Harvard Journal of Law & Technology
Volume 24, Number 2 Spring 2011

"REASONABLE" GRAND JURY SUBPOENAS: ASKING FOR INFORMATION IN THE AGE OF BIG DATA

*Joshua Gruenspecht**

TABLE OF CONTENTS

I. INTRODUCTION

Grand juries use the subpoena duces tecum to request and collect evidence held by a party or witness. In so doing, they serve as an investigative arm of the prosecution.[1] Though subpoenas, unlike war-

* J.D., Harvard Law School; B.S, Computer Science and English, Yale University. I would like to thank Jim Dempsey for his expert guidance through the world of third-party subpoenas and Richard Salgado for his invaluable advice, as well as Abby Lauer, Craig Kitchen, and the editors and staff of the *Harvard Journal of Law & Technology* for their helpful suggestions and editing prowess.

1. "[T]he attorney for the government ordinarily 'fills in the blanks' on a grand jury subpoena and arranges the case to be presented to the grand jury." Charles Doyle, *The Federal Grand Jury*, *in* THE FEDERAL GRAND JURY 1, 10 (Lyn Farrel ed., 2002). In fact, some subpoenas duces tecum permit the witness to present documents directly to the government attorney rather than the grand jury. *See, e.g.*, B & J Peanut Co. v. United States (*In re* Grand Jury Proceedings), 887 F. Supp. 288, 291 (M.D. Ga. 1995) (noting that "[i]n lieu of an appearance before the Grand Jury at this time, this subpoena may be complied with by" mailing the U.S. Attorney the evidence directly).

rants, can be issued with less than probable cause,[2] they receive less attention from commentators because subpoenas do not result in the state's exercise of its powers to search a suspect's property without his consent. Instead, they are used to request documents and information that the prosecution suspects will be material in the case. The advent of mass digital storage, however, has significantly increased the chances that records of any given document exist and is increasingly unifying the locations in which those records can be found. Both in the case of digital data stores held by users themselves and in the case of data stored by users with third parties, the extent of the subpoena power increasingly rests on the question of how specific a prosecutorial request for documents must be.

Faced with increasing amounts of stored digital information, courts and commentators have attempted to apply old rules in a new context. The knotty Fourth Amendment questions that arise from the production of electronically stored information through warrants have received particular scrutiny.[3] Civil liberties groups have argued that the Constitution demands a probable cause standard for various kinds of digital searches by law enforcement,[4] while public interest and industry coalitions have pushed for legislation to address the issue.[5] While standards for the use of warrants for the collection of evidence have been the subject of judicial conflict, scholarly debate, and public outcry, standards for the use of the grand jury subpoena have slipped by relatively unnoticed. Given the potential scope of digital subpoenas, this is surprising. As one commentator has noted, "[w]hereas the subpoena power is fairly narrow in traditional cases, in computer crime cases it is incredibly broad."[6]

The inexpensiveness of digital storage, the increasing ubiquity of computing, and the growth of the type and number of digital sensors associated with devices of all shapes and sizes means that more data is retained in more hands than ever before. In a world of physical documents, use of the subpoena power was cabined by the investigator's reasonable suspicion of the existence of a given document or commu-

2. *See* United States v. R. Enters., 498 U.S. 292, 297 (1991).

3. *See generally* City of Ontario v. Quon, 130 S. Ct. 2619 (2010); United States v. Warshak, 631 F.3d 266 (6th Cir. 2010); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010) [hereinafter Kerr, *Applying the Fourth Amendment to the Internet*].

4. *See, e.g.*, Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Appellee at 21–24, *Warshak*, 490 F.3d 455 (No. 06-4092) (arguing for a probable cause standard in searches of stored email).

5. Most prominently, the Digital Due Process coalition has pulled together a set of principles for reforming the existing standards for searches of stored digital data. *See* DIGITAL DUE PROCESS, http://www.digitalddueprocess.org (last visited May 6, 2011).

6. Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 296 (2005).

nication.[7] An overbroad request from the prosecution to subpoena an entire file cabinet might trigger special judicial scrutiny on a category-by-category basis of the relevance of each category of file therein before production.[8] Now, however, innumerable communications records are created, and few are deleted. Often, neither the document creator nor the prosecution knows precisely what records might exist: because of the networking of digital storage, third parties are now significantly more likely to possess digital data, such as personal communications and stored documents, created by others. Today's digital "file cabinets" are significantly larger and easier to locate than their physical equivalents. The privacy problem presented is clear: "searching [electronic storage] in a comprehensive way can expose both crimes and embarrassing private information that can be admissible in court under the plain view exception."[9] While the civil law, faced with an avalanche of stored information, has started to lay down ground rules for data production, only a few criminal cases have begun to grapple with the production of electronically stored information in response to subpoenas.

This Note discusses the limited constitutional and statutory bounds on the scope of grand jury subpoenas and argues that the increasing use of digital storage technologies challenges even those limited boundaries on the production of subpoenaed data. Part II describes the current constitutional and statutory law, which defines the scope of acceptable grand jury subpoenas duces tecum, and discusses the tests courts use to determine whether that scope has been exceeded. Part III discusses how modern digital storage complicates the application of those tests. Part IV examines the few criminal cases that have applied the tests to electronically stored information. Part V evaluates potential solutions to the mass digital storage problem, including negotiated production of data, court-specified methods of determination of relevant data, the use of independent third parties to determine relevance for the grand jury, and legislative intervention to address notice requirements for subpoenaing data stored with third parties. Part VI concludes.

II. CONSTITUTIONAL AND STATUTORY BOUNDS ON THE GRAND JURY SUBPOENA

The Fourth Amendment requires that all searches and seizures of private documents by the government be reasonable: "Because a sub-

7. *See R. Enters.*, 498 U.S. at 299 ("Grand juries are not licensed to engage in arbitrary fishing expeditions . . . .").

8. *See In re* Horowitz, 482 F.2d 72, 79 (2d Cir. 1973).

9. Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1255 (2010) [hereinafter Kerr, *Ex Ante Regulation of Computer Search and Seizure*].

poena duces tecum leads to 'the *compulsory* production of private papers,' a person served with a subpoena duces tecum is entitled to the Fourth Amendment's protection against unreasonableness."[10] Unlike the issuance of a warrant, however, which allows law enforcement to search and seize property immediately, the issuance of a subpoena "commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands."[11] The additional level of constitutional protection afforded by the probable cause standard for warrants is not necessary for subpoenas because the judicial process that precedes production should ensure that the constitutional reasonableness standard is met.

