounter the successive search warrant problem.

the government seeks to seize is insufficiently particular. The government must instead summarize the nature of the speech, if known, or use metadata that sufficiently describes why speech that meets those parameters provides evidence of a crime.

Second, in determining how broad certain metadata parameters can be, this Part argues that the foregone conclusion doctrine, normally used to protect someone's Fifth Amendment right to respond to a subpoena, should also provide a First Amendment defense to a search warrant. I argue that the court's foregone conclusion doctrine and cases on the First Amendment-Fourth Amendment connection sought to prohibit individuals from having discretion to decide what is responsive to the search warrant or subpoena. Moreover, recognizing a congruence between the foregone conclusion doctrine and a search warrant for speech is desirable as a policy matter because it would ensure that both the government and the defense have equal access to the records of third parties.

Third, because investigators will likely uncover data that is not related to the search warrant, this Part argues that courts should supplement this model by imposing a use restriction, eliminating the plain view exception, or requiring the government to use an independent search team, as discussed in Section IV.B.

When considering the types of searches that would be permissible under a First Amendment model, it is helpful to place all possible searches into five categories. The first category covers what I call "cherry-on-top" searches. In this case, the government has sufficient evidence to obtain a conviction, and is merely conducting a search of a digital device to collect more evidence to support its case. In these circumstances, the government already has a good idea of what it seeks and can easily describe it. There are also "known unknown" searches where the government has a "cherry-on-top" scenario, but the crime under investigation involves a continuous course of conduct (e.g., drug trafficking) which lead the government to believe that other currently unknown evidence also exists. Other times, a search warrant will be issued to discover a particular puzzle piece without the expectation of charges being made from the search itself. Finally, there are laundry list search warrants which identify what can be seized by data categories, and "all data" search warrants. This Article's model would not affect the first three categories; instead, it targets the latter two types of search warrants.

What the model advanced in this Article seeks to prevent are general warrants and warrants that give officers discretion to determine what evidence is relevant to a particular offense. The First Amendment model grants an officer either no discretion or too little discretion to determine what evidence is subject to seizure. To ensure that discretion is properly cabined, the magistrate issuing the

warrant must decide *ex ante* what speech is relevant to a particular search.

Section III.A provides an overview of the Court's jurisprudence on the connection between the First and Fourth Amendments and explains why a First Amendment framework for administering search warrants for digital speech fits within that jurisprudence. Section B uses a search warrant for text messages to illustrate how such a warrant could comply with the First Amendment's heightened particularity standard. Section C explains why the foregone conclusion doctrine should be a First Amendment doctrine limiting search warrants for speech.

A. Stanford *Created a Framework for Administering Search Warrants for Digital Speech*

As noted in Part I, *Wilkes* and *Entick* envisioned a property-based privacy right for irrelevant papers located in the place which a warrant authorized the government to search. Once the U.S. Supreme Court developed a First Amendment jurisprudence to protect speech, questions emerged concerning how the Court would prevent search warrants from being used a weapon to suppress constitutionally-protected speech. In *Stanford v. Texas*, the Court found that a search warrant authorizing the seizure of a laundry list of documents which "concerned the Communist Party of Texas" amounted to an unlawful general warrant. The Court held that when the "things to be seized" contained "books," those papers must be described with the most "scrupulous exactitude."[156]

First Amendment litigators would attempt to expand *Stanford* into a larger First Amendment revolution of the Fourth Amendment. However, these arguments would find little support in the Burger and Rehnquist Courts. For reasons unknown, *Stanford* largely remained dormant once it was limited to the particularity requirement. This Section argues that the rise of search warrants for digital information, particularly for digital speech, provides an opportune moment to reexamine how *Stanford* can help solve the constitutional problems raised by general search warrants for digital speech.

Section 1 tracks the development of the First Amendment jurisprudence that led to the creation of *Stanford*'s "scrupulous exactitude" standard, and how subsequent decisions have limited *Stanford*'s reach. Section 2 explains why, despite the limitations placed on *Stanford*, the case provides a vehicle to restore the double protection of papers in the digital age.

[156] Stanford v. Texas, 379 U.S. 476, 485 (1965).

1. The Scrupulous Exactitude Standard Was Created to Protect the First Amendment Right of Abstract Speech

The federal Alien Registration Act of 1940 (also known as the Smith Act) prohibited a person from "knowingly or willfully" advocating or conspiring to advocate the overthrow of any government in the United States "by force or violence."[157] Its most famous prosecution occurred in *Dennis v. United States*.[158] In *Dennis*, several high-ranking members of the Communist Party of the United States of America were convicted of violating the Smith Act simply for being members.

In its opinion, the Court curtly summarized the facts as follows: "[T]he leaders of the Communist Party in this country[] were unwilling to work within our framework of democracy, but intended to initiate a violent revolution whenever the propitious occasion appeared."[159] Because the Court denied certiorari on the sufficiency of the evidence, the Court accepted the facts of the appellate court.[160] That court found that Dennis and his co-defendants had changed the Communist Party's policies from "peaceful cooperation" with the United States to a "highly-organized," "rigidly controlled" organization that "tolerate[d] no dissension," was "adept at infiltration into strategic positions," and "worked for the overthrow of the Government by force and violence."[161]

The actual facts, however, were tamer. As Justice Black explained in his dissent, "[t]he indictment is that they conspired to organize the Communist Party and to use speech or newspapers and other publications in the future to teach and advocate the forcible overthrow of the Government."[162] Historical accounts of the trial go so far to suggest that the government did not even bother to attempt to show that any of the defendants had engaged in acts to further a hypothetical conspiracy to overthrow the government.[163]

Nevertheless, the Court found that the Smith Act did not violate the First Amendment under the Court's "clear and present danger" test. First, the Court found that the government's interest in preventing the "overthrow of the Government by force and violence . . . a substantial enough interest for the Government to limit speech."[164] Second, the Court found that a present danger existed by relying upon jury instructions to supply the necessary findings. For

---

[157] Pub. L. No. 76-670, 54 Stat. 670 (1940).
[158] 341 U.S. 494 (1951).
[159] *Id.* at 497-98.
[160] *Id.* at 497.
[161] *Id.* at 498
[162] *Id.* at 579 (Black, J., dissenting).
[163] MARTIN H. REDISH, THE LOGIC OF PERSECUTION: FREE EXPRESSION AND THE MCCARTHY ERA 83 (2005).
[164] *Dennis*, 341 U.S. at 507-09.

instance, the Court noted that the jury was instructed to find that overthrowing had to be "intended to overthrow the Government 'as speedily as circumstances would permit.'"[165] Finally, because the government did not, according to the Court, have to wait until an overthrow of the government was imminent, a danger in the future posed by a highly organized party made it a present danger.[166]

Dennis, however, would effectively be limited to its facts in *Yates v. United States*.[167] *Yates* concerned virtually identical facts, with the exception that *Yates* concerned with political activity in California as opposed to at a national level. The newly constituted Warren Court held the First Amendment protection of "advocacy of abstract doctrine" to be "heavily underscored" by the Court's prior First Amendment cases.[168] Consequently, the Court found that the Smith Act could only criminalize "advocacy to action."[169] Advocacy to action could only occur when "the group is of sufficient size and cohesiveness, is sufficiently oriented towards action, and other circumstances are such as reasonably to justify apprehension that action will occur."[170] In contrast, "mere doctrinal [advocacy] of forcible overthrow" of the government "is too remote from concrete action to be regarded as the kind of indoctrination preparatory to action which was condemned in *Dennis*."[171] Put simply, *Yates* neutralized *Dennis* by requiring all convictions under the Smith Act to match the facts in *Dennis*. Because *Dennis*'s facts were not facts at all, prosecution under the Smith Act is now virtually impossible.

The Warren Court's First Amendment revolution would also lead to changes in how the Court treated Fourth Amendment search warrants implicating First Amendment rights. The start of the First and Fourth Amendment connection begins with *Marcus v. Search Warrant*.[172] There, Missouri law enforcement had obtained a search warrant and seized several "stock[s] of [allegedly obscene] magazines running 'into hundreds of thousands . . . [p]robably closer to a million copies.'"[173] The officers determined which magazines were obscene using their "own judgment."[174] After recounting the history of the use of search warrants in suppressing speech in England and at the Founding,[175] the Court held that "the Fourteenth Amendment" prohibits "a State [from] adopt[ing] whatever

[165] *Id.* at 510.
[166] *Id.* at 509.
[167] 354 U.S. 298 (1957).
[168] *Id.* at 318.
[169] *Id.* at 319.
[170] *Id.* at 321-22.
[171] *Id.*
[172] 367 U.S. 717 (1961).
[173] *Id.* at 722.
[174] *Id.* at 731.
[175] *Id.* at 725-29.

procedures it pleases for dealing with obscenity . . . without regard to the possible consequences for constitutionally protected speech."[176] The search and seizure of obscene material called for "sensitive tools," because seizing obscenity "poses problems not raised by the warrants to seize 'gambling implements,' 'all intoxicating liquors'" and other effects.[177]

Although *Marcus* was decided under the Due Process Clause, *Stanford v. Texas*[178] linked the Fourth Amendment interests to the First Amendment. As background, *Stanford* arose during the height of the Second Red Scare. Texas had passed the Suppression Act in response to the perceived Soviet infiltration of the United States. Based upon the legislative findings that "there is a Communist conspiracy committed to the overthrow of the government of the United States, [and the 50 States], by force and violence,"[179] Texas made it a crime to

> Commit . . . or aid in the commission of any act intended to overthrow, destroy, or alter . . . the constitutional form of the United States, or of the State of Texas, or of any political subdivision of either of them by force of violence;
>
> Advocate, abet, advise, or teach by any means and person to commit, attempt to commit, or aid in the commission of any such act, under such circumstances to constitute a clear and present danger to the security of the United States or of the State of Texas, or of any political subdivision of either of them; or
>
> Assist in the formation of, or participate in the management of, or contribute to the support of, or become or remain a member of, . . . the Communist Party of the United States or any component or related part or organization thereof . . . knowing the nature of such organization.[180]

The force of the Suppression Act met John Stanford when Texas law enforcement searched his home, where he operated a mail-order bookstore called All Points of View.[181] Specifically, the affiant indicated that two "credible citizens" had verified that Stanford's home contained "books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments

---

[176] *Id.* at 731.
[177] *Id.* at 730-31 (internal quotation marks and citation omitted).
[178] 379 U.S. 476 (1965).
[179] Vernon's Ann. Revised Civil Statues of Texas, Art. 6889-3A §1 (1960).
[180] *Id.* §5.
[181] Stanford v. Texas, 379 U.S. 476, 479-80 n.2 (1965).

concerning the Communist Party of Texas, and the operations of the Communist Party in Texas . . . ."[182] Based upon this, a judge issued a warrant authorizing the seizure of the laundry list of items "concerning the Communist Party in Texas."[183] The executors of the warrant "spent more than four hours in gathering up about half the books they found in the house" which included "Karl Marx, Jean Paul Sartre, Theodore Draper, Fidel Castro, Earl Browder, Pope John XXIII, and Justice Hugo Black" as well as several of Stanford's personal documents. When Stanford's motion for return of his property was denied, he appealed directly to the U.S. Supreme Court.[184]

