Vanderbilt Journal of Entertainment & Technology Law

Volume 14
Issue 2 *Issue 2 - Winter 2012*

Article 1

2012

Compelled Production of Encrypted Data

John E.D. Larkin

VANDERBILT JOURNAL OF
ENTERTAINMENT AND TECHNOLOGY LAW

VOLUME 14 WINTER 2012 NUMBER 2

Compelled Production of Encrypted Data

*John E. D. Larkin**

ABSTRACT

There is a myth that shadowy and powerful government agencies can crack the encryption software that criminals use to protect computers filled with child pornography and stolen credit card numbers. The reality is that cheap or free encryption programs can place protected data beyond law enforcement's reach. If courts seriously mean to protect the victims of Internet crime—all too often children—then Congress must adopt a legal mechanism to remedy the technological deficiency.

To date, police and prosecutors have relied on subpoenas to either compel defendants to produce their password, or to decipher their protected data. This technique has been met with mixed success.

A better solution would be to couple a subpoena for the deciphered data with a warrant that specifies what and how to search. If the defendant refuses to produce the deciphered data, he can be held in contempt.

Where handing over protected data means the certainty of a lengthy prison sentence, some defendants will prefer contempt to compliance. Therefore, the court needs an additional legal mechanism to allow fact-finders to look into protected data. This Article proposes that when a defendant refuses to comply with a court order to produce deciphered data, the court should be able to issue a missing evidence instruction as a surrogate for actual inspection. If a warrant, a subpoena, and a contempt order cannot induce a defendant to decrypt

* © 2011 *John E. D. Larkin* graduated from Oberlin College and the Villanova University School of Law. He is an Assistant District Attorney, specializing in Appeals, at the Montgomery County District Attorney's Office. He worked on the analysis of the compelled disclosure issue in *Commonwealth* v. *Hurst*, discussed *infra*.

his data, courts should issue an instruction that the fact-finder may presume that the missing data is incriminating.

TABLE OF CONTENTS

Crime is going digital.[1] Child pornography in particular has drawn national attention to Internet crime,[2] but it is hardly unique; wire fraud has turned into email scams,[3] robbery has evolved into "war-driving,"[4] and harassment has become cyber-bullying.[5] Building a case against suspected online criminals has the potential to be

1. "Internet expansion has fostered new kinds of crimes, additional means to commit existing crimes and increased complexities of prosecuting crimes." Shannon L. Hopkins, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, 2 J. HIGH TECH. L. 101, 101 (2003).

2. "[S]uch things as 'sexting,' the sharing of sexually explicit photos, and the use of webcams for sexual interactions make headlines in connection with child pornography, pedophilia, and concerns about early teenage sexuality . . . ." Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technological Change*, 70 MD. L. REV. 614, 624 (2011).

3. *See generally* Lauren D. Lunsford, Note, *Fraud, Fools, and Phishing: Mail Fraud and the Person of Ordinary Prudence in the Internet Age*, 99 KY. L.J. 379 (2011) (examining the application of wire and mail fraud statutes in the digital age).

4. Sarah Jane Hughes, *Payments Data Security Breaches and Oil Spills: What Lessons Can Payments Security Learn from the Laws Governing Remediation of the Exxon Valdez, Deepwater Horizon, and Other Oil Spills?*, 5 BROOK. J. CORP. FIN. & COM. L. 111, 132 (2010) (describing "war driving" as a method by which cybercriminals search for unencrypted data to intercept from moving vehicles).

5. John E. D. Larkin, *Criminal and Civil Liability for User Generated Content: Craigslist, A Case Study*, 15 J. TECH. L. & POL'Y 85, 86 (2010) (describing Margery Tannenbaum's conviction for harassment through Craigslist's casual encounters forum).

relatively simple: Their own computers become a treasure trove of incriminating photographs, emails, documents, and programs.[6]

In 2011, the Montgomery County District Attorney's Office prosecuted a case that was not so simple. In *Commonwealth v. Hurst*, county prosecutors charged the defendant—a vice principal at a local elementary school—with carrying on an inappropriate relationship with one of his minor students.[7] As a part of this relationship, the victim claimed that the defendant sent him inappropriate text messages;[8] the victim substantiated this claim by handing over his own phone, which included dozens of inappropriate text messages from the defendant.[9] Hurst purported to explain the texts by telling the police that a virus had infected his phone.[10] As a demonstration of his ostensible good faith, he handed the phone over to the police voluntarily.[11] However, the phone was encrypted and the defendant refused to tell the police his password.[12]

As a matter of course, the government was interested in searching Hurst's cell phone. Doing so could connect the defendant to the messages sent to the victim and provide the necessary evidence to refute his claim that the texts were sent by a virus (or substantiate it and end the prosecution).[13] This posed the question—one of first impression in Pennsylvania (and most other jurisdictions)—under what circumstances can the government view encrypted data and using what procedural mechanisms?

Charles Hurst ultimately pled guilty, obviating the need for Pennsylvania courts to wrestle with this question.[14] The day when an answer will be needed, however, is fast approaching.[15]

---

6. Rachel Kathleen Gernat, *Avoiding the Pitfalls of Prosecuting Internet Crimes Against Children*, *in* STRATEGIES FOR PROSECUTING INTERNET PORNOGRAPHY CASES: LEADING PROSECUTORS ON INTERVIEWING THE SUSPECT, DEVELOPING A TRIAL STRATEGY, AND NEGOTIATING THE CHARGES 1, 2 (Aspatore 2008) (describing some of the unique challenges and opportunities that cybercrime poses to prosecutors)

7. *See* Regina Medina, *Educator Accused of Sexting Teen*, PHILA. INQUIRER, Sep. 25, 2010, http://articles.philly.com/2010-09-25/news/24977846.

8. *Id.*

9. Carl Hessler Jr., *Phone Battle Wages On in Former NP Vice Principal Charles Hurst's Case*, THEREPORTERONLINE.COM (Mar. 2, 2011), http://www.thereporteronline.com/articles/2011/03/02/news/doc4d6d1f12d1ed6285540546.txt.

10. *Id.*

11. *Id.*

12. *Id.*

13. *See id.*

14. Matt Coughlin, *Frmr Vice Principal Pleads Guilty to Corrupting Boys*, PHILLYBURBS.COM (Mar 16, 2011, 3:03 PM), http://www.phillyburbs.com/news/crime/frmr-vice-principal-pleads-guilty-to-corrupting-boys/article_a7669caa-5000-11e0-bdf5-0017a4a78c22.html.

A few courts in other jurisdictions have considered the question of whether and under what circumstances the police can search an encrypted computer or device,[16] and a small body of academic literature has begun exploring those decisions and their ramifications.[17] Thus far, academia has universally acknowledged that "as criminal activity becomes more sophisticated through the use of computer technology, it is reasonable to conclude that government agents charged with fighting computer crime should be given some latitude and discretion in how to confront these complicated matters."[18] Beyond this broad statement there is little consensus.[19]

Michael Smith, for instance, proposes that courts treat computers like locked containers for Fourth Amendment purposes.[20] On the other hand, Nathan McGregor notes that encrypted data is clearly distinguishable from the contents of a locked container because it is "scrambled."[21] He states that compelling defendants to "unscramble" encrypted data flirts with violating the privilege against compelled self-incrimination.[22] David Colarusso agrees that encrypted data presents Fifth Amendment concerns but declines to opine as to how courts will—or should—resolve the matter.[23]

This Article proceeds in three sections. First, it considers the Fourth Amendment requirements for a constitutional search of a password-protected device. Next, where encryption makes a search impossible, this Article considers the Fifth Amendment ramifications

---

15. *See generally* David Colarusso, Note, *Heads in the Cloud, A Coming Storm the Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection Against Self-Incrimination*, 17 B.U. J. SCI. & TECH. L. 69, 100 (2011).