Because the requirements of constitutional reasonableness are somewhat vague in the subpoena context, they have over time been conflated with the statutory standards of acceptability laid out in the Federal Rules of Criminal Procedure ("FRCrP"). The Supreme Court has suggested that, at most, the constitutional standard guards against indefinite descriptions of the documents to be produced.[12] To determine what makes a description indefinite, however, the Court turned to FRCrP 17,[13] which states that "the court may quash or modify the subpoena if compliance would be unreasonable or oppressive."[14] Most courts that have explicitly considered the issue have agreed that the constitutional and statutory tests of reasonableness coincide.[15]

---

10. United States v. Bailey (*In re* Subpoena Duces Tecum), 228 F.3d 341, 347 (4th Cir. 2000) (quoting Hale v. Henkel, 201 U.S. 43, 76 (1906)).

11. *Id.* at 348 (citing See v. City of Seattle, 387 U.S. 541, 544–45 (1967); Oklahoma Press Publ'g Co. v. Walling, 327 U.S. 186, 217 (1946)).

12. *Oklahoma Press Publ'g Co.*, 327 U.S. at 208 ("[T]he Fourth [Amendment], if applicable, at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant. The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable.").

13. *See* United States v. R. Enters., 498 U.S. 292, 299 (1991) ("[T]he focus of our inquiry [into reasonableness of a subpoena] is the limit imposed on a grand jury by Federal Rule of Criminal Procedure 17(c) . . . .").

14. FED. R. CRIM. P. 17(c)(2).

15. *See In re* Grand Jury Proceedings, 707 F. Supp. 1207, 1216 (D. Haw. 1989) (describing the test laid out in the text as having been adopted by "certain courts" to "determine whether the prerequisites of the Fourth Amendment and Rule 17(c) have been satisfied") (citing *In re* Grand Jury Investigation, 459 F. Supp. 1335, 1341 (E.D. Pa. 1978); *In re* Rabbinical Seminary Netzach Israel Ramailis, 450 F. Supp. 1078, 1084 (E.D.N.Y. 1978)); *see also In re* Berry, 521 F.2d 179, 181 (10th Cir. 1975) (stating that Rule 17 reasonableness challenges to subpoenas are a vehicle for Fourth Amendment reasonableness challenges); *In re* Grand Jury Subpoenas Served Feb. 27, 1984, 599 F. Supp. 1006, 1018–19 (D. Wash. 1984) (finding the test under both to be the same form of "reasonableness"). Some courts, however, state that actions reasonable under the Fourth Amendment can still be ruled unreasonable under Rule 17: "Rule 17(c) gives the court authority to quash or modify subpoenas in addition to that provided by the fourth amendment [sic] when enforcement would be unreasonable or oppressive." Danbom v. United States (*In re* Grand Jury Proceedings: Subpoenas Duces Tecum), 827 F.2d 301, 305 (8th Cir. 1987). Others state the converse, saying that Fourth Amendment reasonableness goes beyond the protections offered by Rule 17:

The most widely accepted test for reasonableness asks whether the materials requested are relevant to the investigation, whether the subpoena specifies the materials to be produced with reasonable particularity, and whether the subpoena commands production of materials covering only a reasonable period of time.[16] Hence, for purposes of both the Fourth Amendment and FRCrP 17, the "unreasonable or oppressive" test breaks down into relevance, particularity, and unreasonable temporal scope.[17] In addition, many courts recognize a fourth "undue burden" test.[18]

There are therefore four prongs to the test determining whether a grand jury subpoena duces tecum will be considered unreasonable and should be quashed. The first is relevance: does it request some set of items which are relevant to the investigation? The second is particularity: is the ratio of relevant to irrelevant items that are likely to turn up high enough to justify production? The third is scope: are the items requested from an appropriately defined period of time? The fourth and final prong is undue burden: will the process of complying with the subpoena incur the undue expenditure of resources by the recipient? The next Part explains how digital storage complicates the process of applying the first two prongs, relevance and particularity.

"Beyond the explicit strictures of Fed.R.Crim.P. [sic] 17(c), the Constitution guards against abusive subpoenas duces tecum. 'The Fourth Amendment provides protection against a grand jury subpoena duces tecum too sweeping in its terms to be regarded as reasonable.'" United States v. Doe 819 (*In re* Grand Jury Subpoena: Subpoena Duces Tecum), 829 F.2d 1291, 1297 (4th Cir. 1987) (quoting United States v. Dionisio, 410 U.S. 1, 11 (1973)). Professors Bellia and Freiwald have argued that failure to meet a Fourth Amendment reasonableness standard should be considered a separate inquiry, especially in the case of subpoenas for email stored with a third party, but the courts have yet to adopt this interpretation of the case law. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored Email*, 2008 U. CHI. LEGAL F. 121, 141–169.

16. *See In re* Grand Jury Matters, 751 F.2d 13, 18 (1st Cir. 1984); *see, e.g.*, United States v. Alewelt, 532 F.2d 1165, 1168 (7th Cir. 1976); United States v. Gurule, 437 F.2d 239, 241 (10th Cir. 1970). Some note that while this test is the general rule, the questions it entails "are not necessarily the only questions a judge may ever ask in the exercise of his rule 17(c) supervisory power." *In re Grand Jury Matters*, 751 F.2d at 18.

17. *See* U.S. DEP'T OF JUSTICE, *Grand Jury Manual*: *Chapter 3, Part I*, http://www.justice.gov/atr/public/guidelines/206696.htm (last visited May 6, 2011) (laying out each of these three concerns separately).

18. *See, e.g.*, *In re* Special, Sept. 1983, Grand Jury, 608 F. Supp. 538, 542–43 (S.D. Ind. 1985) (noting that the Seventh Circuit adopts the test discussed in the text accompanying note 16, *supra*, and adding that "the federal . . . criminal procedure rules authorize courts to quash or modify subpoenas duces tecum which are overbroad or oppressive"). Some courts consider this part of the reasonableness test for overbreadth under the Fourth Amendment as well: "the scope of a subpoena, if not relevant to a legitimate investigation, and overly broad and oppressive, can support a claim of unconstitutionality under the Fourth Amendment." United States v. Bailey (*In re* Subpoena Duces Tecum), 228 F.3d 341, 350 (4th Cir. 2000). "Such challenges overlap with overbreadth challenges. . . . Analytically, however, oppressiveness represents a distinct concern (i.e., the expenditure of resources necessary in order to comply is unduly burdensome)." HOWARD W. GOLDSTEIN, GRAND JURY PRACTICE § 5.04[1][c], at 5-30–5-30.1 (2010).