The Court assumed the constitutionality of the statute and the probable cause underlying the warrant,[185] and focused solely on whether the warrant was sufficiently particular. After recounting the history of the use of search warrants in England to suppress dissident speech,[186] the Court concluded that "'the commands of our First [Fourth, and Fifth] Amendment[s] . . . are indeed closely related, safeguarding not only privacy and protection against self-incrimination but 'conscience and human dignity and freedom of expression as well.'" [187] Therefore, the Court held that "the constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain."[188] Anything that fails to meet that standard would be considered a general warrant.[189]

By creating the "scrupulous exactitude" test, the Court recognized that privacy in papers extended to papers which could be relevant (in the evidentiary sense),[190] as well as papers that were wholly irrelevant to the government's search. Notably, *Stanford* did not clarify how the government could have met this scrupulous exactitude standard. Instead, the Court merely noted that when the government seized "literary material,"[191] it was a "constitutional impossibility" to leave to the protection of First Amendment freedoms to "the whim of the officers charged with executing the

---

[182] *Id.* at 477.
[183] *Id.* at 479-80.
[184] *Id.* at 480.
[185] *Id.* at 480-81.
[186] *See generally id.* at 482-88; *see also* Price, *supra* note 19 (offering a scholarly analysis of First Amendment history).
[187] *Stanford*, 379 U.S. at 484 (quoting Frank v. Maryland, 359 U.S. 360, 376 (1959) (Douglas, J., dissenting)).
[188] *Id.* at 485 (footnote omitted).
[189] *Id.* at 480.
[190] FED. R. EVID. 401 (defining relevant evidence as any material evidence that has any tendency to make fact or more less probable to exist than if it were excluded).
[191] *Stanford*, 379 U.S. at 485-86.

warrant."[192]

The Burger and Rehnquist Courts signaled that *Stanford* would not augur a broad First Amendment revolution for the Fourth Amendment. For instance, in *Andresen v. Maryland*,[193] the Court upheld a search warrant for a laundry list of business records in an office very similar to the warrant in *Stanford*. Although *Stanford*'s scrupulous exactitude standard is not mentioned (indeed, the phrase "First Amendment" appears nowhere in either the majority or dissenting opinions), Justice Brennan accused the majority of rendering limits on the warrant an "empty promise."[194] He observed that although the Court construed the warrant to fit the crime under investigation post hoc, this construction was not "available to the investigators at the time they executed the warrants."[195] Further, in *New York v. P.J. Video*,[196] the Court declined to subject obscene films to a higher probable cause standard, and instead held that searches for papers would be evaluated by the same standard as effects.

Zurcher v. Stanford Daily[197] marked the biggest setback for a First Amendment revolution to the Fourth Amendment. In *Zurcher*, the police sought a warrant to search the *Stanford Daily* newsroom for "[n]egatives and photographs and films" of an assault on a police officer in order to ascertain the identity of the assailant.[198] The *Stanford Daily* contested the search warrant and argued in pertinent part that "the First Amendment . . . justif[ies] a nearly *per se* rule forbidding the search warrant and permitting only the subpoena *duces tecum*" unless someone at the newspaper was involved with the crime or a subpoena would otherwise be impractical.[199] The *Stanford Daily* argued that the need to maintain the timely operation of newspapers and the potential chilling of news sources justified this general requirement for subpoenas of newsrooms.[200]

Although the Court recalled that it had created the scrupulous exactitude test in *Stanford* for papers, the Court found no support for the subpoena-first protocol requested by the *Stanford Daily*.[201] Rather, the Court noted that nothing in the text of the Constitution required a general rule to issue a subpoena on newsrooms. As for the connection between the First and Fourth Amendments, case law required only that "courts apply the warrant requirements with

---

[192] *Id.*
[193] 427 U.S. 463 (1976).
[194] *Id.* at 492.
[195] *Id.* at 493.
[196] 475 U.S. 868 (1986).
[197] 436 U.S. 547 (1978).
[198] *Id.* at 551.
[199] *Id.* at 563.
[200] *Id.* at 563-64.
[201] *Id.* at 565.

particular exactitude when First Amendment interests would be endangered by the search."[202] The Court then summarily dismissed the newspaper's concerns about the threat to First Amendment rights without the subpoena-first protocol as unfounded.[203]

2. Stanford *and* Zurcher *Create a Framework to Govern Search Warrants for Speech*

Although the Court has limited *Stanford*'s reach beyond establishing an *ex ante* particularity requirement, a particularity requirement properly rooted in the First Amendment can solve the problems created by digital search warrants for speech. To understand how, it is helpful to understand why the Court likely decided *Stanford* on particularity grounds.

Stanford never cites *Dennis* or *Yates*. However, given the Suppression Act's similarity to the Smith Act, these cases likely influenced the decision. If the Smith Act (and its state analogs) is still constitutional after *Yates*, then as a matter of law, the First Amendment prohibits convicting someone for engaging in abstract advocacy. To be convicted under the Smith Act, the defendant must be engaged in advocacy to action.

But what if the government sought a search warrant for conduct which it believed crossed the line from abstract advocacy to advocacy to action? That question is squarely before the court in *Stanford*. There, the Court was reviewing the legitimacy of a search warrant issued pursuant to a violation of a state analog to the Smith Act.[204] The distinction between advocacy of doctrine and advocacy of action is a helpful standard on direct appeal of a criminal conviction. But during the investigative stage, the distinction between the two may be impossible to meaningfully distinguish. This is particularly so when *Yates* relied upon the group's size and cohesiveness as primary indicators of advocacy to action. A warrant based on probable cause may not need to meet the *Yates* standard for size and cohesiveness at trial.

One solution to the abstract advocacy versus advocacy-to-action divide in the search warrant context would be to find that the Smith Act and its state analogs violate the First Amendment. This position has never garnered a majority of votes on the Court. Another solution would be to attack the warrant in *Stanford* for a lack of probable cause. Resolving *Stanford* on probable cause grounds, however, does nothing to uphold the advocacy to action distinction established in *Yates*. As *Stanford*'s facts show, one location could, in theory, be a repository for large and cohesive organizational records.

---

[202] *Id.* at 567.
[203] *Id.* at 565-66.
[204] *See supra* Section III.A.1 (discussing the history and facts behind *Stanford*).

More importantly, relief from an erroneous decision by the magistrate to issue a search warrant is available only after the search has been completed. If the mere execution of a search warrant harms protected speech, reversal of conviction, dismissal of a charge, or monetary relief in a civil action is an inadequate remedy. And, if probable cause existed in some cases, the Court would risk exposing people to criminal prosecution for possessing what an appellate court found was constitutionally protected speech. This, of course, assumes that a hypothetical defendant would not plead guilty to avoid the risk of a trial.

Resolving *Stanford* on particularity grounds, however, creates a constitutional violation prior to the execution of the search. If the warrant were insufficiently particular, the search would be illegal at inception. Although a trial court could erroneously uphold another warrant in *Stanford*, these convictions, to the extent they relied upon the fruits of the search, would be overturned for being insufficiently particular. The exclusionary rule would also provide a deterrent against police even requesting these warrants. Therefore, particularity provided a means of allowing search warrants for a legitimate conspiracy to overthrow the government while also prohibiting the pretextual search warrants that were used to suppress protected speech.

Consequently, even if digital devices have increased the circumstances in which the government has probable cause to search for papers, the Court can counterbalance this development with *Stanford*'s heightened particularity standard. If the government seeks to search for speech, it must describe what should be seized in greater depth than the boilerplate description seen in *Stanford*. And because digital devices are places where First Amendment material is found, even when the government does not target protected speech, it may need to adjust its execution of the search warrant to avoid suppressing speech. Although such a standard cannot require a the government to proceed using a subpoena to protect privacy,[205] the government may be required to utilize other methods of limiting the disclosure of First Amendment protected material.

Moreover, applying *Stanford* to digital devices is reasonable. Searches of digital devices or social media accounts raise the same First Amendment concerns seen with literary materials in *Stanford*. Although cell phones carry a variety of private data, law enforcement is most interested in search warrants seeking text or instant message conversations. This evidence is highly persuasive, probative and often the exclusive means of obtaining this kind of evidence. The anticipated private nature of digital conversations makes their content a confession without a credibility problem.

Additionally, *Stanford* should be understood to apply beyond the

[205] Zurcher v. Stanford Dailey, 436 U.S. 547, 559 (1978).

political speech that created the scrupulous exactitude standard. The lesson to draw from *Wilkes*, *Entick*, *Dennis*, and *Yates* is that both governments and courts have been unable to distinguish the harmless political dissident from the criminal mastermind, as both speak with "the voice of nonconformity."[206] One who abstractly advocates for the overthrow of the United States government should receive the same protection as one who abstractly advocates for drug trafficking or robbery to be legal, or who records a simulation of a violent sexual fantasy.[207] All of those abstract and theoretical thoughts occupy the same First Amendment-protected space to explore ideas.[208]

Of course, the mere fact that someone has recorded thoughts that, if acted upon, would be a crime, can be a reason for the government to seize that speech as evidence. But in order to protect a space for private "abstract" speech, the government must have independent knowledge that the sought speech is more than someone's abstract thoughts. The government can demonstrate this knowledge by demonstrating probable cause that evidence exists of a particular crime on the digital device. Requiring a precise description of the speech sought, rather than the types of documents sought, limits the warrant's reach to documents supporting the probable cause underlying the warrant. Such a limitation will restore the double protection of papers in the digital age. Finally, the overseizure of digital data can be controlled through a use restriction or the elimination of the plain view exception.[209]

If standards can be developed for how courts should describe speech in a warrant, *Stanford* is positioned to be a cornerstone of the digital Fourth Amendment. Because a general warrant is invalid

---

[206] Stanford v. Texas, 379 U.S. 476, 486 (1965).

[207] For a case illustrating this point, see *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015). In *Valle*, the defendant was convicted of conspiracy to commit kidnapping because of his conversations about acting on his fetish of kidnapping and cannibalizing women. In upholding the trial judge's judgment of acquittal, the Second Circuit concluded Valle's speech was a mere "fantasy" and "the remaining evidence [was] insufficient to prove the existence of an illegal agreement or Valle's specific intent to kidnap anyone." *Id.* at 511; *see also* PREET BHARARA, DOING JUSTICE: A PROSECUTOR'S THOUGHTS ON CRIME, PUNISHMENT, AND THE RULE OF LAW 161-65 (2019) (discussing Bharara's hesitation and decision to prosecute this case).

[208] *See* Stanley v. Georgia, 394 U.S. 557, 566 (1969) (recognizing First Amendment protection against thought control); Ashcroft v. Free Speech Coalition, 535 U.S. 234, 253 (2002) (same).

[209] The ACLU maintains that the plain view exception does not apply to digital search warrants. *See generally* ACLU Brief, *supra* note 84. Because the plain view exception applies to seizures of rather than searches for evidence, I do not think courts can use the plain view exception to justify a seizure of overseized digital evidence. *See id.* at 21 (making this argument); Kerr, *supra* note 135, at 22-24 (suggesting plain view exception may not apply to digital search warrants for this reason). Ultimately, as both rules both create a constitutional exclusion requirement, the distinction is not something I have strong views on.

even prior to the search's execution, the fruits of search do not affect whether the warrant was sufficiently particular. Consequently, even if Stanford's home contained records that showed the existence of a vast and highly `organized communist conspiracy, *Stanford*'s warrant would still be unconstitutional. Although critics will decry the costs for law enforcement, criminal defense attorneys will be equipped with a Supreme Court precedent over fifty years old that is consistent with the understanding of the Constitution both at the Founding and today. Although *Stanford* has not materialized into the First Amendment revolution civil liberty advocates were hoping for, the Supreme Court has never implicitly or explicitly questioned or overruled its core holding.

