Hofstra Law Review

Volume 47 | Issue 3 Article 9

3-1-2019

Search Warrants in the Digital Age

Yuval Simchi-Levi

SEARCH WARRANTS IN THE DIGITAL AGE

*Yuval Simchi-Levi**

I. INTRODUCTION

Digital devices and social media are a major part of American society, given the increasing use of "smart" phones. Chief Justice John Roberts observed that such cell phones are so prevalent in society that "the proverbial visitor from Mars [would] conclude that they were an important feature of human anatomy."[1] One study estimated that "seven-in-ten Americans use social media to connect with one another . . . ."[2] This is not surprising considering that in 2016, eighty-one percent of all cell phones in the United States were smartphones.[3]

Given the ubiquity of social media and digital storage devices[4] in American society, criminals, witnesses, and victims are likely to have social media accounts as well as cell phones. It should be obvious that today, digital storage devices and social media accounts contain a trove of evidence necessary to investigate and prosecute almost any crime. Whenever there is a mass shooting in the United States, it is almost reflexive for law enforcement and the media simply to look at the public postings on the perpetrator's social media to determine the motive for the tragedy.[5] As one journalist wrote, social media is often the "best way

---

* Yuval Simchi-Levi is an Assistant District Attorney in the New York County District Attorney's Office. The views expressed in this Article are his own. The Author wishes to thank Timothy C. Stone for his valuable comments and insight.

1. Riley v. California, 573 U.S. 373, 385 (2014).

2. *Social Media Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/social-media.

3. Tessa Jolls & Michele Johnsen, *Media Literacy: A Foundational Skill for Democracy in the 21st Century*, 69 HASTINGS L.J. 1379, 1404 (2018).

4. In this Article, I refer to digital storage devices in a broad sense to refer to devices that contain digital evidence, such as cell phones, computers, laptops, iPads, and flash drives. *See, e.g.*, Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH. L. REV. 1, 2 n.1, 12 (2015).

5. Jonathan Mahler & Julie Turkewitz, *Ex-Soldier with a Troubled Past and an Interest in Black Power Groups*, N.Y. TIMES, July 9, 2016, at A13, https://www.nytimes.com/

to find the story behind the story" because "[p]eople reveal themselves" on social media.[6] In 2013, a survey of law enforcement officials found that over eighty percent of those surveyed reported solving crimes with the aid of social media.[7] In a study from 2010, eighty-one percent of matrimonial attorneys surveyed stated that they had used evidence from social media in their cases.[8] Specifically, sixty-six percent of lawyers reported that they used evidence from Facebook.[9]

In today's world, digital data stored on cell phones and social media accounts provide additional evidence even in the most basic of criminal cases. For instance, in a common assault case, the perpetrator, victim, and witnesses may upload a video or photographs of the actual fight and subsequent injuries, as well as comment on the fight on social media. In a case where the police have stopped a car and a person inside the vehicle is found with a large amount of drugs, a search warrant of that person's cell phone may reveal—through text messages—that the person works for a drug-trafficking organization and perhaps even videos of the person weighing drugs. In a shooting case in which the perpetrator is arrested a few days later and claims he was elsewhere at the time of the crime, his social media IP logins can show that he was not where he claimed to be during the shooting. In the case of simple possession of a stolen credit card, a social media and iCloud account search warrant can show that the person with the stolen credit card was buying stolen credit cards from friends who were, in turn, downloading those financial accounts from the dark web. In any case where two criminals are accused of acting-in-concert, a cursory examination of either person's

---

2016/07/09/us/suspect-in-dallas-attack-had-interest-in-black-power-groups.html; *see also* Howard Cohen, *At Least 11 Dead After Shooter Enters Pittsburgh Synagogue and Said 'All Jews Must Die,' Report Says*, MIAMI HERALD (Oct. 27, 2018, 11:33 AM), https://www.miamiherald.com/news/nation-world/national/article220729270.html ("As news broke of the shooting and subsequent arrest, the suspect's social media accounts revealed a history of anti-Semitic posts.").

6. Kevin Roose, *Searching Social Media for Clues About Violent Crimes*, N.Y. TIMES, Nov. 7, 2018, at A2, https://www.nytimes.com/2018/11/07/reader-center/synagogue-shooting-social-media.html.

7. *See, e.g.*, Bruce Wright, *Police Expand Social Media Reach to Help Solve Cases, Fight Crime*, BOS. GLOBE (May 5, 2014), https://www.boston.com/news/innovation/2014/05/05/police-expand-social-media-reach-to-help-solve-cases-fight-crime.

8. Zoe Rosenthal, Note, *"Sharing" with the Court: The Discoverability of Private Social Media Accounts in Civil Litigation*, 25 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 227, 229 (2014); *see, e.g.*, Higgins v. Koch Dev. Corp., No. 3:11-cv-81-RLY-WGH, 2013 WL 3366278, at *1-3 (S.D. Ind. July 5, 2013) (allowing defendant to discover private Facebook information in a negligence action where plaintiffs were allegedly burned by higher-than-intended levels of acid in the water of an attraction at a theme park); Howell v. Buckeye Ranch Inc., No. 2:11-cv-1014, 2012 WL 5265170, at *1 (S.D. Ohio Oct. 1, 2012) (holding that private social media information was discoverable in an employment discrimination case where the plaintiff accused male supervisors and co-workers of making sexual comments and touching her inappropriately).