III. WHY "BIG DATA" IN LOCAL AND THIRD-PARTY STORAGE CHALLENGES THE REASONABLENESS STANDARD

The last twenty years have seen a tremendous surge in the use of digital storage and a corresponding drop in the price.[19] These trends have changed local data storage in three ways. First, it has practically eliminated the requirement that users clean out their email inboxes and Internet browsing history periodically in order to free up storage and keep their computers operational. Second, it has increased the incentive to design software that stores metadata — data about data — which includes information about when documents, programs, and websites are viewed and how they are used.[20] Metadata can improve software performance by helping to predict what data users will want. Third, it has made redundant backup storage common as a hedge against data loss. As a consequence, many computers possess an unbroken record of all of their users' digital documents and online activity stretching back to the first time the user switched on the machine.

At the same time, companies and individuals possess more devices that capture more data in more categories. Where a user once had only a single desktop computer, today that user might have a laptop, a smartphone, a tablet, an e-reader, and a networked entertainment center. Collectively, those devices may maintain records on everything from the phone calls that user makes to the places that user visits.[21] In a corporate environment, an entire internal network of related devices may be exchanging this stored information for both data processing and archival reasons. Because of the sheer amount of data retained and the portability of such devices, any individual data store is increasingly likely to be relevant to a given investigation.

The increasing speed of network connections has also made possible the consolidation of computing resources and associated digital

---

19. The price per megabyte of magnetic hard drive storage space fell from $ 9.00 CAD in 1990 to between $ 0.01 and $ 0.02 CAD in 2000 to between $ 0.00006 and $ 0.0001 CAD in 2010. *See Cost of Hard Drive Storage Space*, NOVA SCOTIA'S ELECTRIC GLEANER, http://ns1758.ca/winch/winchest.html (last visited May 6, 2011).

20. For example, Microsoft Office documents have long contained "a rich history of hidden information" about their authors and revision history. Donna Payne, *Control Metadata in Your Legal Documents*, MICROSOFT OFFICE, http://office.microsoft.com/en-us/word-help/control-metadata-in-your-legal-documents-HA001140034.aspx (last visited May 6, 2011). Modern extensible data formats allow arbitrary additional data to be included. *See* Frank Rice, *Introducing the Office (2007) Open XML File Formats*, MSDN, http://msdn.microsoft.com/en-us/library/aa338205%28v=office.12%29.aspx (last visited May 6, 2011).

21. A user's cell phone service provider, for example, keeps a record of the cellular towers that have "seen" that user's phone in the past. Taken chronologically, this can provide a history of when users have first visited a given subway station, highway, or city block. *See* Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES, Mar. 26, 2011, at A1, *available at* http://www.nytimes.com/2011/03/26/business/media/26privacy.html (describing this process).

stores — a transition popularly known as the move to "cloud computing."[22] When combined with the rapidly declining price of storage and the economies of scale gained from consolidating both storage and processing, the increase in network speed made it economically advantageous to store information in remote, massive data centers.[23] While copies may remain in local data stores for offline use, online storage of data with third parties is increasingly popular for Internet-based services. Corporations are outsourcing large parts of their internal computing operations to third parties, and the market for such services is expected to more than double between 2009 and 2014.[24] Non-traditional devices are also leveraging remote storage of personal data to provide new Internet-based services.[25]

This ongoing consolidation of potentially relevant data into massive digital stores, both locally and with third parties, is a boon to criminal investigation, but it raises the danger that a grand jury will engage in "arbitrary fishing expeditions."[26] In particular, the availability of "big data" exposes the hidden stresses between the relevance and particularity prongs of the test for the reasonableness of a subpoena. A data store that contains a user's complete location history will undoubtedly be relevant in establishing his whereabouts at the time of a crime. One that contains all of a corporation's recorded communications for the last several years may well establish its relationship with a suspect. As the available relevant data grows, the available irrelevant data grows at least as fast. As a result, the particularity requirement becomes more difficult to satisfy.

---

22. "Cloud computing" is a much-disputed term. *See* Geoffrey A. Fowler & Ben Worthen, *The Internet Industry Is on a Cloud — Whatever That May Mean*, THE WALL ST. J., March 26, 2009, http://online.wsj.com/article/SB123802623665542725.html ("While almost everybody in the tech industry seems to have a cloud-themed project, few agree on the term's definition."). The definition offered in the text gives a quick overview of a complex subject.

23. For an early analysis of the legal implications of the move to cloud computing, see Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83 (2005), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=916046.

24. *See* Rachael King, *Flextronics, Siemens Lead 'Big Shift' to Cloud Computing*, BUSINESSWEEK, Dec. 6, 2010, http://www.businessweek.com/technology/content/dec2010/tc2010126_395358.htm (describing the expected growth in the market for outsourced services to $ 148.8 billion in 2014 from $ 58.6 billion in 2009).

25. *See* Matthew L. Wald, *'Smart' Electric Utility Meters, Intended to Create Savings, Instead Prompt Revolt*, N.Y. TIMES, Dec. 14, 2009, at A14, *available at* http://www.nytimes.com/2009/12/14/us/14meters.html (discussing meters that report minute-by-minute power consumption to utilities); Eric A. Taub, *It's a Smart Kitchen*, GADGETWISE BLOG (Jan. 6, 2011, 3:55 PM), http://gadgetwise.blogs.nytimes.com/2011/01/06/its-a-smart-kitchen/ (discussing kitchen appliances that store usage information with service providers).

26. *See* United States v. R. Enters., 498 U.S. 292, 299 (1991). For an example of a similar fishing expedition in the civil context, see Thompson v. Jiffy Lube Int'l, Inc., No. 05-1203-WEB, 2006 WL 1174040, at *3 (D. Kan. May 1, 2006) ("On its face, a [civil discovery] request for the production of *all* corporate and employee email dating back to 1997 is overly broad.").

Consider an analogy to finding a needle in a haystack, where the needle is a piece of evidence. A relevance test requires that the grand jury describe the needle, whereas a particularity test requires that the grand jury explain how it expects the subpoenaed party to extract the needle without disturbing too much hay. In a "big data" world, where the stacks expand and the needles multiply, relevance does not become harder to satisfy — if anything, it becomes easier, given the appearance of additional needles. Particularity, however, becomes more difficult, because sifting through the stack for any specified needle requires disturbing progressively larger amounts of hay. The problem for courts is how to strike the appropriate balance between the demands of each prong.