B. Summarization of Content or Metadata Parameters of the Suspect Content Meet Scrupulous Exactitude

Devising standards for how courts can describe all of the different kinds of speech that exist on digital devices is beyond the scope of this Article. Part of the difficulty is that protected speech exists in many forms: in writing, in images, or possibly even in location-tracking messages.[210] This Article has elected to focus on how courts should describe speech when the government seeks to seize written messages on a digital device. These messages are by far the most common type of evidence sought and used because written materials give the government highly incriminating information. Such speech is also the same speech that is likely to contain the most private details about someone's life. Second, this Article also does not address the parts of particularity descriptions dedicated to whether the government overseizure of data was reasonable.[211] Rather, this Section is focused on particularity concerns with the data seized by the government.

Section 1 explains the legal basis for concluding that requiring an *ex ante* description of the sought-after speech or the metadata parameters describing that speech would be most consistent with *Stanford*'s scrupulous exactitude standard. Section 2 responds to the criticism that metadata manipulation would render a metadata-parameters approach impractical.

---

[210] For a discussion of whether location-tracking signals are "communicative" and therefore protected by the First Amendment, see Section IV.A.1.

[211] United States v. Blake, 868 F.3d 960, 967, 974 (11th Cir. 2017) (concluding that government's search warrant of all Facebook data was unreasonable because of Facebook's ability to reliably limit the disclosure of evidence).

1. *Precedent Supports Summarization of Content or Metadata Parameter Description*

A survey of lower courts that have attempted to define "scrupulous exactitude" reveals courts attempting, unconvincingly, to distinguish *Stanford* from the cases before them. For instance, some courts have distinguished *Stanford* from typical criminal investigations by finding a difference between "the seizure of writings to suppress them and the seizure of writings for use as evidence."[212] Other courts, such as the D.C. Circuit in *United States v. Heldt*,[213] have distinguished *Stanford* by claiming that scrupulous exactitude applies to "books" or "expressions of ideology," but not to speech concerning "ordinary unlawful conspiracies and substantive criminal offenses."[214]

These opinions ignore the critical facts of *Stanford*: Texas was attempting to gather evidence for a criminal case charging Stanford with participating in an unlawful communist conspiracy to overthrow the U.S. government. Texas claimed it had probable cause that Stanford "was an official in the Communist Party of Texas, [who] distributed literature espousing the Communist line, [and] that the literature and books were . . . instruments . . . to forward the aims and purposes of the Communist Party."[215] This literature was a "part of the tools and instruments used in perpetrating the crime of advocating or committing the overthrow of the government by force or violence."[216]

Given that both *Heldt* and *Stanford* involved conspiracies against the federal government, the distinction between an "ideological" and an "ordinary" conspiracy could signal one of two things. First, the distinction could distinguish conspiracies by their objective: in *Stanford*, the defendant had an ideological communist objective, whereas *Heldt*'s conspiracy was an ordinary criminal one. This distinction, however, suggests that ideological conspiracy is merely a code word for dissent the government approves of. But *Stanford*,

---

[212] *See, e.g.*, State v. Jones, 705 A.2d 373, 383 (N.J. App. 1998); Wabun-Inini v. Sessions, 900 F.2d 1234, 1240 (8th Cir. 1990) (finding *Stanford* was a prior restraint case); United States v. Truglio, 731 F.2d 1123, 1127 (4th Cir. 1984) (finding seized evidence not subject to *Stanford* because the items were "evidentiary materials") (citation omitted), *overruled on other grounds by* United States v. Burgos, 94 F.3d 849 (4th Cir. 1996); People v. Allison, 452 N.E.2d 148, 152 (Ill. App. 1983) (finding *Stanford* distinguishable because books seized "were used during the commission of a crime, and were evidence of the offense").

[213] 668 F.2d 1238, 1257 n.27 (D.C. Cir. 1981).

[214] *See, e.g.*, *id.*; *see also* United States v. Hubbard, 493 F. Supp. 209, 224-25 (D.D.C. 1979); United States v. Leta, 332 F. Supp. 1357, 1359-60 (M.D. Pa. 1971).

[215] Supplemental Brief for Respondent at 14-15, Stanford v. Texas, 379 U.S. 476 (1965) (No. 40).

[216] *Id.* at 16.

explicitly, signaled that its decision was made for those whose dissention was nonconforming to current political thought.[217] Indeed, the Supreme Court has reaffirmed that *Stanford* applies in ordinary criminal cases without regard to their special ideological content.[218]

Alternatively, ideological conspiracies could refer to abstract conspiracies in the books of Karl Marx, Fidel Castro, and other communist writers. And an ordinary criminal conspiracy could refer to a concrete ongoing conspiracy in action. If that is the distinction, however, then *Heldt* should not have concluded that the scrupulous exactitude standard does not apply. Instead, *Heldt* should have concluded it was met.

For what it is worth, *Heldt*'s facts also support a finding that scrupulous exactitude was met. The items challenged under the warrant did not contain generic categories such as "books" or "papers." Rather, the warrant identified documents by their titles.[219] And although *Heldt* believed that the probable cause was less than ideal for some items, it concluded that there was probable cause to believe these specific documents were evidence of a crime.[220] Therefore, *Heldt* was a far crime from the vague "books" and "pamphlets" that permitted officers discretion to seize literature about communism as opposed to an active communist conspiracy.

Few lower court opinions accept that *Stanford* applies to criminal activity and is not a prior restraint case. But the few that do offer clues as to how such a standard could apply to digital search warrants for speech. The first principle is simple: Where the government knows the content of the speech it seeks to seize, repeating or summarizing the speech will satisfy scrupulous exactitude. For instance, in *New York v. P.J. Video*,[221] local police officers had obtained several videos to look for possible violations of New York's obscenity laws. The affiant "summariz[ed] the theme of, and conduct depicted in, each film" in the affidavit.[222] Although the issue before the Court was whether the scrupulous exactitude standard required a higher standard of probable cause,[223] the lack of a particularity challenge is enlightening. If the government's

---

[217] Stanford v. Texas, 379 U.S. 476, 486 (1965).
[218] Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978); New York v. P.J. Video, 475 U.S. 868, 871 (1986); *see also* Nixon v. Administrator of General Servs., 433 U.S. 425, 461 (1977) ("*Stanford* invalidated a search aimed at obtaining evidence that an individual had violated a sweeping and many-faceted law which, . . . create[d] various individual criminal offenses, each punishable by imprisonment for up to 20 years.") (internal quotation marks omitted).
[219] United States v. Heldt, 668 F.2d 1238, 1257 n.26 (D.C. Cir. 1981).
[220] *Id.* at n.27.
[221] 475 U.S. 868, 870 (1986).
[222] *Id*.
[223] *Id.* at 874-76.

description of the contents is an accurate summary of what it seeks, then it meets the scrupulous exactitude standard.

Of course, for most digital search warrants, the government seeks to search for conversations or images because it does not know their contents. In this circumstance, scrupulous exactitude requires that warrants particularly describe unknown communications between subjects by metadata that distinguishes the speech that should be seized from that which should not. For text message conversations, this will generally entail a description of the conversation's timeframe, participants, and anticipated subject matter. As an example, suppose that the police are investigating a murder and learn that the suspect and victim were arranging a narcotics transaction shortly before the victim died. Assuming sufficient probable cause, these facts would authorize the seizure of communications between Suspect and Victim from Time A and Time B arranging for the sale of narcotics.

United States v. Klein[224] illustrates how the metadata approach to particularity is consistent with scrupulous exactitude. In *Klein*, federal agents obtained a search warrant to seize "'8-track electronic tapes and tape cartridges which are unauthorized "pirate" reproductions'" in violation of copyright law.[225] Of course, the problem with such a warrant is simple: whether a particular cassette is subject to seizure can only definitively be established by listening to its contents. But like a digital search warrant, to access the contents of the tapes, the agents needed to seize them first.[226]

Relying in part on the First Amendment considerations in *Marcus* and *Stanford*, the First Circuit found the warrant insufficiently particular because it failed to identify how officers were to distinguish pirated tapes from legitimate tapes.[227] However, in dicta, the court indicated that based upon representations by the United States, future search warrants could particularly describe films with "crudely" designed advertising jackets, as well as mismatches between an artist and the production company.[228]

This dicta provides helpful guidance for solving the problems posed by digital search warrants. For digital search warrants, the rich availability of metadata permits agents to use that metadata to particularly describe conversations for which they lack precise knowledge. Indeed, we already employ these rules for searches in the physical world. For instance, the Court has held that officers are allowed to search for sought items only in places where the item could physically be located (e.g., one cannot search for a large TV

[224] 565 F.2d 183 (1st Cir. 1977).
[225] *Id.* at 184.
[226] *Id.* at 188.
[227] *Id.* at 190.
[228] *Id.* at 186 n.5, 188.

in a silverware drawer).[229] The size of the object must be less than or equal to the size of the area to be searched. Our question is how to apply this rule to intangible data. Case law supports the use of subject matter, time, and participants as limiting criteria in the case of a search for certain conversations.

As to subject matter, recall that in *Entick* one of the prime reasons the warrant was found to be a general warrant was that it authorized the seizure of "papers" rather than libelous papers. This description left "nothing in the warrant to confine [the search]."[230] In lamenting the collapse of the mere evidence rule, the Second Circuit noted in *United States v. Bennett*, that "[t]he reason why we shrink from allowing a personal diary to be the object of a search is that the entire diary must be read to discover whether there are incriminating entries; most of us would feel rather differently with respect to a 'diary' whose cover page bore the title 'Robberies I Have Performed.'"[231] Thus, even an imprecise description of the subject matter can help limit what is subject to seizure.

As to participants in the conversation, authority can be gleaned from the Court's handling of wiretaps. *Berger v. New York*[232] required that any warrant for a wiretap particularly describe the "conversations" as property to be seized.[233] Although a Title III wiretap order requires a description of the identities of the persons, if known, whose conversations will be seized,[234] little authority exists on the Fourth Amendment requirement for participants. However, *United States v. Kahn*[235] strongly indicates that some specification is likely required to prevent a warrant for communications from being a general warrant. *Kahn* involved a wiretap order on a residential home, which Irving Kahn was suspected of using as a gambling operation. The government sought a wiretap for his phone for conversations involving him and "others as yet unknown."[236] When the government seized conversations of his wife Minnie Kahn participating in taking bets, the government seized those conversations to use as evidence. The Court rejected the Court of Appeals's suggestion that the warrant for "others yet unknown" was a general warrant because the order "required the agents to execute the search warrant in such a manner as to minimize the interception of any innocent conversations," "limited the length of any possible interception to 15 days," and required "status reports as to the progress of the wiretap to be submitted to the District Judge

[229] Horton v. California, 496 U.S. 128, 141 (1990).
[230] Entick v. Carrington, 19 How. St. Tr. 1029, 1065 (C.P. 1765).
[231] United States v. Bennett, 409 F.2d 888, 897 (2d Cir. 1969).
[232] 388 U.S. 41 (1967).
[233] *Id.* at 58-59.
[234] 18 U.S.C. § 2518(4)(a) (2018).
[235] 415 U.S. 143 (1974).
[236] *Id.* at 149.

every five days."[237]

If the minimization and judicial oversight procedures were the only thing that saved *Kahn* from being a general warrant, then search warrants for text messages are likely susceptible to constitutional challenge. Unlike the wiretap order in *Kahn*, digital search warrants have no requirement for minimization, time restrictions, or judicial oversight. The inability to minimize the seizure of conversations is the exact problem courts are facing now.