16. *See In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009); *see also* United States v. Kirschner, No. 09-MC-50872, 2010 WL 1257355, at *1 (E.D. Mich. Mar. 30, 2010).

17. Nathan K. McGregor, Note, *The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege*, 12 VAND. J. ENT. & TECH. L. 581, 602-03 (2010); *see, e.g.*, Colarusso, *supra* note 15, at 73; *see also* Andrew J. Ungberg, Note, *Protecting Privacy Through a Responsible Decryption Policy*, 22 HARV J.L. & TECH. 537, 539 (2009).

18. Michael Smith, Survey, *The Fourth Amendment, Password-Protected Computer Files and Third Party Consent Searches: The Tenth Circuit Broadens the Scope of Warrantless Searches*, 85 DENV. U. L. REV. 701, 724 (2008).

19. Colarusso, *supra* note 15, at 100; McGregor, *supra* note 17, at 602-03; *see, e.g.*, Smith, *supra* note 18, at 724.

20. Smith, *supra* note 18, at 723.

21. McGregor, *supra* note 17, at 602-03.

22. *Id.* McGregor explains that encryption is inherently different from physical protections like locked briefcases. *Id.* This is so, he argues, because a locked briefcase protects the documents within without altering them; encryption, on the other hand, replaces the protected data with a new scrambled version. *Id.* As such, he argues, compelling defendants to unscramble their data requires them to create a new and inculpatory document. *Id.*

23. Colarusso, *supra* note 15, at 100. Instead, Mr. Colarusso, perhaps wisely, concludes that "[a]ll that is certain is this: a storm is coming." *Id.*

of compelling a defendant to reveal his password or produce a deciphered copy of his protected data. This Article then considers situations in which defendants may refuse to comply with court orders that compel them to hand over incriminating data. This Article concludes by suggesting that courts can give a missing evidence instruction where the defendant is in sole control of the encrypted data and refuses to comply with a court order to produce a deciphered copy.

I. ELECTRONIC DEVICES ARE SUBJECT TO UNIQUE FOURTH AMENDMENT PROTECTIONS

Today, easily obtainable encryption software products can protect data so effectively that many branches of law enforcement cannot decipher the encrypted data.[24] This poses a significant practical problem for police who wish to bypass a defendant's password to search his computer without consent. Techniques are available, however, that law enforcement officers can use to access protected data. For instance, where the password is only a few characters long, a computer can sequentially try each possible combination of letters or numbers until it reaches the correct password.[25] In addition, some popular devices have well-known security flaws built into their operating codes that law enforcement can exploit to reach protected data.[26] And even an unbreakable encryption regime on a secure device can be defeated if the defendant's password is easy to guess; for example, Charles Hurst protected his phone with his birth date.[27]

In the *Hurst* case, the defendant made it clear that he was unwilling to provide the Commonwealth with the password to his phone under any circumstances and that he intended to take his case

24. *Id.* at 77. "Modern innovations, however, have resulted in the creation of encryption schemes so difficult to break that practical considerations render them effectively unbreakable. Given the power of today's computers, it could take longer to break such encryption than there are years left in the universe." *Id.* (footnote omitted).

25. Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 IOWA L. REV. 1125, 1164 (2011). There are only 10,000 possible combinations of four numbers, for instance. *Id.* For instance, a four digit numerical password—like an ATM PIN—can be deciphered in minutes by a computer that sequentially tries each possible combination. *Id.*

26. *Id.*

27. Carl Hessler Jr., *Update: Former North Penn Vice Principal Charles Hurst Cell Phone Password Obtained*, MONTGOMERY NEWS (Mar. 3, 2011), http://www.montgomerynews.com/articles/2011/03/03/north_penn_life/news/doc4d6fa74747db3944451459.txt.

to trial.[28] However, once a cooperating witness provided the password, the defendant decided to accept a plea bargain.[29]

The outcome of the *Hurst* case demonstrates the importance of protected data in such cases. The inappropriate text messages that the police recovered from Hurst's phone were powerful evidence against him. Nevertheless, their evidentiary value was, in some respects, marginal: Had the Commonwealth been unable to decrypt the cell phone, it could have offered the text messages that the victim received. The fact that Hurst predicated his decision to plead guilty, at least in part, on this marginally valuable evidence underscores the fact that, in some cases, the decryption of protected data will itself determine the outcome of the trial.

For instance, the government may receive information from a defendant's Internet Service Provider that he recently downloaded an image that depicts child pornography.[30] This evidence, without more, is strongly indicative that the defendant is guilty of violating the federal child-pornography statute.[31] If the image that the government knows about is encrypted—particularly in cases where investigation would reveal additional illegal images—the defendant may prefer to refuse a court order to decipher his hard drive and accept imprisonment for criminal contempt (in addition to a conviction for a single count of child pornography), rather than expose himself to convictions for hundreds of illegal images.

In short, encryption places protected data beyond the reach of law enforcement; even where courts order the defendant to hand over his password or a copy of the deciphered data, noncompliance may shut the door on effective prosecution. This reality suggests a need to create an alternative and more effective method for courts to compel defendants to disclose the contents of encrypted devices. Any such procedure, however, would self-evidently be subject to the rigorous requirements of the Fourth and Fifth Amendments.

---

28. *Id.*

29. *Id.*; Coughlin, *supra* note 14.

30. Most Internet Service Providers routinely monitor the content of emails by searching for specific files that have already been identified as containing child pornography. Steven R. Morrison, *What the Cops Can't Do, Internet Service Providers Can: Preserving Privacy in Email Contents*, 16 VA. J.L. & TECH. 253, 265 n.68 (2011). When the service provider detects these files being sent, it contacts law enforcement. *Id.*

31. 18 U.S.C. § 2252 (2006).

A. Searching Electronic Devices

Searching electronic devices, regardless of whether they are password protected, poses unique Fourth Amendment problems. In any context, warrantless searches are presumptively unreasonable under the Fourth Amendment.[32] Searches pursuant to a warrant are only valid where the warrant is based on probable cause that evidence of a crime will be found in the place to be searched.[33] Additionally, the warrant must describe with sufficient particularity the place(s) to be searched and the item(s) to be seized.[34]

The particularity requirement is aimed at preventing "general, exploratory rummaging in a person's belongings."[35] "This requirement 'makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.'"[36] Where a search warrant directs the police to seize a tangible object at a particular location, the search protocol is straightforward: The police may search inside closed containers that, by virtue of their size or shape, could contain the sought after contraband.[37] A limited exception to this protocol—the plain view doctrine—permits officers to seize evidence found in the open during an otherwise lawful search, even if the original search warrant did not contemplate the seized contraband.[38]

Unfortunately, computer searches are less straightforward for Fourth Amendment purposes. The metadata associated with computer files (like the files' names, dates of creation and modification, and file types) can be altered or misleading.[39] Thus, because the contents of a computer file cannot be determined without opening it, every computer search risks transforming into a general

---

32. Horton v. California, 496 U.S. 128, 133 (1990).

33. U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . ."); *see also* Illinois v. Gates, 462 U.S. 213, 230 n.6 (1983).

34. U.S. CONST. amend. IV ("Warrants shall issue . . . particularly describing the place to be searched, and the persons or things to be seized."); *see also* Groh v. Ramirez, 540 U.S. 551, 557 (2004).

35. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

36. Andresen v. Maryland, 427 U.S. 463, 480 (1976) (alteration in original) (quoting Stanford v. Texas, 379 U.S. 476, 485 (1965)) (internal quotation marks omitted).

37. United States v. McLevain, 310 F.3d 434, 439 (6th Cir. 2002) (finding search under a bed and in a garage to be objectively reasonable pursuant to a search warrant for a fugitive because a person could hide in these locations).