In the increasingly common cloud computing environment, courts will also have to perform this balancing between finding evidence and preventing overbroad subpoenas, without an adversarial process to help guide their decision-making. The Stored Communications Act ("SCA"), which governs the prosecutorial acquisition of digital communications data stored with third parties,[27] allows a grand jury to compel a third party to turn over certain contents of a user's data store to an investigator.[28] An SCA subpoena for data does not necessarily provide the creator of the data the opportunity to dispute its acquisition in court. The SCA requires notice to the creator of the data upon execution of the subpoena,[29] but that notice can be delayed indefinitely with the "written certification of a supervisory official."[30] Given that the rationale for the lower standard for compelling access to private data by subpoena is the intermediate step of the court process, the absence of the most obvious adversary to the potential data acquisition at the proceeding is troubling. A third-party subpoena recipient rarely disputes the request, or even the delay of notice.[31]

---

27. 18 U.S.C. §§ 2701–11 (2006 & Supp. III 2009). For a description of how the SCA reflects older technological assumptions, see James X. Dempsey, *Digital Search & Seizure: Standards for Government Access to Communications and Associated Data*, *in* 2 TENTH ANNUAL INSTITUTE ON PRIVACY AND DATA SECURITY LAW 687, 707 (PLI Patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Ser. No. 19129, 2009).

28. 18 U.S.C. § 2703(b)(1)(B)(i). Importantly, courts and commentators have noted the questionable constitutionality of the use of the SCA to subpoena the contents of communications. *See* United States v. Warshak, 631 F.3d 266, 285–88 (6th Cir. 2010); Kerr, *Applying the Fourth Amendment to the Internet*, *supra* note 3, at 1017; *see also* Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. F. 10, 11–12 (2005). Note, however, that certain kinds of business records, such as bank records, do not carry a constitutional expectation of privacy. *See* United States v. Miller, 425 U.S. 435, 443 (1976).

29. 18 U.S.C. § 2703(b)(1)(B).

30. *See* 18 U.S.C. § 2705(a)(1)(B), (a)(4) (2006). The certification must be re-entered every ninety days. *Id.* § 2705(a)(4). Such lack of notice is constitutionally permissible. SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984).

31. When it does refuse, that dispute is newsworthy. *See, e.g.*, Scott Shane & John F. Burns, *U.S. Subpoenas Twitter over Wikileaks Supporters*, N.Y. TIMES, Jan. 9, 2011, at A1, *available at* http://www.nytimes.com/2011/01/09/world/09wiki.html (noting Twitter's resistance to a court order asking for customer information).

The problems with subpoenas to cloud computing data service providers go beyond the service providers' lack of interest in disputing governmental requests. Under existing law, the absence of notice to the creator of the data does not make a subpoena unreasonable because of the third-party doctrine, which states that data disclosed to a third party in the ordinary course of business can be subpoenaed without notice.[32] However, the type of data held by third parties in the cases that developed this doctrine was "business records"[33]: data whose content is *shared* with the holding party. In contrast, cloud computing data is merely *stored* with a third party. There is generally no expectation that the third party or its employees have access to the content of the data as part of their provision of services.[34] Thus cloud computing data holders, unlike traditional business records holders, may not be in a position to address the questions of relevance and particularity, since they do not know what information they possess. Even a data holder willing to dispute a subpoena may not have sufficient knowledge to argue against its unreasonableness. Given these distinctions, in the absence of notice to the creator, there should be an extra burden on the court to ensure the reasonableness of the request.

IV. THE CASE LAW ON REQUESTING ACCESS TO DIGITALLY STORED DATA BY SUBPOENA

Relatively few federal court cases have addressed the reasonableness of criminal subpoenas of digital data.[35] In cases where witnesses are subpoenaed for data on their own devices, this may be because "companies [and other parties] do not wish their first significant inter-

32. *See Miller*, 425 U.S. at 443 n.5.

33. *See, e.g.*, *id.* at 440–41.

34. Some cloud computing services allow for automated analysis of content to create advertising "targeted to the content of information stored on [their] Services." *See Google Terms of Service*, GOOGLE, http://www.google.com/accounts/TOS (last visited May 6, 2011). This is distinguishable from the traditional business records data sharing scenario in two ways. First, the content is scanned not as an integral part of the provision of the cloud computing services, but to provide financial support for the provision of those services. *See id.* Second, permission is granted only for automated scans, not for human examination of the content, and thus content is not shared with any entity capable of making an informed defense against a subpoena. *See Google Privacy Center: Advertising and Privacy*, GOOGLE, http://www.google.com/privacy_ads.html (last visited May 6, 2011) ("The whole process is automated and involves no humans matching ads to Gmail content.").

35. The unreasonableness and overbreadth of civil subpoenas has been more widely discussed in the academic community. *See infra* Part V.A. This is unsurprising, given the contentious issue of electronic discovery. *See* Henry S. Noyes, *Good Cause Is Bad Medicine for the New E-Discovery Rules*, 21 HARV. J.L. & TECH. 49, 50–53 (2007) (describing the Rules Advisory Committee's efforts to establish guidelines for electronic discovery); Mark Herrmann et al., Debate, *Plausible Denial: Should Congress Overrule* Twombly *and* Iqbal*?*, 158 U. PA. L. REV. PENNUMBRA 141, 144, 158 (2009), http://www.pennumbra.com/debates/debate.php?did=24 (discussing how those efforts have failed to simplify electronic discovery in the eyes of trial lawyers).

action with the criminal prosecutor to be a motion to quash the subpoena."[36] In cases where third parties are issued a subpoena under the SCA, this may simply be because there is little motivation to dispute the production. The few cases addressing this issue have recognized the centrality of relevance and particularity, but have differed in the ways in which they balance the two.

The earliest federal case on digital subpoenas is *In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993* (*In re Grand Jury Subpoena 1993*),[37] from the Southern District of New York, in which a grand jury subpoena demanded data created by senior officials at "Corporation X," as well as the central processing units, hard drives, and floppy disks associated with corporate computers used by those officials. The court quashed the subpoena as unreasonably broad, stating that the correct way to balance relevance and particularity was to consider relevance at the level of categories of materials.[38] In particular, it stated that documents, rather than storage media, was the appropriate category of materials to which to address a subpoena.[39] Targeting hard drives, the court reasoned, would be like targeting file cabinets rather than files, and would necessarily produce irrelevant documents.[40] In the case at hand, where the subpoena requested all documents on a drive, the court suggested that a search procedure for distinguishing relevant and irrelevant documents could cure the subpoena.[41]

Several years later, in *United States v. Vilar*, an opinion from the same district downplayed the dangers of insufficiently particular subpoenas.[42] In *Vilar*, a subpoena requested:

> Computers, hard drives, and any other devices or equipments [sic] capable of storing data or text in any format, including but not limited to cellular telephones, personal digital assistants, and any other storage media capable of containing data or text in magnetic, electronic, optical, digital, analog, or any

36. Daniel R. Margolis et al., *When Responding to a Criminal Subpoena Turns Electronic*, N.Y. L.J., March 22, 2010, at S2.