Moreover, the basics of timeframe descriptions are settled law: even the federal government instructs agents to impose time parameters on search warrants where a timeframe will be known.[238] For most state-law crimes, the time parameters could be based on the probable cause that lays out the facts. For instance, for state-law crimes that are incident-based time parameters to encompass a reasonable amount of time before or after the crime could be imposed. For crimes involving a continuous course of conduct (such as conspiracies or narcotics trafficking), time parameters for which there is probable cause could be imposed. Courts could elect to set bright-line rules regarding reasonable time parameters or allow fact-specific decisions.

Last, the rules for particularity should be functional. If a search warrant were to authorize the seizure of John Doe and Jane Roe, contact names may be under aliases or nicknames to help avoid detection by law enforcement. To solve this problem, the metadata descriptions should operate functionally: The government could be authorized to seize conversations between two people, no matter how the metadata expresses those identities. One could even imagine the contents of the messages themselves being used to prove circumstantially that a conversation occurred between two people.

2. *Scrupulous Exactitude, When Combined with a Use Restriction, Can Properly Balance Law Enforcement Needs with Privacy Rights*

Kerr has objected to the use of metadata in certain proposed search protocols. Kerr rightly notes that criminals can change metadata, such as a "date created" field, and that such manipulation could thwart a search protocol.[239] If the government fails to find any evidence specified in the search warrant, he argues, the only way to rule out whether that evidence exists elsewhere is to search the entire

---

[237] *Id.* at 154-55.

[238] United States v. Ford, 184 F.3d 566, 576 (6th Cir. 1999) ("Failure to limit broad descriptive terms by relevant dates, when such dates are available to police, will render a warrant overbroad."); DOJ Manual, *supra* note 15, at 73.

[239] Kerr, *supra* note 135, at 16-17.

device in light of this risk of metadata manipulation.[240]

If we move from a search protocol model to a particularity model, we can avoid this problem. Metadata parameters describe only what the government is ultimately authorized to seize. Thus, if the government believes that metadata has been manipulated, they are more than welcome to search whatever areas of the digital device they believe may contain the evidence, so long as they have particularly described what they are looking for.

However, a scrupulous exactitude model is not sufficient to protect privacy. If officers uncover evidence that they cannot show falls within the metadata parameters described in the search warrant, a use restriction must preclude use of that evidence at trial. If *Stanford*'s "scrupulous exactitude" requirement is combined with the use restriction model, the government will be incentivized to execute searches reasonably. Under this model, the reasonable execution of the search is not a problem that the judiciary has to solve ex ante or post hoc.

For instance, suppose that the government obtains a warrant to search someone's cell phone for text messages sent from the suspect to the victim concerning a robbery on a particular day. If the government does not believe that the robbery suspect has manipulated the metadata on his phone, they will likely not look at conversations from three months prior. With every search there is always a risk that there could be evidence of criminal activity related or unrelated to the criminal activity under investigation. If the government wishes to preserve its ability to obtain a subsequent search warrant, it will need to limit its exposure to data outside the scope of the warrant. To do that under a use restriction regime, the government needs to limit the amount of overseized data it requests or is exposed to. Consequently, the chance of finding highly desired needles related to this crime or other crimes in the largely unresponsive hay acts a threat to ensure reasonable execution of the warrant—if the government looks beyond the scope of its warrant, those needles may be unusable.

There are two main anticipated objections to this approach. One might question whether the metadata categories listed in Section 1 are sufficient to describe speech with scrupulous exactitude. The other objection is that in vast, multi-year conspiracies, the description of things to be seized will either insufficiently protect privacy or hamper government investigations.[241] This latter criticism is addressed in Part III.C.2.

---

[240] *Id.*

[241] For instance, if someone is suspected of being middle management in a human trafficking ring, the government may seek a search warrant for that person's cell phone, claiming probable cause to believe evidence of illegal conduct pervades the entire device.

Regarding the first objection, concerns over the manipulation or nonexistence of reliable metadata are overblown. At the outset, those concerned about the manipulation of metadata make empirical claims about the risk without any statistical evidence to back up their claims.[242] For instance, the Sixth Circuit concluded that "most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers" have failed due to the concerns over the manipulation of data.[243] However, in reaching that conclusion, the Sixth Circuit relied on cases involving only child pornography.[244] But the challenges in combating child pornography should not create a race to the bottom for everyone's privacy, particularly when child pornography is not suspected of being on a device.

I raise the lack of empirical support for widespread data manipulation because in my role as a defense attorney, I have seen hundreds of returns from digital search warrants and forensic analyses of cell phones, and I have never experienced nor had a prosecutor assert that a client manipulated data to avoid detection. Instead, the most common way for criminal defendants to manipulate data is to delete it altogether. I do not bring this up to debate using anecdotal evidence. Rather, courts should be more mindful of when they accept "criminals manipulate metadata" rationales when the Supreme Court has repeatedly rejected government fear about this criminal behavior with new technology as lacking sufficient empirical support to affect constitutional law.[245] Expansive warrants based upon manipulation of metadata concerns

---

[242] *See, e.g.*, United States v. Ulbricht, 858 F.3d 71, 102 (2d Cir. 2017) ("Files and documents can easily be given misleading or coded names, and words that might be expected to occur in pertinent documents can be encrypted; even very simple codes can defeat a pre-planned word search."); United States v. Mann, 592 F.3d 779, 782-83 (7th Cir. 2010) (rejecting search protocol for images because "computer files may be manipulated to hide their true contents"); United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) ("Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.").

[243] United States v. Richards, 659 F.3d 527, 538-39 (6th Cir. 2011).

[244] *Id*. (citing United States v. Stabile, 633 F.3d 219, 239 (3d Cir. 2011); United States v. Banks, 556 F.3d 967, 973 (9th Cir. 2009); United States v. Summage, 481 F.3d 1075, 1079-80 (8th Cir. 2007); United States v. Grimmett, 439 F.3d 1263, 1269-70 (10th Cir. 2006); Guest v. Lies, 255 F.3d 325, 336 (6th Cir. 2001); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999)).

[245] *See, e.g.*, Riley v. California, 573 U.S. 373, 389 (2014) (rejecting concerns over remote-wiping of a cell phone or fears of a suspect encrypting a digital device in response to potential search because of inability to show "that either problem is prevalent"); Ashcroft v. Free Speech Coalition, 535 U.S. 234, 254 (2002) (rejecting government argument that "virtual images [of child pornography] . . . are indistinguishable from real ones" to justify ban on virtual child pornography because "[f]ew pornographers would risk prosecution by abusing real children if fictional, computerized images would suffice.").

should be based upon particular crimes, or particular characteristics of the defendant or their phone (such as the possession of apps that could manipulate metadata).

Second, metadata manipulation assumes a criminal's plan is to hide incriminating information as opposed to deleting it. This will depend on the crime. People in possession of child pornography have an incentive to hide the file, but a robber has no need to keep his conversations regarding the robbery. The robber, like most criminals, would be incentivized to delete metadata rather than manipulate it. (Most criminals, however, are unaware that information is not actually "deleted" from a digital device until it is overwritten by other data.)

Third, even if metadata manipulation of conversation participants or time were effective or widespread, other rules could help facilitate the government's seizure of that data. For instance, a rule that found that the government has the authority to seize any communications whose authentic metadata contained participants *A*, *B*, *C* between times *X* and *Y* would permit the government to seize evidence whose metadata did not reflect those parameters but, based upon circumstantial evidence, could be determined was manipulated. Indeed, if a search warrant for a suspect's home for clothes worn during a murder results in the discovery of clothes in the dryer with a host of cleaning products, the seizure of the items has become more probative due to the potential evidence of tampering. In this vein, an investigation into the manipulation of metadata could be upheld for similar reasons.[246]

Finally, even if a risk of metadata manipulation exists, there should be a justification of the invasion of privacy. The more one is willing to entertain the risks of manipulated metadata (such as dates) and content, the higher the risk of seizing innocuous speech as evidence of criminal activity becomes. Consider the problem posed by violent rap lyrics being used as evidence of criminal activity. In *State v. Skinner*,[247] the New Jersey Supreme Court held the use of fictitious violent rap lyrics as evidence of prior bad acts in a murder case was impermissible without "a strong nexus" between the lyrics and the underlying offense. As the court correctly noted, "the difficulty" in using fictional narratives as probative evidence is that "one cannot presume that, simply because an author has chosen to write about certain topics, he or she has acted in accordance with those views."[248] For example, "[o]ne would not presume that Bob Marley, who wrote the well-known song 'I Shot the Sheriff,' actually

[246] For an explanation of why such a search would not have to independently meet *Stanford*'s scrupulous exactitude requirement, see Part IV, explaining the business records exception.
[247] 95 A.3d 236, 239 (N.J. 2014).
[248] *Id.* at 251.

shot a sheriff . . . ."[249]

The New Jersey Supreme Court's "strong nexus" requirement for other bad acts evidence is consistent with the Supreme Court's treatment of abstract speech in *Dennis* and *Yates*. Recall in *Yates*, the Court found that speech could not be criminalized for advocating violent acts unless it crossed an impermissible threshold of "advocacy to action."[250] *Skinner* simply applies *Yates*'s distinction for the rules of evidence. This transference is consistent with the underlying harm *Yates* sought to prevent: convictions based on someone's unpopular thoughts.

But if officers are permitted to seize any evidence that, within an officer's sole discretion, is viewed as manipulated, then *Stanford*'s requirements are effectively evaded. The harms identified in *Yates* and *Skinner* can occur in the search warrant context if an officer is permitted to seize anything within its discretion as manipulated data. But if there limits to courts' willingness to entertain an officer's claims that data was manipulated, these limits should be similar to the "strong nexus" requirement in *Skinner* or the "advocacy to action" standard in *Yates*. The "scrupulous exactitude" is the search warrant equivalent of these free speech doctrines. Therefore, the scrupulous exactitude requirement, as I see it, was designed to preserve *Yates* in the search warrant context.

C. Controlling for Breadth with the Foregone Conclusion Floor

Once a set of metadata parameters can be used to help separate speech which should not be seized, the next question is how broad to make those parameters. I propose that the foregone conclusion doctrine from the Fifth Amendment context provides a First Amendment floor by which the government must be able to particularly describe the items to be seized in a search warrant.