38. Horton v. California, 496 U.S. 128, 142 (1990).

39. United States v. Tillotson, No. 2:08-CR-33, 2008 WL 5140773, at *5 (E.D. Tenn. Dec. 2, 2008) ("Data can be obscured or hidden by placing it in files with misleading names, or even in files that suggest the contents are something completely different from what they actually are.").

search.[40] Moreover, because computer data is never in "view" in the same way as tangible evidence, the application of the plain view doctrine is uncertain in the electronic context.[41] This danger is compounded by the fact that most computers contain sensitive data,[42] such as medical records, wills and trusts documents, business emails, and confidential communications with attorneys.[43]

The US Supreme Court has not yet addressed this question, and the circuit courts have adopted varying strategies to cope with this reality. The US Court of Appeals for the Ninth Circuit has done the most to protect individual privacy, and in a concurring opinion by Chief Judge Kozinski, suggests that:

> [T]he warrant application should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown. The procedure might involve, as in this case, a requirement that the segregation be done by specially trained computer personnel who are not involved in the investigation. In that case, it should be made clear that only those personnel may examine and segregate the data. The government should also agree that such computer personnel will not communicate any information they learn during the segregation process absent further approval of the court.
>
> . . . .
>
> Once the data has been segregated (and, if necessary, redacted), the government agents involved in the investigation should be allowed to examine only the information covered by the terms of the warrant. Absent further judicial authorization, any remaining copies should be destroyed or, at least so long as they may be lawfully possessed by the party from whom they were seized, returned along with the actual physical medium that may have been seized (such as a hard drive or computer). The government should not retain copies of such returned data unless it obtains specific judicial authorization to do so.[44]

Judge Kozinski would require police officers to include a search protocol in their application for a warrant to search a seized

---

40. *Id.* ("Recalling that pornography could be located in files with misleading names, authorizing a search of all files on the computer was as specific as the warrant could be under the circumstances.").

41. 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, 619 (2010); Bryan K. Weir, Note, *It's (Not So) Plain to See: The Circuit Split on the Plain View Doctrine in Digital Searches*, 21 GEO. MASON U. C.R. L.J. 83 (2010). *See generally* James Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 FORDHAM L. REV. 2809 (2011).

42. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551-52 (2005) ("A computer is akin to a virtual warehouse of private information . . . .").

43. Grubb v. Bd. of Trs. of the Univ. of Ill., 730 F. Supp. 2d 860, 862 (N.D. Ill. 2010) (involving an employee's laptop, which contained "personal and sensitive information, as well as testing data and private patient information").

44. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179 (9th Cir. 2010) (Kozinski, C.J., concurring).

computer.[45] Courts in the Second Circuit[46] and the Eighth Circuit[47] have rejected Judge Kozinski's search protocol as a per se requirement, but have nevertheless expressed approval of the procedure.[48]

One court in the Sixth Circuit, however, has rejected the use of such protocols altogether. Specifically, the US District Court for the Eastern District of Tennessee has observed that "[t]he warrant process is primarily concerned with identifying what may be searched or seized—not how—and whether there is sufficient cause for the invasion of privacy thus entailed."[49] On this basis, the Court concluded that "when the search warrant permits the agents to search a computer, they may search all of the files in that computer for the items to be seized."[50]

The US Court of Appeals for the Tenth Circuit,[51] has charted a middle path, and the US Courts of Appeals for the Third,[52] Fifth,[53] Seventh,[54] and Eleventh Circuits have joined it.[55] Each of these courts rejects the Ninth Circuit's suggestion that a search protocol must be attached to every warrant application.[56] However, they also do not

45. *Id.*

46. United States v. Dupree, 781 F. Supp. 2d 115, 152 (E.D.N.Y. 2011) ("Although the government is not required to include in its application for a search warrant a search protocol, enumerating the methods that the government might use to search computers, where the government does so, courts have found the warrant sufficiently particular.").

47. United States v. Cartier, 543 F.3d 442, 447-48 (8th Cir. 2008) ("While we acknowledge that there may be times that a search methodology or strategy may be useful or necessary, we decline to make a blanket finding that the absence of a search methodology or strategy renders a search warrant invalid per se.").

48. *Id.; Dupree*, 781 F. Supp. 2d at 152.

49. United States v. Kernell, No. 308-CR-142, 2010 WL 1491873, at *8 (E.D. Tenn. Mar. 31, 2010) (quoting United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999)) (internal quotation marks omitted).

50. *Id.* (citing United States v. Ogden, No. 06-20033-STA, 2008 WL 4982756, at *3 (W.D. Tenn. Nov. 18, 2008)).

51. United States v. Brooks, 427 F.3d 1246, 1251-52 (10th Cir. 2005).

52. United States v. Stabile, 633 F.3d 219, 239-40 (3d Cir. 2011).

53. United States v. Kim, 677 F. Supp. 2d 930, 947 (S.D. Tex. 2009).

54. United States v. Mann, 592 F.3d 779, 785-86 (7th Cir. 2010) ("We are also skeptical of a rule requiring officers to always obtain pre-approval from a magistrate judge to use the electronic tools necessary to conduct searches tailored to uncovering evidence that is responsive to a properly circumscribed warrant. Instead, we simply counsel officers and others involved in searches of digital media to exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described."), *cert. denied,* 130 S. Ct. 3525 (2010).

55. United States v. Khanani, 502 F.3d 1281, 1290-91 (11th Cir. 2007).

56. *See, e.g., Brooks*, 427 F.3d at 1251 ("This court has never required warrants to contain a particularized computer search strategy.").

accept the conclusion that a warrant to search a computer grants *carte blanche* to view every file.[57]

Instead, the Tenth Circuit has directed searching officers to attempt, where feasible, to sort files into a set of relevant and irrelevant documents (or pictures, spreadsheets, videos, or music files) before opening them.[58] Having done so, the officer is afforded broad discretion to search the relevant data; the reviewing magistrate then considers the reasonableness of the search by examining "(1) the object of the search, (2) the types of files that may reasonably contain those objects, and (3) whether officers actually expand the scope of the search upon locating evidence of a different crime."[59]

The Third Circuit takes a similar approach and directs searching officers to employ "search methods such as focusing on the file type identified in the warrant, file names, keyword search, and directory structure."[60] In the Fifth Circuit, the US District Court for the Southern District of Texas takes this a step further and urges law enforcement to exclude files from searches based on metadata that contraindicates relevance; for example, officers should not open files created long before the date of the crime being investigated.[61] The Seventh and Eleventh Circuits decline to identify specific factors they will consider when reviewing a warrant application but have expressed support for the use of sorting and keyword searching.[62]

B. Searching Electronic Devices that Have Been Encrypted or Password Protected

Where defendants have password protected or encrypted their electronic devices, this protection poses Fourth Amendment, as well as technological, challenges for law enforcement.

---

57. *Id.* ("Recognizing the difficulties inherent in computer searches, in some circumstances, we have suggested that 'law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant.'" (quoting United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999))).

58. *Id.*

59. *Id.* at 1252.

60. United States v. Stabile, 633 F.3d 219, 239 (3d Cir. 2011) (citing *Carey*, 172 F.3d at 1276).

61. United States v. Kim, 677 F. Supp. 2d 930, 947 (S.D. Tex. 2009).

62. United States v. Khanani, 502 F.3d 1281, 1290-91 (11th Cir. 2007) ("Agent Scott Skinner testified that agents used 'keyword searches,' and 'if a document was opened and it wasn't . . . covered by the warrant, then it wasn't analyzed.' Khanani and Portlock fail to cite any binding case law that would lead us to conclude the procedures used in this case infringed defendants' Fourth Amendment rights." (alteration in original) (citation omitted)); *see also* United States v. Mann, 592 F.3d 779, 785-86 (7th Cir. 2010), *cert. denied*, 130 S. Ct. 3525 (2010).