37. 846 F. Supp. 11 (S.D.N.Y. 1994).

38. *Id.* at 13–14.

39. *Id.* at 13.

40. *Id.* at 12–13 (citing *In re* Horowitz, 482 F.2d 72, 79 (2d Cir. 1973)).

41. *Id.* at 13 ("It follows that a subpoena demanding documents containing specified key words would identify relevant documents without requiring the production of irrelevant documents. To the extent the grand jury has reason to suspect that subpoenaed documents are being withheld, a court-appointed expert could search the hard drives and floppy disks.").

42. No. S305CR621KMK, 2007 WL 1075041, at *48 (S.D.N.Y. Apr. 4, 2007).

> other format, used to store information described above . . . .[43]

The information described above included "all corporate records of the [shell companies in question]."[44] The *Vilar* court found that "[u]nlike the subpoena in *In re Grand Jury Subpoena 1993*, . . . the subpoena here specifies, albeit broadly, the information that is sought. . . . [I]n the less stringent context of a subpoena [as compared to a warrant], it adequately restricts the production to relevant documents."[45] The *Vilar* court thus implicitly questioned the analogy of data stores to file cabinets: as long as a digital store contains some piece of relevant information, the prosecution can demand the production of the entire store.

In *In re Amato*,[46] the District Court of Maine took an opposite position, emphasizing the importance of particularity.[47] The subpoena at issue requested, among other things, "[a]ny computer equipment and storage device capable of being used to commit, further, or store documents or data described [in the subpoena]."[48] The court, looking to *In re Grand Jury Subpoena 1993* for guidance, found that requesting all devices "capable of being used" for data storage was, by definition, overbroad under the Fourth Amendment, citing to a number of search warrant cases.[49] Ultimately, the *Amato* court concluded that a subpoena that "requests the turnover of all computers (and related objects) . . . with no express safeguard against a subsequent rummaging through, and seizure of, irrelevant as well as relevant data . . . cannot withstand Fourth Amendment reasonableness scrutiny."[50] This

---

43. Defendant Alberto Vilar's Memorandum in Further Support of Motions (1) To Suppress Evidence Seized from Amerindo US, (2) To Suppress Evidence Seized from the United Kingdom, and (3) To Quash the Subpoena Served on Amerindo US at 50, *Vilar*, 2007 WL 1075041 (No. S305CR621KMK), 2006 WL 4793063 (omission in original).

44. *Vilar*, 2007 WL 1075041, at *46. More specifically, it included "all corporate records of the Amerindo entities, 'including but not limited to' several categories . . . . [including] documents 'concerning the formation of each of the . . . Amerindo entities,' as well as documents listing the 'principles, officers, directors and employees' of the Amerindo entities, and documents reflecting 'changes in ownership, bylaws, [and] resolutions.'" *Id.* (second alteration and second omission in original).

45. *Id.* at *50.

46. No. 05-MC-29PDMC, 2005 WL 1429743 (D. Me. June 17, 2005).

47. The court used the term "overbreadth" as a substitute for a combination of particularity and overbroad temporal scope, but then clarified in a footnote that its objections were based only on the former. *Id.* at *11 n.16. The court also recognized that this was a question distinct from a relevance analysis: "In a footnote, Dr. Amato raises what might be construed as a challenge to the relevance of the Amato P.C. records. . . . I perceive no relevance problem in the request for records of the New York-based corporation." *Id.* at *10 n.15.

48. *Id.* at *3–4.

49. *Id.* at *11. The overbreadth analysis for searches and for subpoenas, the court said, should be identical: "I discern no reason why, for purposes of overbreadth analysis, the off-site search of computer equipment obtained as a result of a subpoena should be treated differently from the off-site search of equipment seized pursuant to a search warrant." *Id.*

50. *Id.* at *12.

goes further than *In re Grand Jury Subpoena 1993* on particularity, suggesting the reasonableness standard is met only by subpoenas that explain how relevant data will be distinguished from irrelevant data.

Most recently, the Ninth Circuit decided *United States v. Comprehensive Drug Testing, Inc.* (*CDT*).[51] In the first version of its en banc opinion, the court stated its desire to "take the opportunity to guide our district and magistrate judges in the proper administration of search warrants and grand jury subpoenas for electronically stored information."[52] While a later revised version moved the advisory part of the opinion into a concurrence,[53] the revised per curiam majority opinion pointedly retained a conclusion noting "the reality that overseizing is an inherent part of the electronic search process" and calling "for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures."[54]

Federal courts have not yet addressed the relevance and particularity requirements for third-party subpoenas of large amounts of data in the context of the SCA. As the use of cloud computing has grown, however, the appropriate legal process for third-party stored data has become a contentious issue. The Sixth Circuit recently struck down the SCA insofar as it permits access to personal communications without a warrant.[55] The Third Circuit recently read the SCA to allow a magistrate judge to require a showing of more than specific and articulable facts in order to grant a court order for stored location data, in part due to "the possibility that such disclosure would implicate the Fourth Amendment."[56] Subpoena standards will likely follow. As the Ninth Circuit has noted, "[s]eizure of, for example, Google's email servers to look for a few incriminating messages could jeopardize the privacy of millions."[57] This is just as true of subpoenas as seizures.

---

51. 621 F.3d 1162 (9th Cir. 2010) (en banc).

52. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 994 (9th Cir. 2009) (en banc), *amended by* 621 F.3d 1162 (9th Cir. 2010) (en banc). Even the unamended version of *CDT* offered little specific guidance on the subpoena side other than directing courts to ask for more investigative history as part of any subpoena request. *See id.* at 1006 ("Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.").

53. *CDT*, 621 F.3d at 1178 (Kozinski, J., concurring).

54. *Id.* at 1177 (per curiam).

55. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010). The Eleventh Circuit, in *Rehberg v. Paulk*, 598 F.3d 1268 (11th Cir. 2010), *vacated*, 611 F.3d 828 (11th Cir. 2010), *cert. granted*, No. 10-788, 2011 WL 940891 (U.S. Mar. 21, 2011), had suggested that email stored with third parties was not subject to the protection of the Fourth Amendment, but it subsequently vacated that opinion and replaced it with one which did not decide the question.