First, this Foregone Conclusion Floor is consistent with Supreme Court doctrine. An analysis of the cases that created the foregone conclusion doctrine and *Stanford* demonstrates that the principal evil these decisions targeted was the discretion that the executor of the search warrant or the records custodian had in determining what to seize or disclose. Eliminating this discretion in the would also restore the double protection of papers: the government would be limited to seizing items based on the probable cause it had independently developed prior to the execution of the search warrant.

Second, the Foregone Conclusion Floor ensures that the government does not have greater access to compulsory process than the defense. Unequal means of compulsory process damages the criminal justice system in two respects. It prevents the defense from

---

[249] *Id.*

[250] *Yates v. United States*, 354 U.S. 298, 322 (1957).

being able to equally discover evidence to help its case. And second, it incentivizes the government to proceed with search warrants to have broader access to information. Understanding this incentive structure helps explain the battle over compelled decryption of digital devices and why it matters to the government.

1. Supreme Court Doctrine Supports a Foregone Conclusion Floor for Search Warrants

To help demonstrate a convergence between First, Fourth, and Fifth Amendment jurisprudence, this subsection begins with an explanation of the foregone conclusion doctrine. Recall the *Boyd* Court's conception that the Fourth and Fifth Amendments "run almost into each other."[251] In making this observation, *Boyd* held that seizing someone's papers for their contents would amount to "forcible and compulsory extortion of a man's own testimony."[252] However, after the collapse of the mere evidence rule in *Warden v. Hayden*,[253] *Boyd*'s conclusions concerning a Fifth Amendment right in the contents of papers were sure to follow.

In *Fisher v. United States*,[254] the Court revamped the Fifth Amendment's relationship to papers. *Fisher* concerned an Internal Revenue Service investigation into various taxpayers for violations of civil and criminal income tax laws.[255] The government learned that the papers it sought for the investigation were in the hands of the taxpayers' lawyers and issued subpoenas for income tax records, accountant work product, and deposit slips. The lawyers objected to the subpoena on the grounds that the Fifth Amendment protected the papers from seizure due to their contents.[256] The Court overruled *Boyd* and found that because the act of producing the documents does not "ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought," the incriminating nature of the document itself could not be the basis of a Fifth Amendment objection.[257]

Still, because the government does compel the production of documents, the Court found that compliance has "communicative aspects of its own."[258] For instance, "[c]ompliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the

[251] Boyd v. United States, 116 U.S. 616, 630 (1886).
[252] *Id.*
[253] 387 U.S. 294 (1967).
[254] 425 U.S. 391 (1976).
[255] *Id.* at 393-94.
[256] *Id.* at 405-08.
[257] *Id.* at 409.
[258] *Id.* at 410.

subpoena."[259] The Court nevertheless found that the records at issue here "belong to the accountant, were prepared by him, and are the kind usually prepared by an accountant working on the tax returns of his client."[260] These characteristics made the "existence and location of the papers . . . a foregone conclusion."[261] Because the government was not relying upon the testimony of the taxpayer, the question became one of surrender rather than of testimony.[262]

The only definitive limit placed on the foregone conclusion doctrine was developed in *United States v. Hubbell*.[263] There, an investigation into a possible violation of Hubbell's plea agreement was launched and the Independent Counsel sought, among other records, "'any and all documents reflecting, referring, or relating to any direct or indirect sources of money or other things of value received by or provided to' an individual or members of his family during a 3-year period."[264] Hubbell complied with the subpoena only when the government gave him immunity "to the extent allowed by law."[265] Upon examination of the documents, the Independent Counsel obtained an indictment for tax evasion.[266] On appeal, the government argued that the records' existence was a foregone conclusion because "a businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena."[267] The Court rejected this "overbroad argument" because the government had not shown that it knew of "the existence or whereabouts" of the documents sought.[268]

Although the Supreme Court has never articulated how the government should show it has the requisite knowledge of the existence and whereabouts of responsive documents, half of the federal courts of appeals have explicitly or implicitly adopted a "reasonable particularity" standard.[269] Under this standard, courts

---

[259] *Id.*
[260] *Id.* at 411.
[261] *Id.*
[262] *Id.*
[263] 530 U.S. 27 (2000).
[264] *Id.* at 41.
[265] *Id.* at 30-31.
[266] *Id.*
[267] *Id.* at 45.
[268] *Id.*
[269] *See, e.g.*, United States v. Apple MacPro Computer, 851 F.3d 238, 247-48 (3d Cir. 2017) (reasonable particularity met for compelled decryption of digital device where government demonstrated files exist and defendant could access them); In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1344 (11th Cir. 2011) (holding that where "the location, existence, and authenticity of the purported evidence is known with reasonable particularity," the foregone conclusion doctrine applies); United States v. Ponds, 454 F.3d 313,

look to how well the government has described the documents as a way to infer whether the government had sufficient knowledge of their existence or whereabouts at the time the subpoena was issued.[270] The more particular the description, the more likely the government is not relying upon the communicative aspects of production to establish the existence or whereabouts of an object.

The widespread adoption of the reasonable particularity standard is interesting because courts are using the Fourth Amendment concept of particularity to help define the limits of a Fifth Amendment right. In that respect, *Boyd*'s conclusion that the Fourth and Fifth Amendments "almost run into one another" remains true to a certain extent. What has changed is the point of intersection. Whereas the mere evidence rule defined the intersection broadly based on the documents' contents, the reasonable particularity standard shifts the intersection to the act of production.

Doctrinally, *Stanford*'s scrupulous exactitude standard appears to govern search warrants in a similar manner that the forgone conclusion doctrine governs subpoenas. Courts should recognize this intersection because both doctrines seek to prohibit the same discretion in the person executing the warrant or complying with the subpoena. In this respect, while the Fifth Amendment prevents self-incrimination in response to an overbroad subpoena, the First Amendment protects the government's discovery of the same material from a general warrant to protect First Amendment speech.

As proof that both doctrines prohibit the same mental task, consider the particularity descriptions of items to be seized in

---

324 (D.C. Cir. 2006) (holding that government failed to meet reasonable particularity standard when it did not *ex ante* know the location or existence of "most of the subpoenaed documents"); In re Grand Jury Subpoena Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004) (reasonable particularity standard not met where the "breadth of the subpoena . . . far exceeded the government's knowledge about the actual documents that Doe created or possessed"); In re Grand Jury Subpoena Duces Tecum Dated Oct. 29 1992, 1 F.3d 87, 93 (2d Cir. 1992) (holding target's uncoerced statements and prior production of documents satisfied reasonable particularity standard); *see also* In re Grand Jury Proceedings, Subpoena for Documents, 41 F.3d 377, 380 (8th Cir. 1994) (holding that application of foregone conclusion doctrine depends "on the particular wording of the subpoena in question—the broader, more general, and subjective the language of the subpoena, the more likely compliance with the subpoena would be testimonial"). No circuit has disagreed with the reasonable particularity standard. Rather, other circuits have decided these cases without articulating a legal rule. United States v. Stone, 976 F.2d 909, 911-12 (4th Cir. 1992) (finding foregone conclusion met through analogy to *Fisher*); Butcher v. Bailey, 753 F.2d 465, 469 (6th Cir. 1985) (distinguishing *Fisher* because producing documents would authenticate them); United States v. Bengivenga, 845 F.2d 593, 600-01 (5th Cir. 1985) (holding without further explanation that the production of baggage claim stub was nontestimonial).

[270] Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 775 (2019).

Hubbell:

> Any and all documents *reflecting*, *referring*, or *relating* to any direct or indirect sources of money or other things of value received by or provided to Webster Hubbell, his wife, or children from January 1, 1993 to the present, including but not limited to the identity of employers or clients of legal or any other type of work.[271]

And compare it to the description relied on in *Stanford*:

> [B]ooks, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments *concerning* the Communist Party of Texas, and the operations of the Communist Party in Texas . . . .[272]

The problem with *Stanford*'s search warrant and *Hubbell*'s subpoena is deferring entirely on the question of responsiveness to the individual executing the warrant or responding to the subpoena. *Stanford*'s warrant gave the executors the discretion to decide what "concerned" the Communist Party in Texas or forced the respondent to use the contents of the mind to determine whether a document "reflect[ed], refer[red] or relat[ed]" to indirect sources of money amongst Hubbell's family members. In order to comply with *Stanford* or *Hubbell*, the government would have to describe the items in such a way as to demonstrate it knew that such documents existed.

To hold otherwise would mean that the government's actual error in *Hubbell* was not proceeding by a search warrant, and that *Stanford*'s warrant could be cured by proceeding with a subpoena. But if the legal process changed, the underlying logic from both opinions should follow the change. Consequently, the First, Fourth, and Fifth Amendments "almost run into one another" because they require the government to demonstrate *ex ante* what concerns, relates, refers, or relates to the particular subject matter so that the only task for the executor or records custodian is to find the particularly described items.

To see how such a standard would affect currently issued digital search warrants, reconsider the facts of *Knoefel*. There, the government's probable cause to search the phone was based upon

---

[271] *Hubbell*, 530 U.S. at 46 (emphasis added). There were ten other categories for similar types of items with similar breadth.

[272] Stanford v. Texas, 379 U.S. 476, 478-79 (1965) (emphasis added). The description is taken from the district court order. Although it is not clear from the court records, the warrant likely lifted language from the statute itself, as the statute contains identical language. Vernon's Ann. Revised Civil Statues of Texas, Art. 6889-3A §9 (1960).

three facts: (1) the location of the phones in room where a murder took place; (2) that the suspect was in the room where the phones took place; and (3) the detective's experience and training that people communicate through cell phones. However, the magistrate issued a warrant authorizing the seizure of all digital data in a laundry list reminiscent of the warrant in *Stanford* with the limiting criterion to seize "anything *in connection* with the crimes of Murder and/or Aggravated Murder."[273]

Under the Foregone Conclusion Floor, this warrant would be a general warrant with respect to the speech is seized because it left it within the discretion of the executing officer to decide what evidence had a "connection" to the murder. Although the state can argue that it is a "foregone conclusion" that people communicate through cell phones, this is similar to the rejected businessmen-keep-business-records rationale in *Hubbell*.[274] Rather, it was a task for the magistrate to decide what was connected to the murder, and the only task for the executing officer should have been to determine "is this item within a list of particularly described speech?" Thus, the inability to describe the sought speech precludes rather permits sought search warrant.

In sum, when the particularly requirement is broader than the Foregone Conclusion Floor, individuals know that their digital devices can be rifled through according to whatever an officer believes is evidence. Placing such judgment in the "hands of every petty officer" was the quintessential feature of the general warrant.[275] But the consequences for searches of speech are more far-reaching. If the threat of surveillance is sufficiently felt individuals will be less likely to commit their private unpopular thoughts to paper or to communicate them on documents. This threatens the ability of individuals to privately determine whether laws should change, explore the world, and harbor thoughts that if acted upon society would condemn. On a long enough timeline, this fear will in itself be used to control thoughts—a position that is "wholly inconsistent with the philosophy of the First Amendment."[276]

However, when the Foregone Conclusion Floor limits the scope of the government's search warrant, the warrant is limited to

---

[273] State v. Knoefel, No. 2014-L-088, 2015-Ohio-5207, ¶128 (Ohio App. 2015) (emphasis added). The exact description was a list of all possible kinds of documents that could exist on a phone. *See supra* note 4 and accompanying text for the exact list. Because such a list in the abstract would be a general warrant, the court made a post hoc construction which is quoted here.