For instance, in the *Hurst* case, the defendant voluntarily provided his cell phone to police.[63] On the one hand, by consensually handing over his cell phone, Hurst arguably forfeited his right to privacy in the data contained within.[64] Nevertheless, the fact that Hurst consented to the police possessing and inspecting the phone does not necessarily mean he specifically consented to a search of the phone's password-protected contents.[65] On the other hand, by handing over a password-protected device and refusing to provide the password, the defendant arguably declined consent to search the data on his phone.

In this way, password-protected devices, like Hurst's cell phone, pose two serious obstacles to searches. First, they may be impossible to decrypt without assistance from the defendant.[66] Moreover, when police can hack or guess the password, complying with the requirements of the Fourth Amendment may be challenging; just finding the appropriate software and hardware to enable a forensic search of obsolete or uncommon devices may be difficult or impossible, making conformity to the Ninth Circuit's particularity requirements a daunting task.[67]

This, however, is not a new challenge—courts have long been faced with instances where the nature of the needed evidence makes constitutionally permissible searches difficult.[68] Typically, in response to this challenge, courts require defendants to produce the sought-after information via a subpoena *duces tecum*.[69] This procedure avoids the danger that police will read irrelevant private information and neatly skirts many of the Fourth Amendment issues

---

63. Hessler, *supra* note 9.

64. *See* Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (stating that consent is an exception to both warrant and probable cause requirements).

65. United States v. Jones, 356 F.3d 529, 534 (4th Cir. 2004) ("[A] suspect's general, blanket consent to search a given area or item, by itself, would not likely permit officers to break into a locked container located within the area being searched.").

66. Ungberg, *supra* note 17, at 541 ("The primary problem for law enforcement is the fact that modern encryption software is extremely difficult to break. For example, a brute-force attack on the widely available PGP encryption suite could take billions of years. Furthermore, the underlying algorithms are incredibly complex, and 'solving' them is far beyond realistic capabilities of law enforcement. Practically speaking, encryption today is impenetrable insofar as it cannot be bypassed by available means within a reasonable amount of time." (footnotes omitted)).

67. *See generally* Oren Bar-Gill & Rebecca Stone, Mobile Misperceptions, 23 HARV. J.L. & TECH. 49, 60 (2009) (describing multiple hardware standards).

68. *See In re* Establishment Inspection of Skil Corp., 846 F.2d 1127, 1133 (7th Cir. 1988) (holding subpoena *duces tecum* to be less intrusive than search warrant because it involves no entry).

69. *Id.*

explored above.[70] It does, however, raise Fifth Amendment concerns, as discussed below.[71]

II. COMPELLING DEFENDANTS TO SURRENDER THEIR PASSWORDS POSES SERIOUS OBSTACLES IN THE FIFTH AMENDMENT CONTEXT

As noted above, searching a computer or electronic device without the owner's permission may be difficult or impossible in cases where he has encrypted the sought-after data.[72] Because the government can compel defendants to produce incriminating documents—so long as their *creation* was not compelled—one solution to this problem is for the court to order the defendant to decrypt the protected device. Decisions from the US Supreme Court, however, as well as recent case law from district courts in Michigan and Vermont, suggest that the answer is not that simple.

A. Historical Jurisprudence

The Fifth Amendment protects defendants from the compelled production of incriminating testimony or evidence.[73] The definition of incriminating evidence includes otherwise innocuous information that can lead investigators to proof of guilt.[74]

Additionally, this privilege extends further than statements that tend to incriminate the speaker; the act of production itself can be privileged under the Fifth Amendment.[75] If the mere act of production can "implicitly communicate incriminating facts, such as the admission that 'papers existed, were in [the] produc[ing] party's possession or control, and were authentic,'" the court cannot compel production without complex safeguards.[76]

---

70. Thomas Kiefer Wedeles, Note, Fishing for Clarity in A Post-Hubbell World: *The Need for a Bright-Line Rule in the Self-Incrimination Clause's Act of Production Doctrine*, 56 VAND. L. REV. 613, 619 (2003) ("[A] subpoena will be less disruptive to the third party's operations than a search warrant.").

71. *See* discussion *infra* Part II.

72. Ungberg, *supra* note 17, at 541.

73. Commonwealth v. Padillas, 997 A.2d 356, 362 (Pa. Super. Ct. 2010) (citing United States v. Doe, 465 U.S. 605, 610 (1984)).

74. Commonwealth v. Rickabaugh, 633 A.2d 647, 648 n.2 (Pa. Super. Ct. 1993) (citing Commonwealth v. Hawthorne, 236 A.2d 519, 519 (Pa. 1968)).

75. Fisher v. United States, 425 U.S. 391, 391 (1976); *see, e.g.*, *In re* Search Warrant B-21778, 521 A.2d 422, 428 (Pa. 1987); *see also* Andreson v. Maryland, 427 U.S. 463, 463 (1976).

76. SEC v. Ryan, 747 F. Supp. 2d 355, 363 (N.D.N.Y. 2010) (quoting United States v. Cianciulli, No. M18304 (RMBTHK), 2002 WL 1484396, at *2 (S.D.N.Y. July, 10, 2002)); *see also* United States v. O'Shea, 662 F. Supp. 2d 535, 544 (S.D. W. Va. 2009) ("The act of production doctrine permits individuals to resist the government's attempts to compel the individual to hand over documents in certain circumstances. According to this doctrine, the Self-Incrimination

On the other hand, the "Fifth Amendment has consistently been held to exclude only evidence which is testimonial in nature."[77] "Testimonial evidence is communicative evidence as distinguished from demonstrative or physical evidence."[78] In order to be testimonial, "an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information."[79]

Moreover, so long as the act of production doctrine is not a bar, courts and prosecuting authorities may subpoena defendants to produce incriminating evidence so long as its *creation* is not compelled.[80] In other words, prosecutors can compel defendants to produce the contents of personal or business records to be used as substantive evidence of the guilt of their author, in spite of the prohibition against self-incrimination.[81] This well-settled principle is known as the *Fisher* doctrine.[82]

For instance, in *Doe v. United States* (*Doe II*), the defendant was called before a grand jury to testify about possible federal offenses relating to unreported income.[83] The grand jury issued a subpoena requiring him to produce records of transactions at three banks in the Cayman Islands and Bermuda, but the defendant, citing his Fifth Amendment privilege against self-incrimination, refused to comply. In an attempt to circumvent the issue, the federal prosecutors subpoenaed the records directly from the foreign banks.[84] The banks, however, claimed that local regulations prevented them from releasing records without the signed consent of an authorized account holder.[85] The government then tried to subpoena the signed consent forms from the defendant who, again, invoked his privilege against compelled self-incrimination.[86]

Clause may apply if the *act* of producing a document communicates potentially incriminating information independent of the contents of the document.").

77. Commonwealth v. Fernandez, 482 A.2d 567, 569 (Pa. Super. Ct. 1984) (citing United States v. Lamb, 575 F.2d 1310, 1310 (10th Cir. 1978)).

78. *Id.* (citing Schmerber v. California, 384 U.S. 757, 757 (1966)).

79. Doe v. United States, 487 U.S. 201, 210 (1988).

80. United States v. Hubbell, 530 U.S. 27, 35-36 (2000) ("[A] person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' . . . .").

81. United States v. Ponds, 454 F.3d 313, 319 (D.C. Cir. 2006); *see also* Bear Sterns & Co., Inc. v. Wyler, 182 F. Supp. 2d 679, 681 (N.D. Ill. 2002) ("The Fifth Amendment protects the person asserting the privilege only from testimony that is compelled; as the preparation and maintenance of business records is voluntary, no compulsion is involved." (citing United States v. Doe, 465 U.S. 605, 610 (1984)).