56. *In re* United States, 620 F.3d 304, 317 (3d Cir. 2010).

57. *CDT*, 621 F.3d at 1176.

V. POSSIBLE WAYS TO BALANCE JUDICIAL OVERSIGHT AND LAW ENFORCEMENT NEEDS

It is clear that the federal courts have seen the "big data" problem in the subpoena context but have not settled on a means of addressing it.[58] Though the few district courts to address the issue have considered a number of solutions, including using technological tools,[59] employing intermediaries,[60] and demanding ex ante search procedure descriptions,[61] the appropriate balance between relevance and particularity has yet to be struck. This Part considers some of the alternative solutions to this balancing problem.

A. Restrict or Eliminate the Plain View Doctrine in Digital Search Cases

Restricting or eliminating the plain view doctrine, which allows a law enforcement official to seize and search evidence found in plain view during a lawful observation,[62] would avoid the balancing problem entirely and instead directly address the harms caused by insufficient particularity. In the warrant context, Professor Orin Kerr has suggested this approach as the best means of addressing privacy concerns.[63] Kerr lays out a range of options for narrowing the doctrine, ultimately concluding that complete elimination in the digital search context might be the best option.[64] He admits that elimination of the doctrine would be "severe," and does not advocate immediate aboli-

58. State courts have only addressed the relevant issues in a hybrid First Amendment context. The Pennsylvania Supreme Court, in quashing a subpoena issued to a local newspaper, held that "any direct and compelled transfer to the executive branch of general-use media computer hardware should be pursuant to a due and proper warrant, issued upon probable cause." *In re* Twenty-Fourth Statewide Investigating Grand Jury, 907 A.2d 505, 514 (Pa. 2006). The court noted the special nature of digital storage in its analysis. *See id.* ("The extraction by the executive branch of entire 'filing cabinets' . . . tests the limits of credulity in the attempt to maintain the understanding that no search or seizure is involved."). However, it also noted that there were special First Amendment concerns. *Id.* ("This case . . . . involves production from the news media, which heightens the potential First Amendment concerns."); *see also* Thayer v. Chiczewski, 257 F.R.D. 466, 471 (N.D. Ill. 2009) (holding that a videographer involved in war protests was not required to turn over all of his media storage under Federal Rule of Civil Procedure 45).

59. *In re Grand Jury Subpoena 1993*, 846 F. Supp. 11, 13 (S.D.N.Y. 1994).

60. *Id.*

61. *In re* Amato, No. 05-MC-29PDMC, 2005 WL 1429743, at *12 (D. Me. June 17, 2005).

62 *See* Minnesota v. Dickerson, 508 U.S. 366, 369 (1991).

63. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 576–84 (2005) [hereinafter Kerr, *Searches and Seizures in a Digital World*].

64. *Id.* Other commentators have suggested additional alternatives for narrowing without elimination. *See* Andrew Vahid Moshirnia, Note, *Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain*, 23 HARV. J.L. & TECH. 609, 622–33 (2010).

tion.[65] However, Kerr finds elimination preferable to ex ante narrowing of search warrants by judges, which he has argued is both bad for search procedurally[66] and constitutionally flawed.[67]

Though elimination of the plain view doctrine would address the privacy concerns associated with digital searches of broad scope, the courts have not even attempted to narrow the doctrine.[68] Moreover, any such elimination would undoubtedly face resistance in the law enforcement community: restricting law enforcement officers, prosecutors, and grand juries from using relevant evidence that is already right in front of them is a hard sell.

Meanwhile, many of the concerns that Kerr has with ex ante judicial narrowing of warrants are not present in the context of a subpoena quashal proceeding.[69] In such a proceeding, the court appropriately determines reasonableness subject to both constitutional and statutory commands. It passes judgment on a present request rather than a future action, and therefore does not create a conflict between the effects of prospective and retrospective analyses of reasonableness, which might introduce constitutional error. There is also no evidence in subpoena appeal cases of the compliance/non-compliance dynamic, which Kerr argues stunts the development of law when magistrate judges create ex ante warrant requirements.[70] While Kerr's arguments are formidable in the warrant context, they should not discourage courts from requiring subpoenas to be crafted with an appropriate level of particularity. As Kerr notes, ex ante review of particularity is a core purpose of the Fourth Amendment.[71] It would be inappropriate for courts to wait for new developments in the plain view doctrine and thereby avoid the responsibility to address reasonableness questions now. The next three sections thus examine different possibilities for ex ante judicial narrowing of subpoenas.

Before continuing, it is important to note that one of Kerr's arguments against ex ante judicial narrowing of search may still apply to certain solutions in the subpoena context. He notes that the Supreme Court has reversed courts that use creative tailoring of the search

65. Kerr, *Searches and Seizures in a Digital World*, *supra* note 63, at 583.

66. *Id.* at 575–76.

67. *See generally* Kerr, *Ex Ante Regulation of Computer Search and Seizure*, *supra* note 9 (arguing that ex ante regulation of computer searches invites constitutional errors in the search process).

68. The only decision to approach doing so is the *CDT* concurrence, which invites magistrate judges to require waiver of the plain view doctrine by prosecutors as an ex ante requirement for digital search warrants. *CDT*, 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, J., concurring). Because of its reliance on ex ante rather than ex post review, Kerr has suggested that the decision is flawed. *See* Kerr, *Ex Ante Regulation of Computer Search and Seizure*, *supra* note 9, at 1277–78.

69. For Kerr's legal concerns, see Kerr, *Ex Ante Regulation of Computer Search and Seizure*, *supra* note 9, at 1260–76. For his policy concerns, see *id.* at 1276–92.

70. *See id.* at 1287–90.

71. *Id.* at 1290–91 (citing Johnson v. United States, 333 U.S. 10, 13–14 (1948)).

methodologies laid out in warrants to define reasonableness through procedure.[72] Judge-designed procedures could be problematic in the subpoena context as well, especially given the traditional deference to the grand jury.