[274] *See supra* notes 251-256 and accompanying text.

[275] *Stanford*, 379 U.S. at 482.

[276] Stanley v. Georgia, 394 U.S. 557, 566 (1969); *see also* Ashcroft v. Free Speech Coalition, 535 U.S. 234, 253 (2000) ("First Amendment freedoms are most in danger when the government seeks to control thought or to justify its laws for that impermissible end.").

authorizing the seizure of items for which it has independent probable cause to collect. Such a limitation helps restore the double protection of papers for digital speech. Although the government may have an easier time obtaining probable cause for search warrants, *Stanford* provides a doctrinal basis for limiting the scope of the government's warrant to the probable cause that gave rise to the search. When this limitation is enforced, it counterbalances the government's easier access to digital papers by narrowly limiting the kinds of data subject to seizure.

2. How the Foregone Conclusion Floor Applies to Continuous Course of Conduct Crimes

This Article has so far considered single-incident crimes. Special consideration should be taken for crimes involving a continuous course of conduct. In these cases, questions arise as to whether the police may only obtain a search warrant to search for evidence of the instances of conduct they are already aware of, or whether the government can search for conduct they believe—but do not know—exists. My view is that where the government can plead sufficient facts within an affidavit to show a continuous course of conduct within a given timeframe, the government's search warrant may search for speech related to the known incidents as well as for speech with other individuals currently unknown to the government.

For example, if the government has conducted several controlled buys with a drug trafficker between time *A* and time *B*, the government may search for conversations with other buyers and suppliers of the drugs during that timeframe. Once the pattern of conduct can be established through the officer's affidavit that probable cause exists to seize some conversations about narcotics transactions that may make it a forgone conclusion that other conversations with other persons currently unknown also exist within a specified timeframe.

However, the standard for whether a continuous course of conduct standard applies should not merely be a question of recidivist behavior. For instance, if the government were to get a search warrant for evidence of domestic violence, the government should not be able to seize earlier conversations only because domestic violence has a high recidivism rate,[277] unless there is independent probable cause that another incident occurred. Recall

[277] The Bureau of Justice Statistics has indicated that close to eighty percent of females who had been a victim of domestic violence had more than one domestic violence incident with the same person. *Intimate Partner Violence*, BUREAU JUST. STAT. 4, https://www.bjs.gov/content/pub/pdf/ipv9310.pdf [https://perma.cc/TC8P-E5XL].

that a search warrant requires evidence of a *crime* to be the found at the particular place to be searched.[278] Without the underlying physical evidence of violence, evidence that an argument occurred is not evidence of domestic violence. However, the same result may not be reached if the government were to obtain a search warrant for the crime of stalking, which in some states may be committed through mere electronic communication.[279]

This framework still properly preserves *Stanford*'s role of protecting speech while not requiring the police to know of every unlawful transaction prior to searching for speech related to the transaction. Because the government's ability to search someone's device is linked to the amount of probable cause the police have, the scope of the search will be limited by the probable cause underlying the warrant.

3. The Foregone Conclusion Floor Promotes Equal Compulsory Process Powers

Linking the foregone conclusion doctrine to search warrants has additional policy benefits, such as the elimination of legal process shopping by the government. Consider the issue of compelled passcode decryption, which is currently being litigated across the county.[280] In these cases, the government has obtained a search warrant to obtain evidence from a digital device but cannot gain access to the device because the passcode on the phone has encrypted the device. Consequently, the government seeks a court order compelling the defendant to decrypt the device so the government can execute the search warrant. If the government had obtained a subpoena for the defendant to turn over incriminating documents, the government would have to satisfy the foregone conclusion doctrine to overcome any Fifth Amendment objection. Thus, if the particularity requirement for speech is broader than the foregone conclusion doctrine, we should expect prosecutors to opt to issue search warrants because it allows them to seize more information.

Some may say that search warrants need to be broader than subpoenas to solve crime. However, such an argument ignores that the defense also has an equally important interest in discovering the truth, yet the defense would not have access to a search warrant. Consider a hypothetical where the defense believes that evidence that an alternate perpetrator of a homicide exists on the Alt Perp's

---

[278] Illinois v. Gates, 462 U.S. 213, 238 (1983).
[279] *See, e.g.*, KY. REV. STAT. ANN. 508.140 (West 2019); *see also* KY. REV. STAT. ANN. 508.130(1)(b)-(2) (West 2019).
[280] *See, e.g.*, In Re Grand Jury Subpoena Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012).

Facebook account, and that the defense has probable cause that such evidence exists on the account. Under current law, the defense attorney would be unable to obtain information from the social media company itself.[281] Although the defense attorney could subpoena the Alt Perp to produce her Facebook records, the Alt Perp could likely raise a valid Fifth Amendment objection to the production of the records to the extent it was not a foregone conclusion that certain evidence existed. But if a search warrant permits greater access than the foregone conclusion doctrine, the government can access more social media records than the defense attorney.

Such a result is untenable. Our Constitution has an amendment restricting the government's ability to obtain evidence and another protecting a criminal defendant's right procure evidence from third parties. If the concept of adversarial justice means anything, then it should not rely upon a prosecutor's discretion on whether to seek a search warrant. Instead, if courts are satisfied that the defense should not be given access to records unless it can meet a certain standard, the government should be held at least to the same standard.

IV. WHEN DOES SCRUPULOUS EXACTITUDE APPLY?

Part III addressed how a search warrant could meet *Stanford*'s scrupulous exactitude requirement. This Part addresses the scope of *Stanford's* application. If the scrupulous exactitude requirement does not apply, the standard rules that govern search warrants should apply. This Part argues that the scrupulous exactitude standard should apply whenever the government seeks to seize a record whose evidentiary purpose is to show that a person acted in a certain manner or believed certain things. An easy, though inexact, shorthand for applying this test is to ask whether the government is seizing content (in which case scrupulous exactitude applies) or metadata (in which case a boilerplate particularity description is sufficient). Whenever the government seeks communicative content, it will almost always attempt to prove that a person acted in a particular manner or holds certain beliefs.

However, upon closer inspection, the shorthand content/metadata distinction is both over-inclusive and under-inclusive concerning certain data. For instance, the Supreme Court has exempted business records from the scrupulous exactitude requirement. Therefore, search warrants for a corporation's books and records can still proceed with a boilerplate particularity description, although they are communicative. Second, there are certain crimes, such as child pornography or fraud, whose very

[281] United States v. Pierce, 785 F.3d 832, 842 (2d Cir. 2015) ("The SCA does not, on its face, permit a defendant to obtain" the contents of communications).

nature do not implicate the free speech concerns in *Stanford*. And last, certain forms of metadata, such as location tracking metadata, may be forms of speech.

Additionally, even when the government is not seizing content, the First Amendment may require the use of independent search executors when the government seeks to search a device that likely contains First Amendment protected material or when the amount of responsive material permeates the device to such a degree that the scrupulous exactitude standard is impractical. In both of these circumstances, I argue that that independent search executors are required to filter the responsive material from the nonresponsive material. Although this will generate criticism that the doctrine forecloses this kind of search protocol, I argue that the nature of First Amendment protections and the need for a solution to the Digital Disclosure Trilemma provide the basis for these independent search executors.

The goals within this Part are more modest than the previous Sections'. The immediate goal is to cabin the scrupulous exactitude/use restriction model to ensure an administrable path for many questions that are outstanding from Part III. Instead of providing comprehensive answers to all of these questions, it aims to show that an answer exists, and invites others to follow up on where this Article ends. Section A explains the basic test to determine when the government is seeking to seize speech. It also explains the basis of the "business records" exception and how to determine what constitutes a business record. Section B explains when independent search executors are required by the First Amendment and why doctrine supports such a requirement.

A. Scrupulous Exactitude Generally Applies to Content

Simply because the government is seeking to seize speech does not mean that the government must particularly describe the speech with scrupulous exactitude. *Stanford* was concerned with the particular threat that vague search warrants could allow too much discretion in their execution or were pretextually issued to suppress speech. If the government had evidence of an active plot of a conspiracy to overthrow the government, a warrant could be issued only if it could describe *ex ante* why the sought speech was part of that plot. This way, citizens would not have to worry about possessing or distributing literature abstractly theorizing about the benefits of overthrowing the government.[282]

However, *Stanford* also recognized that its new standard wouldn't apply in all situations. For instance, when the government

[282] See Section III.A *supra* for discussion of the historical connection between the First and Fourth Amendments.

sought the books because the books were stolen or contraband, the government would not need to describe the books with scrupulous exactitude.[283] Similarly, if the books to be seized involved "a ledger of an unlawful enterprise," they "might stand on a quite different constitutional footing" than the books seized in *Stanford*.[284]

Both of these exceptions deserve individual treatment. Section 1 covers the exception derived from stolen items or contraband. It argues that this exception was created to account for circumstances in which the government is seizing the books for a reason other than to obtain their contents. In those circumstances, a more generic description of the items to be seized is permitted because there is a decreased risk of suppression of speech from a less precise description. Section 2 argues that *Stanford*'s unlawful ledger exception should be understood and an exemption holding that business records are exempt from the scrupulous exactitude standard.

1. Scrupulous Exactitude Does Not Apply Where the Government is Indifferent to Proving a Person's Conformity with the Speech

Often when the government seeks a search warrant for communicative materials, the government will be very interested in the content of the sought speech. The government will want to know what potential suspects said to one another, or the content of communications between a suspect and a victim. In such circumstances, the government will likely be trying to seize speech to prove how someone acted or what that person believes or knows. There are other instances, however, when the government seizes speech and it is indifferent to showing that a person's actions have conformed to the content of the speech. For instance, Michael Price has noted that [i]t is difficult to find a significant First Amendment expressive or associational interest" in medical records "even though many people would consider it highly private information."[285] If *Stanford* is understood as limited to instances in which the government seeks evidence to prove someone's conduct or mental state, then this helps explain why medical records may not be protected under a First Amendment framework. One's medical records rarely, if ever, expose speech about someone's conduct or mental state.[286]

---

[283] Stanford v. Texas, 379 U.S. 476, 485 n. 16 (1965).
[284] *Id*.
[285] Price, *supra* note 19, at 298.
[286] Of course, there are some exceptions. A statement by a person of how they were injured would contain expressive speech. However, if the government knows of an assault and the records custodian of where the victim went to get treatment, obtaining a warrant that complied with scrupulous exactitude, even it applied, would not be difficult.

Similarly, certain crimes could be exempt from scrupulous exactitude's reach entirely. Take child pornography as an example. Although child pornography is not constitutionally protected speech,[287] the Court has found its unconstitutionality is linked to the use of real children.[288] For the Court, the state's interest in preventing child abuse is only implicated if a real (as opposed to a digitally created) child is used to produce the material.[289] Thus, a search warrant to discover child pornography is indifferent to the direction, cinematography, or plot of any child pornographic film or image. Instead, its sole interest is its documentation of underlying abuse. If we were to consider the mere use of a real child in child pornography a speech act (which it may not be),[290] it is hard to see what constitutionally-protected speech is at risk of being suppressed from a search warrant authorizing the seizure of "all child pornography."