82. Fisher v. United States, 425 U.S. 391, 391 (1976).

83. *Doe*, 487 U.S. at 202-03.

84. *Id.*

85. *Id.*

86. *Id.*

The US District Court for the Southern District of Texas refused to enforce the subpoena because the defendant, by signing the consent forms, would be admitting to ownership of and control over the foreign accounts.[87] His act of production would be testimonial, and therefore the Court declined to compel it.[88] In response, the federal prosecutors redrafted the consent form they had asked the defendant to sign, so as to avoid testimonial implications stemming from production.[89] Under the new language of the consent form, the defendant directed not only the specific target banks, but also any bank from which he was authorized to withdraw and deposit money, to provide relevant records to federal prosecutors in response to subpoenas.[90] By doing so, the government hoped to remove any information value from the consent form and, thus, negate the Fifth Amendment issue. Again, the defendant refused to comply.[91]

Ultimately, the US Supreme Court concluded that the new consent forms were so carefully drafted that the defendant's act of production would not be incriminating.[92] Moreover, the Court concluded that the consent forms were not sufficiently "testimonial" so as to fall within the ambit of the Fifth Amendment, because they did not "relate a factual assertion or disclose information."[93] Because the defendant did not specify to which banks he was directing his consent,

---

87. *Id.* at 203-04.

88. *Id.*

89. *Id.* at 204-05. The revised consent form read:

> I, _____, of the State of Texas in the United States of America, do hereby direct any bank or trust company at which I may have a bank account of any kind or at which a corporation has a bank account of any kind upon which I am authorized to draw, and its officers, employees and agents, to disclose all information and deliver copies of all documents of every nature in your possession or control which relate to said bank account to Grand Jury 84-2, empaneled May 7, 1984 and sitting in the Southern District of Texas, or to any attorney of the District of Texas, or to any attorney of the United States Department of Justice assisting said Grand Jury, and to give evidence relevant thereto, in the investigation conducted by Grand Jury 84-2 in the Southern District of Texas, and this shall be irrevocable authority for so doing. This direction has been executed pursuant to that certain order of the United States District Court for the Southern District of Texas issued in connection with the aforesaid investigation, dated _____. This direction is intended to apply to the Confidential Relationships (Preservation) Law of the Cayman Islands, and to any implied contract of confidentiality between Bermuda banks and their customers which may be imposed by Bermuda common law, and shall be construed as consent with respect thereto as the same shall apply to any of the bank accounts for which I may be a relevant principal.

Id. at 204 n.2 (citation omitted) (internal quotation marks omitted).

90. *Id.*

91. *Id.* at 201.

92. *Id.* at 216.

93. *Id.* at 210.

the government was not compelling him to disclose the bank he had used, and no testimonial information was revealed.[94]

Justice Stevens filed a dissent, in which he noted that:

> A defendant can be compelled to produce material evidence that is incriminating. Fingerprints, blood samples, voice exemplars, handwriting specimens, or other items of physical evidence may be extracted from a defendant against his will. But can he be compelled to use his mind to assist the prosecution in convicting him of a crime? I think not. He may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or deed.[95]

B. Recent Developments

Only three US courts have encountered the specific question of whether the Fifth Amendment protects a computer password. These courts reached opposing conclusions.

In *United States v. Kirschner*, a federal grand jury participated in an investigation of the defendant for three counts of felony possession of child pornography.[96] The defendant's use of password-encrypted files frustrated the investigation.[97] The prosecutors subpoenaed the defendant to testify before the grand jury, and asked him to reveal the password that would decrypt the contents of the files.[98] The defendant declined, and filed a motion to quash the subpoena invoking his Fifth Amendment right against self-incrimination.[99]

The US District Court for the Eastern District of Michigan characterized the issue as "whether requiring the Defendant to provide the password is a testimonial communication."[100] The court noted that, in *Doe*, the US Supreme Court had defined a testimonial act to occur any time "the accused is forced to reveal his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the government."[101] The district court also carefully noted that, in *Doe*, the revised form offered by the government was carefully tailored not to reveal any facts or convey information to the government.[102]

---

94. *Id.* at 215.

95. *Id.* at 219 (Stevens, J., dissenting).

96. United States v. Kirschner, No. 09-MC-50872, 2010 WL 1257355, at *1 (E.D. Mich. Mar. 30, 2010).

97. *Id.*

98. *Id.*

99. *Id.*

100. *Id.* at *3.

101. *Id.* (citing Doe v. United States, 487 U.S. 201 (1988)).

102. *Id.*

In the case at bar, however, the court concluded that the compelled disclosure of a password, unlike the form offered in *Doe*, communicated knowledge to the government and was therefore a violation of the Fifth Amendment.[103] The Court went on to assert that "even if the government provides Defendant with immunity with regard to the act of producing the password to the grand jury, that does not suffice to protect Defendant's invocation of his Fifth Amendment privilege in response to questioning that would require him to reveal his password."[104] On this basis, it quashed the government's subpoena.[105]

The District Court for the District of Vermont reached a different conclusion in *In re Boucher*.[106] In that case, a border patrol officer stopped the defendant at the Canadian border and searched his computer.[107] The border patrol officer found over 40,000 pornographic images, many of which the officer suspected to be child pornography. He seized the computer and federal prosecutors charged the defendant with possession of child pornography.[108]

Further investigation revealed that the child pornography was password protected.[109] Thus, an investigating grand jury subpoenaed the defendant to reveal his password, or an unencrypted version of his hard drive.[110] The defendant refused to comply with the subpoena, and invoked his Fifth Amendment privilege.[111] The government appealed.[112]

The court noted that there was "no question that the contents of the laptop were voluntarily prepared or compiled and are not testimonial, and therefore do not enjoy Fifth Amendment protection."[113] Moreover, the court observed that because the government was able to connect the defendant to the laptop without using his production of the unencrypted files as evidence of ownership, his act of production claim was moot.[114] The defendant was therefore required to produce an unencrypted copy of the laptop's hard drive.[115]

---

103. *Id.*
104. *Id.* at *4.
105. *Id.*
106. *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009).
107. *Id.*
108. *Id.* at *2.
109. *Id.*
110. *Id.*
111. *Id.* at *1.
112. *Id.*
113. *Id.* at *2.
114. *Id.* at *3.
115. *Id.* at *4.

Most recently, in *United States v. Fricosu* the US District Court for the District of Colorado was confronted with a similar situation.[116] There, like in *Boucher*, the government sought a writ to compel the defendant to produce an unencrypted version of the password-protected hard drive seized from her home.[117] Data found on the computer confirmed that it belonged to the defendant, and, in any event, the government offered her immunity for producing the unencrypted data.[118] On this basis, the court found that the act of production doctrine did not apply.[119] The court then observed that, as in *Boucher*, the government had only requested a copy of the unencrypted data on Fricosu's computer, as opposed to the actual password that the government requested in *Kirschner*.[120] Under the *Fisher* doctrine, the court held that the government's request for preexisting unencrypted documents, and not for the defendant's password, raised no Fifth Amendment concerns.[121] It therefore granted the government's request.[122]

C. Analysis of the Recent Developments

In *Kirschner*, the district court refused to allow the government to enforce a subpoena for the defendant's password because, according to that court, the password itself was testimonial.[123] This conclusion suffers from several defects.

First, the district court's holding that a password is testimonial ignores the reality that a password, like the document it protects, was created by the defendant.[124] Moreover, the password was written down and stored on the computer itself.[125] Thus, under *Fisher*, the government should be able to compel the defendant to produce the

---

116. United States v. Fricosu, No. 10-cr-00509-REB-02, 2012 U.S. Dist. LEXIS 11083, at *1 (D. Colo. Jan. 23, 2012).

117. *Id.* at *16.