B. Look for Lessons from the Civil Law

Because of the growth in both corporate data retention and corporate civil litigation, civil law has passed criminal law in addressing "big data" concerns. The Federal Rules of Civil Procedure have recently been amended to contain guidelines explaining how best to mediate electronic discovery, including subpoenas for digital data.[73] The new Rules directly address undue burden,[74] and also encourage parties to agree on the scope of discovery without judicial intervention.[75] As a result, courts are taking a more active role in determining the reasonableness of subpoenas.[76]

At least one court has used the civil rules to guide negotiations over the relevance of requested information during electronic discovery in a criminal matter,[77] and at least one set of criminal defense attorneys has suggested that this should be a model for future courts addressing subpoenas for digitally stored data.[78] Those attorneys argue that "[i]t should not be unreasonable for prosecutors and defense counsel to engage in a voluntary meet and confer session with respect to [stored data] similar to that required under FRCP 26(f)."[79] This

---

72. *See, e.g.*, *id.* at 1261–64 (discussing Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979), in which the Court reversed a judge's issuance of a warrant after his own visit to a local bookstore to pre-determine what was obscene and therefore seizable); *id.* at 1267–69 (discussing United States v. Grubbs, 547 U.S. 90 (2006), in which the Court reversed the invalidation of a warrant where permission to search was conditioned on the occurrence of a particular event).

73. The e-discovery amendments took effect in 2006. For details, see Noyes, *supra* note 35, at 50–51.

74. FED. R. CIV. P. 26(b)(2)(B) ("A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.").

75. At the request of the judge, parties are required to confer and develop a discovery plan that discusses "any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced." *Id.* 26(f)(3)(C).

76. *See, e.g.*, Hoover v. Florida Hydro, Inc., No. 07-1100, 2009 WL 586507, at *3–4 (E.D. La. Mar. 6, 2009) (after subpoena of third-party witness computer, requiring production of the device); Integrated Serv. Solutions, Inc. v. Rodman, No. 07-3591, 2008 WL 4791654, at *2–5 (E.D. Pa. Nov. 3, 2008) (after negotiated search in response to a subpoena, ruling subpoena issuer was not entitled to additional information from searched computers barring bad faith on the part of electronic search service); Hardin v. Belmont Textile Mach. Co., No. 3:05CV492-MU, 2007 WL 2300795, at *4–5 (W.D.N.C. Aug. 7, 2007) (after subpoena for eight computers, discussing the relevance of the contents and the burden of producing them).

77. United States v. O'Keefe, 537 F. Supp. 2d 14, 15, 19 (D.D.C. 2008).

78. *See* Margolis et al., *supra* note 36.

79. *Id*.

solution has some merit as a policy matter. It allows subpoena recipients to perform an initial balancing between their need to avoid overbroad disclosure and any burden that would arise from setting a particular standard and then meet the government in the middle.

However, this solution also has significant drawbacks. First, it is a variant of the kind of ex ante judge-designed procedural mechanism that Kerr noted is not welcomed by the Supreme Court. Though judges have supervisory powers to control the rules of courtroom procedure, they rarely restrict grand juries with these powers.[80] This problem could potentially be cured by a legislative enactment or an amendment to the criminal rules.[81] Second, subpoena recipients have little leverage in negotiations with the government. Faced with the possibility of legal action for failing to produce relevant data, they may simply throw up their hands and yield to prosecutorial demands. Third, negotiation sessions would not address the increasingly important problem of accessing data held by third parties. Three-way negotiation sessions might well prove to be an administrative nightmare. In fact, in the civil context, judges have avoided this complexity by allowing recipients to raise the SCA as a shield.[82]

C. Employ Independent Examiners to Filter Out Irrelevant Material Before Production

Rather than disclose digitally stored documents directly to the grand jury, the court could employ an intermediary for the search process. Under such a plan, a defendant would turn the digitally stored documents over to a court-appointed special master to perform a search of the data and turn over all relevant information to the grand jury.[83] This solves the relevance and particularity issues (since the irrelevant information is removed before it reaches the grand jury), and the undue burden issue (since the cost of searching for relevant information is borne by the judicial system rather than the defense).

---

80. The grand jury is an independent fact-finding body with a judicial role independent of the judiciary. As a result, the courts have been reluctant to restrict the grand jury's ability to request information ex ante. *See* United States v. R. Enters., 498 U.S. 292, 297 (1991).

81. Congress can limit grand jury subpoenas by statute. *See* Gelbard v. United States, 408 U.S. 41, 52 (1972).

82. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 976 (C.D. Cal. 2010); *In re* AOL, LLC, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008); Ryan A. Ward, Note, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 HARV. J.L. & TECH. 563 (2011). This is also true for criminal defendants attempting to access stored data. *See* Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L & CRIMINOLOGY 569, 583–90 (2007) (analyzing the SCA's application to criminal defendants' requests for both content and other records during discovery).

83. This is suggested as an alternative to a pure technological solution in both *In re Grand Jury Subpoena 1993* and *CDT*. *See In re Grand Jury Subpoena 1993*, 846 F. Supp. 11, 13 (S.D.N.Y. 1994); *CDT*, 621 F.3d 1162, 1169 (9th Cir. 2010).

There are two significant problems with this solution. First, the authority of the courts to regularly employ such special masters is not clear. Again, it raises the concern of court-designed procedural intrusion. This is especially daunting in light of the second problem: the administrability of this solution. Independent third parties would need to be called upon to scan and sort digital data every time it becomes part of a criminal case. Assuming that subpoenas of digitally stored information continue to grow as discussed in the earlier sections of this paper, this means the development of an entire cadre of specialists to work alongside grand juries as they develop the factual records needed to begin prosecution. The resulting expense and procedural burden on an already overburdened court system make this solution impracticable, especially given that the preexisting expertise in search within the justice system lies with law enforcement rather than the courts. Court-appointed experts could serve as an option in especially delicate cases, but are unlikely to be broadly useful.

D. Use Technological Classifications to Narrow Data Production

Courts themselves might direct the sorting and production of relevant data through the specification of certain file criteria or search keywords. Both were explicitly embraced in *In re Grand Jury Subpoena 1993*, which suggested narrowing searches by category of document and searching by keyword.[84] In the more widely discussed context of warrants to search digitally stored data, this solution has had proponents both in the courts and among commentators.[85] However, such technological solutions currently have more detractors than supporters.[86] Courts have been swayed by the argument that the computer "forensics process is too contingent and unpredictable for judges to establish effective ex ante rules."[87] It is important that courts not draw too broad a conclusion from this argument — it is possible to demand particularity in the object of a search without demanding a specific forensics process. In order to do so, however, courts need to demystify computer search.

Courts build up the process of engaging in routine computer forensics, suggesting that it "can be as much an art as a science."[88] In

84. 846 F. Supp. at 13–14.

85. *See CDT*, 621 F.3d at 1178–79 (Kozinski, J., concurring); Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 103–09 (1994).