Additionally, fraud could be a category of crimes that is exempt from the scrupulous exactitude standard. In *Andresen v. Maryland*,[291] the defendant was suspected of fraudulently conveying land by falsely claiming that property was free of liens.[292] A search warrant on the defendant's corporate offices was issued to search for various financial documents as well as "books, records, documents, papers, memoranda, and correspondence, showing or tending to show a fraudulent intent and/or knowledge elements of the crime of fraudulent pretenses . . . together with other fruits, instrumentalities and evidence of crime at this [time] unknown."[293] Even though the quoted list is strikingly similar to the one in *Stanford*'s invalidated warrant, the Court does not apply the scrupulous exactitude standard to the warrant, despite quoting *Stanford* in the opinion. Justice Brennan's dissent focused solely on the Court's decision to uphold the warrant because, in his view, the "other fruits" clause made the warrant a general warrant.[294] No one thought that First Amendment concerns were at issue in search of business records.

At first blush, one might think that the Court's ruling confined *Stanford* to its facts. However, in *Lo-Ji Sales v. New York*,[295] decided three years after *Andresen*, the Court struck down a warrant to seize two particularly described obscene films and all "similar" films as a

---

[287] New York v. Ferber, 458 U.S. 747 (1982).
[288] Ashcroft v. Free Speech Coalition, 535 U.S. 234, 240 (2002).
[289] *Id.*
[290] For instance, the court my distinguish a child pornographic film as having an erotic message that can be divorced from its use of a real child. *See* Barnes v. Glen Theatre, 501 U.S. 560, 568-71 (1991) (treating nude dancing in this manner).
[291] 427 U.S. 463 (1976).
[292] *Id.* at 465.
[293] *Id.* at 481 n.10.
[294] *Id.* at 492-93 (Brennan, J., dissenting).
[295] 442 U.S. 319 (1979).

general warrant prohibited by *Stanford*.[296] Consequently, all other fruits and instrumentalities of crimes clauses are prohibited when the materials raise First Amendment considerations. The question, then, is why *Andresen* was upheld.

One answer, addressed in Section 2, is that the government sought business records and these records are exempt from the scrupulous exactitude requirement. But another reason is that fraud, as a general matter, may be an exempt crime. When the government seeks to punish the act of fraud, the government is not deterring the speech act of representing a piece of land as clear of all liens. Nor is the government deterring proper record keeping showing that a specific piece of land has liens on them. Instead, the government seeks to punish the concurrence of saying the former while knowing the latter. Because the concerns that gave rise to *Stanford* are not implicated with a search warrant for fraud, the standard generally does not apply.[297] Granted, a search warrant for documents of a plan to commit fraud would implicate the scrupulous exactitude standard. But where the government has probable cause that some evidence of fraud exists on a phone, it is hard to imagine a case where the scope of the warrant could not extend to documentation of a plan to commit fraud.

Similarly, not all records on digital devices will implicate the scrupulous exactitude standard because these types of records do not in themselves contain evidence of someone's thoughts or conduct. Contact lists, call histories, and lists of installed apps are not the kinds of records used to show that someone acted or believes something in conformity with speech. This does not mean that the First Amendment plays no role. For instance, a search warrant for these items would likely raise First Amendment concerns about freedom of association.[298]

For those kinds of search warrants, I suspect, a similar framework to the standard proposed here would be required. As I have articulated, search warrants for speech should specify some combination of participant, content, and timeframe. These factors were used because it was established in case law, and it is a set of criteria that can be reliably used by law enforcement. Similarly, search warrants for someone's associations should probably require a particularity description that relies upon similar functional facts to limit officer discretion on how to segregate data. Because of the innumerable kinds of associations, concerns about the privacy

---

[296] *Id.* at 321, 325.

[297] One important exception of course could be if the government were to seize a search warrant for a *de facto* diary saying of a defendant saying "I want to commit fraud." In that narrow circumstance, *Stanford*'s scrupulous exactitude requirement would be implicated.

[298] The Eighth Circuit started to explore this matter in United States v. Apker, 705 F.2d 293 (8th Cir. 1983).

implications of aggregating associations, and the lack of case law on the intersection between the freedom of association and search warrants, those concerns are beyond the scope of this Article.

Location tracking information, however, raises the question whether some data we typically believe is metadata might constitute protected speech.[299] One could imagine that the signal that a GPS device sends to the receiver is akin to a message saying, "I am here." It seems that "being here" as opposed to "being somewhere else" is attempt to use speech to prove conduct in conformity with the speech. However, because such speech is automatically transmitted without knowledge of the end user, the chilling of such speech is not as obviously present.[300]

On the other hand, perhaps the better metaphor for GPS signals is to analogize them to the symbolic speech on the petitioner's jacket in *Cohen v. California*.[301] It is perhaps the case that once Cohen put on his jacket saying "Fuck the Draft," he was "automatically" transmitting a message without any thought. The decision to turn on a cell phone and connect to a cell-site tower may be akin to putting on clothing expressing symbolic speech. Just as one cannot avoid transmitting location information "[a]part from disconnecting the phone from the network,"[302] we might think *Cohen*'s decision to put on his jacket is akin to an end user deciding to use a cell phone.

The Supreme Court's location tracking cases can to a certain extent be better explained through this free speech lens. Take the case of searches for location information in *United States v. Jones*.[303] There, the federal government installed a GPS device on a car for twenty-eight days and used the information from that tracking device to convict the defendant of narcotics trafficking.[304] The majority opinion concluded that a "search" had occurred because the government trespassed onto Jones's property by installing the GPS device.[305] Justice Alito correctly noted that the majority "largely disregard[ed] . . . the use of a GPS for the purpose of long-term tracking" which is "what is really important," and instead "attache[d] great significance to something that most would view as relatively minor."[306]

Jones, of course, concerned the question of whether a warrant

---

[299] For a scholarly work that considers this question outside of the Fourth Amendment, see Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014).
[300] *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (finding third-party doctrine does not apply to cell-site location information because the end user is unaware of its transmission).
[301] 403 U.S. 15 (1971).
[302] *Carpenter*, 138 S. Ct. at 2220.
[303] 565 U.S. 400 (2000).
[304] *Id.* at 402-04.
[305] *Id.* at 408-09.
[306] United States v. Jones, 565 U.S. 400, 424 (2012) (Alito, J., dissenting).

was required for GPS tracking. The Court never, however, opined on what warrants for GPS tracking should look like. If we believe that GPS tracking raises *Stanford* concerns, then the foregone conclusion doctrine and metadata parameters (persons or objects subject to tracking, for a particular length of time, etc.) can create guidelines for how to best administer those warrants.

This discussion raises an important question: how to determine whether law enforcement seeks a warrant to search for speech to show conformity of conduct or belief to the sought speech, or not. My tentative belief is that courts should use a totality of the circumstances test to make this determination. Courts may look to the probable cause underlying the warrant and the authorized items seized and ask how these items would be used to help prove the existence of a violation of criminal law. Although this test is vague, I generally think administration difficulties will be rare. Giving courts flexibility to issue search warrants will improve their handling of unique situations.

First, the need for the government to state the probable cause that gives rise to the search for particular items demonstrates the anticipated evidentiary purpose. Because the government is required to explain reasons for wanting to seize certain evidence, evaluating the desired evidentiary use should be easy. Put another way, if it is difficult to evaluate the evidentiary use of a particular item, the warrant likely lacks probable cause to obtain that item in the first place.

Second, if there is speech in excess of the boilerplate description, this information would have to be filtered out through the use of an independent search team, elimination of the plain view exception, or a use restriction. Consequently, the probable cause requirement and whatever rule to protect the foregone conclusion floor will jointly protect privacy for speech seized in excess of the warrant.

Third, when it is a close call, the government is also protected by the good-faith exception. If courts rule on the underlying constitutional issue, but uphold the search on the good-faith exception, the law on when someone falls within the scrupulous exactitude standard can still meaningfully develop. Similarly, courts could develop certain presumptions for when *Stanford* applies. For instance, courts might say that literature, text message conversations, emails, and instant messages are presumptively protected by *Stanford* to help guide lower courts.

2. The Business Records Exception

In creating the scrupulous exactitude standard, the Court noted in dicta that "a ledger of an unlawful enterprise thus might stand on a quite different constitutional footing" from the books discussed in

Stanford.[307] However, the opinion lacked a clear rationale. The Court cites *Marron* v. *United States*,[308] but in *Marron*, the Court found a seizure of the ledger and bills of a conspiracy was outside the scope of a search warrant for the premises.[309] Instead, the Court upheld the arrest warrant and the seizure of bills and ledgers that were instrumentalities of the conspiracy that the officers seized incident to a lawful arrest.[310] Consequently, it is curious why the Court relied on a precedent for a warrantless search to affect the law for search warrants. Despite the flimsy doctrinal support for the exception, it is one that lower courts must interpret.

This Section argues that the "unlawful ledger" exception should be understood to create a commercial speech or business records exception. First, as a historical matter, the Court's Fourth Amendment jurisprudence has consistently treated commercial speech as less deserving of Fourth Amendment protection. For instance, despite *Boyd*'s near absolutist protection of papers, that case exempted corporate books and records required to kept by law, counterfeit coins, lottery tickets, and other prohibited gambling implements.[311] Meanwhile, in *United States v. Miller*,[312] the Court found that the Fourth Amendment did not protect someone's financial documents held by a bank. Similarly, the Court in *Smith v. Maryland*[313] found that the use of a pen register to collect phone numbers did not implicate the Fourth Amendment. Consequently, it should not be a surprise that in *California Bankers Association v. Shultz*,[314] the Court found that *Stanford* did apply to mandatory deposit reporting for banks because "the information sought is about commerce, not literature." Most other lower courts that have considered the question of *Stanford*'s applicability to business records have concluded it does not apply.[315]

Second, business records challenge core privacy assumptions that were made in *Stanford*. Recall my argument that the scrupulous exactitude requirement applies to private papers when the government attempts to use those papers to prove the conformity of

---

[307] Stanford v. Texas, 379 U.S. 476, 485 n.16 (1965).
[308] 275 U.S. 192 (1927).
[309] Marron v. United States, 275 U.S. 192, 198 (1927).
[310] *Id.* at 199.
[311] 116 U.S. 616, 623-24 (1886).
[312] 425 U.S. 435, 444-45 (1976).
[313] 442 U.S. 735, 742-46 (1979).
[314] 416 U.S. 21, 62 (1974).
[315] *See, e.g.*, United States v. Stelten, 867 F.2d 446, 450-51 (8th Cir. 1989); United States v. Espinoza, 641 F.2d 153, 164-65 (4th Cir. 1981); United States v. Clough, 246 F. Supp. 2d 84, 87 (2003); State v. Tunnel Citgo Services, 374 A.2d 32, 34-35 (N.J. App. 1977). *But see* Voss v. Bergsgaard, 774 F.2d 402, 405-06 (10th Cir. 1985) (finding scrupulous exactitude applied to warrant where it authorized seizure of "all business records," which included literature criticizing federal tax system).

mind or conduct to the ideas expressed in the papers. When the government attempts to use papers as evidence of criminality in this manner, it threatens the space individuals need to explore ideas.[316] Such space is necessary to prevent individuals from self-censoring their private thoughts.