118. *Id.* at *10-12.

119. *Id.* at *13-14.

120. *Id.* at *8-10.

121. *Id.* at *6-7, *11-12.

122. *Id.* at *13.

123. United States v. Kirschner, No. 09-MC-50872, 2010 WL 1257355, at *3 (E.D. Mich. Mar. 30, 2010).

124. Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 195-97. Philip Reitinger observes that the encryption key is stored along with the encrypted data. *Id.* Unlike the encrypted data, however, the key is not scrambled. *Id.* Thus, he argues, producing the encryption key does not compel a defendant to create new and inculpatory material, merely to disclose data that he has already created. *Id.* Using the encryption key, the government can decrypt the protected information without the defendant's assistance. *Id.*

125. *Id.* at 204-05 ("[B]ecause the key is stored on the computer, albeit in encrypted form, the government may subpoena it . . . .").

passwords.[126] If courts accept the premise that courts can compel defendants to produce documents that already exist, then their password, which they created and which is stored on their computers, is just such a document, and the court can compel its disclosure.

Second, the very premise that a password is "testimonial" is flawed. Many computers use biometric information—for example, a fingerprint, a voiceprint, or facial recognition—in lieu of a password.[127] It is well settled that this type of information is outside the ambit of the Fifth Amendment.[128] Compelling some defendants to surrender their "passwords" in the form of a fingerprint, but allowing others to keep an alphanumeric password secret, creates an arbitrary distinction[129] in a way that ignores the purpose of the Fifth Amendment's important protections.[130] The rationale of *Kirschner*'s holding, therefore, does not provide a good model for a general rule with respect to compelled production of encrypted data.

In *Boucher*, unlike *Kirschner*, the government chose to circumvent the defendant's password altogether: Instead of requesting that the defendant produce his password, the government simply demanded an unencrypted copy of the protected data.[131] This approach avoided the concerns raised by the dissent in *Doe II* about compelling defendants to surrender the combination to a safe,[132] and

126. Fisher v. United States, 425 U.S. 391, 409-10 (1976).

127. Aaron M. Clemens, Note, *No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or Private Key*, 2004 UCLA J.L. & TECH. 2 n.149 ("[B]oth the governmental and private sectors are making extensive use of biometrics to provide better service to the public." (alteration in original) (quoting John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 97-98 (1997) (internal quotation marks omitted)).

128. United States v. Dionisio, 410 U.S. 1, 5-6 (1973) (compelling production of voice exemplars does not violate the Fifth Amendment right against self-incrimination); Gilbert v. California, 388 U.S. 263, 266-67 (1967) (compelling production of handwriting exemplars does not violate the Fifth Amendment right against self-incrimination); Schmerber v. California, 384 U.S. 757, 765 (1966) (compelling blood test does not violate the Fifth Amendment right against self-incrimination); see also South Dakota v. Neville, 459 U.S. 553, 555 (1983) (admitting into evidence a refusal to take a blood-alcohol test does not violate the Fifth Amendment right against self-incrimination).

129. "[I]t may not be prudent to so closely analogize encryption keys to safe combinations given that non-privileged biometric data can be used in the place of a password. Should the protection afforded encrypted files depend on this choice of encryption keys? What would justify such a distinction?" Colarusso, *supra* note 15, at 85 (footnote omitted).

130. The Supreme Court "has often found . . . that the privilege recognizes the unseemliness, the insult to human dignity, created when a person must convict himself out of his own mouth. 'At its core, the privilege reflects our fierce unwillingness to subject those suspected of crime to the cruel [choice] of self-accusation, perjury or contempt.'" United States v. Balsys, 524 U.S. 666, 713 (1998) (quoting Pennsylvania v. Muniz, 496 U.S. 582, 596 (1990)).

131. *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009).

132. Doe v. United States, 487 U.S. 201, 221 (1988).

the trial court ultimately endorsed it.[133] There are, however, drawbacks to this approach as well.

First, a subpoena for the deciphered contents of an entire computer hard drive is likely overbroad.[134] Indeed, the majority of the files on any computer hard drive will usually be irrelevant to a criminal prosecution.[135] The hard drive subpoenaed in *Boucher*, for instance, was likely filled mostly with files used by the operating system, applications such as Word and Excel, and innocuous user-created content such as documents and spreadsheets.[136] Thus, a subpoena that demands the contents of an entire hard drive, like the subpoena in the *Boucher* case, requests mostly irrelevant data and risks getting quashed.[137] The issue of breadth was not raised in *In Re Boucher*, but this issue still remains.

Moreover, as McGregor notes, unlike documents in a safe, a readable version of the protected data ceases to exist when it is encrypted.[138] In place of legible data—a document, a photograph, or a video, for instance—the protected device holds machine code that is, without the encryption key, meaningless.[139] The meaningless data ceases to exist when it is deciphered, and the original document is created and stored in its place.[140] Thus, unless the defendant keeps an unencrypted copy of the data in another location, compelling his production of an unencrypted copy compels him to "create" incriminating data in violation of the private papers doctrine.[141]

---

133. *Id.*

134. It is, of course, well settled that subpoenas must request specific things that are relevant to the case at hand. *See, e.g.*, United States v. McDonald, No. 10-5150, 2011 WL 3805759, at *2 (4th Cir. Aug. 30, 2011) ("We have reviewed the subpoenas in this case, and we easily conclude that they are overbroad and unspecific. The district court properly found that McDonald was using the subpoenas to engage in a fishing expedition, and we find no error in the court's granting of the motion to quash.").

135. Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. PITT. J. TECH. L. & POL'Y 2, ¶ 42 (2007). Since many computers share common operating systems and applications—such as Windows, Word, Excel, and Powerpoint—the files associated with those programs can be recognized by forensic programs like EnCase and ignored. *Id.*

136. *See id.*

137. It is hornbook law that subpoenas must request specific things that are relevant to the case at hand. *See, e.g.*, *McDonald*, 2011 WL 3805759, at *2.

138. McGregor, *supra* note 17, at 602-03.

139. *Id.*

140. *Id.*

141. *Id.*

D. Analysis of Alternative Approaches

Other authors have argued that courts should extend constitutional protection to encrypted data based on the function of the protection, and not its technical methodology.[142] In other words, these authors argue that a defendant who chooses to store and encrypt child pornography on his computer is entitled to no greater protection than if he had locked it in a safe.[143] Affording special legal protection to encryption, these authors suggest, provides a windfall to computer users that does not correspond to the doctrinal basis of the Fifth Amendment.[144]

There is an intrinsic appeal to the function-over-method approach. It relies on analogies to existing technologies that are familiar to the courts[145] and, importantly, it rejects the notion that encryption creates a safe haven for dangerous contraband like child pornography.[146] Nevertheless, this approach is likely to be impractical to implement.

First, *Doe II* makes clear that, under some circumstances, the method by which even a real-world safe is secured can affect the government's access to the protected contents within.[147] Several jurisdictions have adopted this reasoning and have concluded that the methodology of encryption can have constitutional ramifications.[148] Thus, although intellectually appealing, the function-over-method approach may be difficult to apply in practice.

Moreover, there is broad agreement in academic literature that the analogy between computer encryption and real-world safeguards is a false one.[149] And, although courts have been quick to analogize

---

142. Reitinger, *supra* note 124, at 175-76.

143. *Id.*

144. *Id.*

145. "Courts naturally and necessarily turn to analogical reasoning to incorporate cyber-technologies into existing doctrinal rules." Luke M. Milligan, *Analogy Breakers: A Reality Check on Emerging Technologies*, 80 MISS. L.J. 1319, 1338 (2011).

146. McGregor, *supra* note 17, at 599 ("[P]roperly implemented, a strong encryption regime provides near absolute privacy.").