86. *See* United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, at *37–38 (S.D.N.Y Apr. 4, 2007) (citing a number of cases in which this policy was rejected as insufficiently flexible for law enforcement); *see also* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 197–220 (2005) (describing the movement toward this point of view between 1995 and 2005).

87. Kerr, *Searches and Seizures in a Digital World*, *supra* note 63, at 572.

88. United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005).

fact, it is usually less of either than a process of following checklists. While it is certainly true that "[a]nalyzing a computer is a continuous process that involves performing hundreds or even thousands of individual steps,"[89] those individual steps are usually not complicated and rarely require creativity. Most criminal computer forensics involves publicly documented tools such as EnCase.[90] As the manual for that product demonstrates, the basic use of such tools may involve several steps, but often follows prescribed paths through those steps.[91] The danger that the court will disrupt such processes is relatively limited. This is not to say that courts should prescribe which particular tools, or suggest which internal modules within those tools, should be part of a given search; it is intended only to note that forensic search is not an overwhelmingly complex process.

The basics of the search process are likely to stay constant because digital storage is organized around a series of standard assumptions. Information is stored as bits and organized into files. Because files are encoded according to standard formats so that they can be read by the programs that interpret them, those contents are also recognizable to forensics programs. Courts often suggest that searches by keyword or category of file are insufficient because metadata, such as file title, file extension, or date stamp, can be easily changed, and thus data fitting the relevant category may not be found by a search.[92] First, this assumes a very superficial search. The actual contents of a file are not changed simply because a user changes its extension from .pdf to .doc, and standard computer forensics programs are capable of recognizing a file's true format without relying on its extension.[93] Second, such concerns are less relevant outside of the warrant context. Cooperative data creators turning data over in response to a subpoena, aware of their own data management habits, will be able to overcome these minor concerns. Separately, commentators often suggest that data in encrypted or obfuscated files (such as those protected by digital rights management) will not be identified through the use of con-

89. Kerr, *Searches and Seizures in a Digital World*, *supra* note 63, at 576.

90. For a basic description of EnCase, see *EnCase Forensic*, GUIDANCE SOFTWARE, http://www.guidancesoftware.com/forensic.htm (last visited Apr. 13, 2011).

91. *See generally* GUIDANCE SOFTWARE, ENCASE VERSION 6.12 MODULES MANUAL (2008), *available at* http://download.guidancesoftware.com/bu871Xx3vGYhxQL5lGGRjP0xJM4XyLXqPbpeGKhnKeU4oIAGHY0M0mlGq7Fib4CG (download zipfile, unzip for pdf) (offering step-by-step instructions on how to perform assorted forensic searches).

92. *See* United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006).

93. Programs do this through file signature analysis — recognizing the byte patterns at certain points in a given file that indicate a JPEG image, Word document, or some other type of file. This is a standard attribute of forensics programs. *See, e.g.*, *EnCase Forensic*, GUIDANCE SOFTWARE, http://www.guidancesoftware.com/forensic.htm#tab=2 (last visited May 6, 2011) (discussing ability to do "file signature analysis . . . even within compounded files or unallocated disk space").

tent-based file searches.[94] This may be true, but remains true irrespective of any court-driven determination of the content to be searched. Such files would not be found using any standard forensic search technique; they are by definition unreadable without a key. Moreover, such concerns are less relevant when cooperative users, who possess those keys, turn over files.

It is easy to see that the courts are not in the best position to design technological search methods given their lack of specialized knowledge of technology.[95] What they can do, however, is ask for particularity in the form of categories of files (images, audio files, text files, email, etc.) and, in the specific case of text files, a description of the documents desired (authors, subjects, etc.). Specific file types or keyword lists would also not dictate the form of the search, given the standard assumptions about digital storage described above, but might assume too much about the data to be searched and thus over-specify the search procedure. By requesting these general descriptions of the data desired by the grand jury, courts can best balance the demands of relevance and particularity.

E. For Third-Party Digital Subpoenas, Make Legislative Changes to Increase Notice to or Protections for Data Creators

Finally, in the increasingly common case in which data is subpoenaed from third parties, judicial review of the reasonableness of that subpoena is particularly important. Notice to the creator of the stored data is one obvious means to ensure that reasonableness is argued before the court, but the third-party doctrine cases deny that notice is a requirement for constitutional reasonableness.[96] The debate over the application of the doctrine in cloud computing cases is beyond the scope of this Note.[97] However, barring reconsideration of these precedents, only legislative intervention is likely to change the standard for reviewing third-party subpoenas.[98]

---

94. Kerr, *Searches and Seizures in a Digital World*, *supra* note 63, at 575. For a brief explanation of this process, see Mathias Klang, *A Critical Look at the Regulation of Computer Viruses*, 11 INT'L J.L. & INFO. TECH. 162, 165–67 (2003) (describing the various tools a computer virus may use to avoid detection).

95. *See* Kerr, *Searches and Seizures in a Digital World*, *supra* note 63, at 575–77.

96. *See supra* Part III.

97. For more on the subject, compare Kerr, *Applying the Fourth Amendment to the Internet*, *supra* note 3, at 1029 (arguing that items in the cloud should be protected by the Fourth Amendment despite the third-party doctrine), and Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 579–81 (2009) (justifying the non-application of the third-party doctrine in similar cases by arguing for the technological neutrality of Fourth Amendment protections), with *In re* United States, 665 F. Supp. 2d 1210, 1223–24 (D. Or. 2009) (holding that the third-party doctrine applies to requests for data held by cloud computing providers).

98. Potential changes to the notice standard range from requiring full notice and an opportunity for the data creator to issue a motion to quash to simply requiring in camera re-

VI. CONCLUSION

Criminal investigators in the era of digital data storage are faced with a bounty of information that can be both tempting and bewildering. The grand jury subpoena is a powerful tool for acquiring such data, and investigators can and should make use of it. Unchecked access to these massive new stores of information, however, will lead to data collection that is clearly unreasonable. Courts must carefully consider how to limit subpoena requests in order to ensure that guarantees of relevance and particularity in the data produced are satisfied, and that the reasonable expectation of privacy ensured by the Fourth Amendment continues to be upheld. Requiring that the subpoenas identify more specific categories of files or a base of relevant text is a good first step to achieving that balance.

---

view by the court before turning over data to the requester. At least one state already requires this latter type of hearing for subpoenas of data held by third parties. *See* Kling vs. Superior Court, 239 P.3d 670, 674–75 (Cal. 2010) (explaining that the application of this rule maintains the court's control over the criminal discovery process).