But business records challenge three assumptions made in *Stanford*. First, when it comes to the financial documents in *California Banker's Association*, *Miller*, or *Smith*'s pen register, it is hard to think of the statements made in these documents in the same way as the literature seized in *Stanford*, which might reveal someone's beliefs or values. Commercial statements do not reflect individuals' beliefs.

Third, determining whether corporate speech is private can be especially tricky. One's work at a corporation is not the same as one's personal records. Instead, it is shared with other people who may or may not leak the documents to the press. Even if it is not left to the press, the individual at issue may not have control over the disclosure of the information. When the person leaves the corporation, that individual typically loses control over what happens to the papers. We might think that bestowing the benefits of incorporation and government regulation necessitates a lessened expectation of privacy in the records. Indeed, stipulating that the foregone conclusion floor is tied between an intersection between *Stanford* and *Fisher*, it is worth noting that it is much more difficult for a records custodian of a corporation to assert a Fifth Amendment privilege for disclosing records under the subpoena.[317]

Of course, basing a lessened degree of particularity upon the corporate form can raise more issues. For instance, as the Court's decision in *Citizens United v. Federal Election Commission*[318] shows, individuals may take the corporate form to amplify their own speech. Whether courts are willing to subcategorize business records remains to be seen. However, the Court's decision in *Carpenter v. United States*[319] to not protect business records with a warrant suggests that a majority of the Court is at least comfortable in distinguishing business records from other forms of data.

Finally, for many kinds of business records, the government has no interest in proving the conformity of mind or conduct to the ideas expressed within the documents. For instance, the government may seek a defendant's medical records in a homicide case to determine whether the defendant's injuries affect whether to or what charge to bring against a defendant based upon a possible self-defense argument. With respect to the doctor's diagnosis of any injury

---

[316] *See supra* note 267 and accompanying text.
[317] *See* Braswell v. United States, 487 U.S. 99 (1988).
[318] 558 U.S. 310 (2010).
[319] 138 S.Ct. 2206, 2221-22 (2018).

sustained, the state is unconcerned with who made the speech or what their particular conclusion was; instead, the government solely seeks to seize the speech to prove that it exists.

A corporate speech exception would have to confront the problem of organized crime, which can operate like a corporation without formally taking the corporate form. For those cases, *Marron*, which concerned an illegal conspiracy violating Prohibition, serves as a basis for finding these organizations records are subject to the business records exception. Although courts could exploit such an exception to deem all group crime rings a business, courts could look to the Racketeer Influenced and Corrupt Organization Act's definition of "enterprise" to determine when group activity rises to level of a corporate entity.[320]

I hesitate to take this analysis further because the questions depend on how one wishes to determine which records constitute business records or are otherwise exempt from the scrupulous exactitude standard. Formalists will likely want to use the reasons noted here to exempt all corporate books and records and create a simple, predictable framework for the Fourth Amendment. For these individuals, if additional protections are warranted, they will invite Congress to provide greater protections. However, as concerns over protecting corporate political speech show, courts may be tempted to opt for a more pragmatic approach to corporate speech. However, like other pragmatic solutions, such an approach creates doctrinal instability as lines are drawn and litigants attempt to stretch or narrow exceptions.

B. The First Amendment May Require Independent Search Teams

As discussed in Section A, there will be cases when the government seeks to search a digital device and will not be required to comply with *Stanford*'s scrupulous exactitude standard. Additionally, there will be times when *Stanford*'s scrupulous exactitude standard cannot meaningfully distinguish between seizeable and nonseizeable speech. These latter cases will most likely occur in continuous course of conduct crimes, where the government has probable cause that responsive files exist throughout the device. In either circumstance, this Section argues that the First Amendment should require the use of independent search teams to filter out the files responsive to the search warrant for case investigators.

First, as a matter of doctrine, the Court has recognized that searches of papers implicate information privacy concerns for speech unrelated to the search warrant. For instance, in *Andresen*,

[320] 18 U.S.C. §1961(4) (2018).

the Court declared that "In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. . . . [R]esponsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy."[321] *Zurcher* also noted that the nature of a newsroom required that "courts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search."[322]

Moreover, in *Nixon v. Administrator General Services*,[323] the Court made clear that such teams would be consistent with the scrupulous exactitude requirement. In that case, former President Nixon challenged new laws that would release government documents to the public. He argued, in pertinent part, that *Stanford* precluded such a search of his papers to determine which documents were government documents and which were personal papers because discretion would be placed in the hands of government archivists. The Court distinguished *Stanford* on several grounds, but also noted that "the screening will be undertaken by Government archivists with, as the District Court noted, an unblemished record for discretion . . . ."[324] Consequently, the Court found that such a screening procedure could be constitutional.[325]

Admittedly, precedent suggesting that the First Amendment *requires* the use of independent search teams is thin. However, the concept would not be unprecedented to protect highly valued speech. For instance, when a search warrant is executed on an attorney's office, taint teams or independent search executors are often used to filter out privileged communications.[326] This would only seek an extension of that rule for First Amendment protected material for the reasons given in *Stanford*.

Second, use of such taint teams may be necessary in order to solve the Digital Disclosure Trilemma. If one is to solve the Digital Disclosure Trilemma without affecting the scope of the government's *Brady* obligations or the manner in which the government searches for evidence, then the only avenue left is to control when the government obtains custody of the relevant files. If the government must utilize an independent search team to filter out files (*Brady* material or child pornography) that would create a Digital Disclosure Trilemma, it becomes harder to argue against

---

[321] Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).
[322] Zurcher v. Stanford Daily, 436 U.S. 547, 565 (1978).
[323] 433 U.S. 425 (1977).
[324] *Id.* at 462 (internal quotation marks and citation omitted).
[325] *Id.* at 463-65.
[326] UNITED STATES ATTORNEY JUSTICE MANUAL § 9-13-420.

such teams from also filtering out the nonresponsive files from the responsive ones.

A more difficult question surrounding *Brady* material arises when the search of a third party's digital device reveals exculpatory evidence that is outside the scope of the warrant. For instance, in one of my homicide cases, a search warrant was executed on the deceased's Facebook profile. Upon disclosure of records from Facebook, it was discovered that the deceased and several people he was with the night he died had planned and carried out several robberies. My client told the police he acted in self-defense. Should the law subordinate the privacy of a third party to prevent an innocent person from being convicted? This is a question of values rather than law.

V. OPERATIONALIZING THE SCRUPULOUS EXACTITUDE REQUIREMENT

As I criticized search protocols in Part II for being persistently unable to overcome the good-faith exception,[327] it is appropriate to make a case for a First Amendment-based model of the Fourth Amendment to survive the good-faith exception. Because my model is based primarily on history and established Fourth Amendment precedent, a First Amendment-based model will have the highest chances of success against the good-faith exception out of any current model to limit search warrants.

Although this Article has discussed several novel theories, such as the double protection of papers, the Digital Disclosure Trilemma, and the Foregone Conclusion Floor, all criminal defendants need is one fact: that the warrant issued in their case is indistinguishable from the warrant issued in *Stanford*. Because *Stanford* is concerned with the particularity requirement, a *Stanford* violation fits within one of the exceptions to the good-faith exception.

Moreover, several recent Supreme Court decisions have buttressed the First Amendment implications of search warrants on digital devices. Cell phones, the Court has noted, store "many distinct types of information" which allow for "[t]he sum of an individual's private life [to] be reconstructed."[328] Further, within the context of social media, the Court has recognized that social media platforms are "the most important place[] for the exchange of views."[329] This observation led the Court to conclude that "the Court must exercise extreme caution before suggesting that the First Amendment provides scant protection for access to vast networks in that medium." Finally, *Carpenter*'s holding that the Fourth

[327] *See supra* Section II.B.
[328] Riley v. California, 573 U.S. 373, 394 (2014).
[329] Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017).

Amendment protects "the privacies of life" while preventing "a too permeating police surveillance" suggests our private conversations are ripe for Fourth Amendment protection.[330]

And while the government will likely protest that *Andresen* created ambiguity as to *Stanford*'s reach, the *Carpenter* decision to exempt corporate books and records from location data should signal a commitment to a distinction for business records.[331] If the government executes a search warrant for (traditional) speech on a digital device, it must distinguish its warrant from the warrant in *Stanford*. Defense attorneys can distinguish several harmful digital particularity cases on the grounds that the First Amendment issues were not raised by prior litigants. And when the government uses cases for the search of effects to digital search warrants for speech, defense attorneys should use *Marcus* and *Stanford* to argue that different particularity rules apply to papers.

Even if courts attempt to chalk up the officer's mistake to ordinary negligence, a *Stanford* violation is very receptive to an attack under widespread and systemic ordinary negligence prong. Unlike unlawful *Terry* stops, which are difficult to document accurately, the legality of the warrant is confined to the warrant itself and the four corners of the incorporated affidavit.[332] If a police department consistently relies on boilerplate particularity descriptions, defense attorneys should be able to collect records to establish a widespread and systemic pattern of negligence. Because the standard for reasonableness under the good-faith exception is the same as for qualified immunity, impact litigators can assist defense attorneys by bringing civil suits and have the more generous civil discovery tools available to them.[333]

Finally, and perhaps most importantly, a First Amendment argument for exclusion of the evidence permits defendants to change the calculus as to whether evidence should be excluded. For a *Stanford* violation, the calculus is not merely whether the cost of suppressing evidence is worth the price of deterring the police. Now, criminal defendants will be able to leverage the collective harms of a First Amendment violation with their Fourth Amendment violation. Of course, arguing a *Stanford* violation to a court will lead a judge to inquire how courts can lawfully issue digital search warrants for speech. That is when the rest of the Article comes into focus.

---

[330] 138 S. Ct. 2206, 2214 (2018) (internal quotation marks and citations omitted).
[331] *Id.* at 2221.
[332] Groh v. Ramirez, 540 U.S. 551, 557-58 (2004) (noting that Fourth Amendment violations are concerned whether a warrant, which can incorporate affidavit by reference, are valid).
[333] *See* Leah Litman, *Remedial Convergence and Collapse*, 106 CALIF. L. REV. 1477, 1492-97 (2018) (documenting the harms caused by this convergence).

CONCLUSION

The scrupulous exactitude model was developed by the Supreme Court in response to concerns that granting officers unbounded discretion creates a risk that the instructions on what to seize will be too vague to ensure the warrant does not chill speech or is pretextually used to suppress speech. To prevent these First Amendment harms, the model requires the magistrate issuing the warrant to decide what forms of speech are relevant to the charges and therefore may be seized. As the Court explained in a different context in *Johnson v. United States*, the Fourth Amendment does not "den[y] law enforcement the support of the usual inferences which reasonable men draw from evidence." However, it "require[s] that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime."[334] This Article has applied this principle to the particularity requirement for search warrants for digital speech.

At the same time, where the government does have the authority to seize a large swath of information, the First Amendment does not disappear due to the government's interest in solving a crime. In those circumstances, the government must employ measures to ensure the screening of responsive or nonresponsive information and only hand off responsive information to investigators. *Wilkes*, *Entick*, and *Stanford* all rejected the seize-first-and-search-later approach because such indiscriminate seizures create societal harms. If the courts will acquiesce to the reasonable overseizure of information to execute a search warrant, courts must preserve First Amendment protections by ensuring that that the government will only get the speech it came for.

[334] 333 U.S. 10, 13-14 (1948).