147. Doe v. United States, 487 U.S. 201, 219 (1988) (Stevens, J., dissenting). Even in Stevens's dissent, he acknowledges that defendants can be forced to "surrender a key to a strongbox containing incriminating documents . . . ." *Id.* This distinction was adopted in a later majority opinion. *See* United States v. Hubbell, 530 U.S. 27, 43 (2000).

148. United States v. Green, 272 F.3d 748, 753 (5th Cir. 2001); *see, e.g.*, United States v. Kirschner, No. 09-MC-50872, 2010 WL 1257355, at *3 (E.D. Mich. Mar. 30, 2010); *see also* Commonwealth v. Burgess, 688 N.E.2d 439, 449 n.6 (Mass. 1997).

149. Milligan, *supra* note 145, at 1338 ("Courts naturally and necessarily turn to analogical reasoning to incorporate cyber-technologies into existing doctrinal rules. . . . Such reasoning, however, is indeterminate, undisciplined, and in disregard of the subtleties of landmark cases . . . ."); McGregor, *supra* note 17, at 602 ("[T]he safe analogy fails to capture the

encryption to wall safes,[150] they have also, on occasion, been willing to accept that computers are a *sui generis* category of constitutional searches.[151] Judge Kozinski's concurrence in theUS Court of Appeals for the Ninth Circuit case, *Comprehensive Drug Testing*, for example, recognizes that computers contain immense amounts of personal data and argues that they should be subject to unique Fourth Amendment requirements.[152] The bulk of commentators agree;[153] therefore, an investigative strategy that treats encrypted data like documents in a safe will be unsuccessful.

Andrew Ungberg proposes another approach.[154] He agrees that computers are a novel constitutional object, and therefore suggests a unique approach to computer searches that blends the Fourth and Fifth Amendment concerns discussed above.[155] Specifically, he suggests that all searches of encrypted data begin with a search warrant that specifies—with particularity—the data sought.[156] If the warrant is issued, the police can then subpoena the defendant's password, which the court will (presumably) compel.[157] Once the data is decrypted, the police will only be authorized to search the computer for the data listed in the warrant.[158] Ungberg suggests that if police discovered "evidence of a crime about which they had no knowledge, [the defendant would be] immunized from prosecution because the agents have no right to use evidence not specified in the warrant."[159]

By limiting computer searches to the subject of a pre-obtained warrant, Ungberg's protocol strikes a laudable balance between the government's compelling interest in finding evidence of crime—particularly dangerous contraband such as child pornography—and a defendant's privacy interest. However, his proposal that police should never be permitted to seize unanticipated contraband found during the course of a warranted search ignores the plain view exception discussed above. While several commentators have questioned the viability of the plain view exception as applied to

---

essence of encryption."); *see* Ungberg, *supra* note 17, at 548 ("A hard drive is not simply a locked box full of documents. Encryption is neither a bank nor a safe." (footnote omitted)).

150. *See Kirschner*, 2010 WL 1257355, at *3.

151. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178-79 (Kozinski, C.J., concurring).

152. *Id.*

153. McGregor, *supra* note 17; Smith, *supra* note 18; Ungberg, *supra* note 17.

154. Ungberg, *supra* note 17.

155. *Id.* at 556-58.

156. *Id.* at 556.

157. *Id.*

158. *Id.*

159. *Id.*

computer searches,[160] there is no principled reason why courts should abandon it simply because the data searched is compulsorily deciphered, particularly in situations where, as he suggests, the police are "acting in good faith."[161]

In addition, Ungberg's approach may be problematic when applied to non-computer devices such as cell phones because, as noted above, the variety of devices used makes it difficult or impossible to find forensic technology.[162] Whereas computers generally have only a few distinct types of file architecture,[163] cell phones have dozens.[164] Accordingly, while it is relatively simple for forensic technicians to obtain the tools and software necessary to image, sort, and search computers,[165] doing so for every cell phone make and model is not a practical solution for most police departments. Penalizing law enforcement for a general search of a cell phone—a search procedure that current technology makes necessary—ignores the prophylactic purpose of the exclusionary rule, which is to deter law enforcement misconduct, not to reward clever defendants.[166]

Additionally, Ungberg's proposal that police subpoena the defendant's password, as opposed to the underlying data, is one that was rejected in *Kirschner*[167] and treated negatively in dicta in

160. *See generally,* Moshirnia, *supra* note 41; Saylor, *supra* note 41; Weir, *supra* note 41.

161. Ungberg, *supra* note 17, at 558.

162. *See generally* Bar-Gill, *supra* note 67, at 60.

163. Jekot, *supra* note 135.

164. *See* Wayne Jansen et al., *Overcoming Impediments to Cell Phone Forensics*, HAW. INT'L CONF. ON SYS. SCI., Jan. 16, 2008, *available at* http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51264; *see also* WAYNE JANSEN & RICK AYERS, NAT'L INST. OF STANDARDS & TECH., GUIDELINES ON CELL PHONE FORENSICS: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2007). The distinctions between cell phones, moreover, unlike the distinctions between computer brands, are as much a function of hardware as they are of software. *See* sources cited *supra* note 164. Different service providers—such as AT&T, T-Mobile, Sprint-Nextel, and Verizon—each require manufacturers to deploy different technologies when building what is branded as an identical phone. *See* sources cited *supra* note 164. It is for this reason that users often cannot change service providers and keep their original handset. *See* sources cited *supra* note 164. Indeed, as the top shelf of many of our closets can attest, even the cables that handsets accept vary from phone to phone, making physical connectivity a real problem. *See* sources cited *supra* note 164. Moreover, individual handsets, even when they employ substantially identical hardware, can be operated with radically different software. *See* sources cited *supra* note 164. Thus, the file system architecture of the iPhone is not compatible with software designed to work with phones that run Google's Android operating system, or with Palm OS, webOS, Windows Mobile, or Symbian. *See* sources cited *supra* note 164.

165. David D. Thomas, Note, *Dangerously Sidestepping the Fourth Amendment: How Courts Are Allowing Third-Party Consent to Bypass Warrants for Searching Password-Protected Computers*, 57 CLEV. ST. L. REV. 279, 289-90 (2009). The industry standard software package is currently EnCase. *Id.* at 289.

166. Schneckloth v. Bustamonte, 412 U.S. 218, 251 (1973).

167. *See generally* United States v. Kirschner, No. 09-MC-50872, 2010 WL 1257355 (E.D. Mich. Mar. 30, 2010).

Fricosu.[168] Therefore, although compelled production of a computer password is technologically indistinguishable from compelled production of encrypted data,[169] it is a procedure that needlessly risks suppression based on the *Kirschner* and *Fricosu* decisions.

The best approach would be to couple a warrant—made expressly subject to the practical limitations of the particularity requirement[170]—with a subpoena to produce an unencrypted copy of the protected hard drive. By subpoenaing the data, as opposed to the password, the government would employ a procedure that two courts have already endorsed as constitutional.[171] When the act of producing the data is incriminating in itself, the government can offer the defendant use immunity.[172] If the amount of data on the device makes production of an unencrypted copy overbroad, the court can limit production in its discretion.[173] In that way, the defendant is protected against a general search in a principled manner: The police will only have access to the data specified by warrant.

However, this proposal suffers from the inherent flaw that all schemes for compelled production of a password share: It relies on the

---

168. *See generally* United States v. Fricosu, No. 10-cr-00509-REB-02, 2012 U.S. Dist. LEXIS 11083 (D. Colo. Jan. 23, 2012).

169. Reitinger, *supra* note 124, at 203-04.

170. Jansen et al., *supra* note 164. Specifically, the warrant must acknowledge that some devices—such as phones—are not susceptible to the kind of forensic examination that computer hard drives routinely undergo. *Id.*

171. *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009). McGregor's complaint that deciphering encrypted data may rise to the level of "creating" inculpating evidence was not addressed by the *Boucher* court. *Id.* It seems unlikely, moreover, that it will be adopted because, taken to its logical conclusion, its result would harm defendants: if defendants concede that deciphering encrypted data is, in fact, a creative process, then courts must conclude that the defendant has "created" child pornography *every time* he himself deciphers his encrypted data. Because the mandatory minimum for creating child pornography is so much higher than possession, as is true for most possession crimes, it seems unlikely that defendants will embrace McGregor's analysis.

172. Reitinger, *supra* note 124 (noting use immunity is now routinely used as a tool to compel production of encryption passwords).

173. Ordering the defendant to produce an unencrypted copy of the protected data seems, at first blush, to be ordering the fox to guard the henhouse. Ordering him to sort the data on his hard drive and hand over only the subpoenaed directories or file types seems worse. Usually, though, the *only* copy of the data is the encrypted copy. Even if the defendant routinely backed up the data on his protected device, the backup copy would be stripped of important metadata like the date the files were created and last accessed. Thus, ordering a defendant to produce an unencrypted copy of a seized hard drive is really an order that he decrypt the copy already in police possession. Given this reality, there is no opportunity for defendants to tamper with incriminating data when they decrypt the hard drive in police custody; presumably, the police will have a forensic technician present at the time the defendant enters his password, and can ensure that the protected data is not altered. Similarly, where a defendant is ordered to hand over just a few files or directories, a forensic technician can ensure that he fully complies with the terms of the subpoena. The danger, already minimal, could be reduced still more if a court ordered the defendant's attorney to comply with the subpoena on his behalf.

defendant to comply with a court order to produce incriminating data. Because receipt of a single image depicting minors engaging in "sexually explicit conduct" will result in a minimum sentence of five years,[174] many defendants with similar contraband may find criminal contempt to be a preferable alternative.

III. A THIRD COMPONENT: THE MISSING WITNESS INSTRUCTION

As mentioned above, both the incentives to the defendant and the cost to the government of noncompliance with subpoenas in this context are high. Therefore, an additional legal mechanism should be implemented. Criminal contempt is one sanction that courts have used in the past but many defendants may find criminal contempt preferable to a police investigation of their computer or device.[175] A more effective sanction is a missing evidence instruction.

Missing witness instructions are not novel. Today, when evidence or a potential witness is available to only one of the parties, and the evidence is likely to be material and not cumulative, then, provided the party fails to produce the evidence or witness through bad faith, the court may instruct the jury to draw an inference that the missing evidence or testimony would have been unfavorable.[176] Where applicable, this instruction is equally available to both the government and the defense.[177]

The benefit of a missing witness instruction, used in conjunction with an order compelling a defendant to provide his password or an unencrypted copy of the protected data, is twofold. First, in cases where prosecution is completely foreclosed by the absence of the encrypted data, a jury instruction permits the

---

174. 18 U.S.C. § 2252 provides for a five to twenty-five years' imprisonment for defendants who receive or distribute child pornography via a computer.

175. *See supra* pp. 254-57.

176. An adverse inference drawn from the destruction of records is predicated on bad conduct. United States v. Wise, 221 F.3d 140, 156 (5th Cir. 2000); Coates v. Johnson & Johnson, 756 F.2d 524, 551 (7th Cir. 1985) ("The prevailing rule is that bad faith destruction of a document relevant to proof of an issue at trial gives rise to a strong inference that production of the document would have been unfavorable to the party responsible for its destruction."); Commonwealth v. Chapman, 386 A.2d 994, 1005 (Pa. Super. Ct. 1978) (instructing trial court to give missing evidence instruction where Commonwealth destroyed tangible evidence prior to defendant's retrial); *see also* Eaton Corp. v. Appliance Valves Corp., 790 F.2d 874, 878 (Fed. Cir. 1986) ("If a court finds that both conditions precedent, evidence destruction and bad faith, are met, it may then infer that the evidence would be unfavorable to the destroying party if introduced in court.").

177. *See* United States v. Crowder, 543 F.2d 312, 318 n.* (D.C. Cir. 1976) ("The prosecution might even claim the benefit of a 'missing evidence' instruction if Crowder declined to permit the surgical excision."); *see also* Commonwealth v. Chamberlain, 658 A.2d 395, 398 (Pa. Super. Ct. 1995) (affirming trial court's missing witness instruction where defendant failed to call her husband to testify at DUI trial).

prosecution to continue. In this way, it deprives the defendant of the unfair advantage he derives from encryption, and allows the prosecution a constructive method to see inside encryption that it cannot otherwise break.

Second, like the particularity requirement of a warrant, a missing evidence instruction limits the presumption to specific evidence that there is reason to believe exists on the defendant's computer. Thus, although the instruction acts like a constructive search, it does not open the defendant's hard drive up to a "general, exploratory rummaging."[178]

There is good reason, moreover, to believe that defendants will fear a missing witness instruction more than contempt. This is so because missing witness instructions have a strong influence on juries.[179] In light of that influence, noncomplying defendants will risk not just the—relatively minor—punishment of contempt, but also the severe penalties that accompany conviction. Thus, defendants who would otherwise refuse to comply with a subpoena may, instead, produce the requested data when confronted with the possibility of a missing witness instruction.[180]

IV. CONCLUSION

Encryption offers a safe haven for cyber thieves, Internet stalkers, and child predators. Without a legal mechanism to compel defendants to decipher the data on protected devices, these criminals will escape prosecution to the detriment of victims and society.

The current strategies invoked by prosecutors to compel defendants to hand over encrypted data are insufficient. Where prosecutors have demanded defendants' passwords, court have quashed their subpoenas.[181] And although prosecutors have successfully demanded the production of the deciphered data itself—at least on one occasion—this procedure risks getting quashed for overbreadth, and thus will not pass Fourth Amendment scrutiny in many circuits.[182] Worse still, both techniques assume that defendants

178. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

179. Robert Stier, for instance, suggests that the instruction is *too* powerful and should be discarded entirely. Robert H. Stier, Jr., *Revisiting the Missing Witness Inference—Quieting the Loud Voice from the Empty Chair*, 44 MD. L. REV. 137, 175-76 (1985).

180. John Leubsdorf, *Evidence Law as a System of Incentives*, 95 IOWA L. REV. 1621, 1653 (2010) (referring to the missing witness instruction as a deterrent to bad conduct).

181. *See generally* United States v. Kirschner, No. 09-MC-50872, 2010 WL 1257355 (E.D. Mich. Mar. 30, 2010).

182. *See generally* United States v. McDonald, No. 10-5150, 2011 WL 3805759, at *2 n.* (4th Cir. Aug. 30, 2011).

will comply with court orders and hand over data that will almost certainly result in convictions and decades of imprisonment.

One approach that avoids all of these dangers is for courts to issue subpoenas for the deciphered data with a warrants that specify what and how to search. If the defendant refuses to produce the deciphered data, the court can hold him in contempt.

However, this too, is incomplete. Warrants and subpoenas are some of the useful tools by which to ask defendants to decipher their protected data, but they are not fail safe. On the contrary, defendants may well prefer contempt to compliance, where handing over protected data almost certainly will result in a lengthy prison sentence.

Ultimately, the necessary legal mechanism that allows fact-finders to look into protected data is a missing evidence instruction; if the combination of a warrant, a subpoena, and contempt cannot induce a defendant to decrypt his data, the court must issue an instruction that the fact-finder may presume the missing data to be incriminating. Such an instruction does not open a defendant's computer or electronic device to search, and does not compel him to provide incriminating testimony. Nevertheless, by doing so, the legal system will defeat a criminal's technological advantage and offer justice to his victims.