9. Rosenthal, *supra* note 8, at 230.

social media account may uncover photographs of the two individuals together, demonstrating unequivocally that they knew one another. And, most critically, evidence exonerating individuals accused of crimes may be located in their social media accounts and cell phones as well.

Despite the pervasiveness of electronic evidence, courts are still trying to resolve several significant questions in this context that directly impact criminal investigations.[10] For instance, as to social media accounts, some courts have ruled that the government should be limited in what it can search.[11] As to both digital storage devices and social media accounts, it is unresolved what law enforcement officials should do when they execute search warrants on these devices or social media accounts and in turn encounter evidence of unrelated crimes.[12]

This Article argues that, although some courts distinguish between the scope of digital storage device search warrants and social media search warrants, the same analysis should apply to *all* electronically stored evidence.[13] This Article further contends that when searches of digital storage devices and social media accounts are executed in a reasonable manner and in accordance with the search, the plain-view doctrine should apply.[14]

This Article proceeds as follows: In Part II, the legal requirements for searching cell phones and social media accounts are explained.[15] In Part III, the practicality of obtaining a search warrant for cell phones and social media accounts is described.[16] Part IV explains why digital storage devices and social media accounts should be treated similarly.[17] Part V analyzes how the plain-view doctrine applies to digital evidence.[18] Part VI provides an account for how a search into social media accounts and digital storage devices proposed in this Article fits squarely into well-established Fourth Amendment analysis.[19]

---

10. *See* Justin P. Murphy & Adrian Fontecilla, *Social Media in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, RICH. J. L. & TECH., 2013, at 1, 14.

11. Bland v. Roberts, 730 F.3d 368, 385, 388 (4th Cir. 2013) (holding that both "likes" and comments on Facebook constitute protected First Amendment speech); Palmieri v. United States, 72 F. Supp. 3d 191, 210 (D.D.C. 2014) (holding that once Facebook information was voluntarily shared with a "friend," including a known government agent, the account holder had no reasonable expectation of privacy in the data).

12. *See* Murphy & Fontecilla, *supra* note 10, at 10-11.

13. *See infra* Part IV.

14. *See infra* Parts IV–V.

15. *See infra* Part II.

16. *See infra* Part III.

17. *See infra* Part IV.

18. *See infra* Part V.

19. *See infra* Part VI.

II. SEARCH WARRANT REQUIREMENTS FOR CELL PHONES AND SOCIAL MEDIA ACCOUNTS

The Fourth Amendment of the United States Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[20] "[A] warrant may not be issued unless probable cause is properly established."[21] Further, the scope of the search warrant must be set out with particularity, meaning that the warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized."[22] This prevents "general searches" and limits "the discretion of the officer executing the warrant."[23] Relatedly, "[a] warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material."[24] Although an "infirmity due to overbreadth does not doom the entire warrant," it requires the suppression of evidence beyond its valid portions.[25]

A person can challenge a search only when his own Fourth Amendment rights have been violated.[26] There is a two-part test to make that determination: (1) whether a person has exhibited an actual subjective expectation of privacy; and (2) whether that person's subjective expectation of privacy, when viewed objectively, is "justifiable" under the circumstances.[27]

For most of the history of the United States, Fourth Amendment jurisprudence was focused on "common-law trespass," inquiring whether the government could physically intrude upon constitutionally protected areas.[28] However, the U.S. Supreme Court has clarified that the Fourth Amendment does not simply protect property rights, but

20. U.S. CONST. amend. IV.

21. Kentucky v. King, 563 U.S. 452, 459 (2011); *see also* Payton v. New York, 445 U.S. 573, 584 (1980).

22. U.S. CONST. amend. IV; *King*, 563 U.S. at 459; *see also Payton*, 445 U.S. at 585.

23. United States v. Blake, 868 F.3d 960, 973 (11th Cir. 2017); Cassady v. Goering, 567 F.3d 628, 635 (10th Cir. 2009) (citing U.S. CONST. amend. IV); *see* United States v. Mankani, 738 F.2d 538, 546 (2d Cir. 1984).

24. United States v. Ulbricht, 858 F.3d 71, 102 (2d Cir. 2016).

25. United States v. Lowry, No. 16-4139, 2017 U.S. App. LEXIS 21346, at *5 (6th Cir. Oct. 24, 2017) (quoting United States v. Greene, 250 F.3d 471, 477 (6th Cir. 2001)); *see also* United States v. Flores, 802 F.3d 1028, 1045-46 (9th Cir. 2015) (quoting United States v. Gomez-Soto, 723 F.2d 649, 654 (9th Cir. 1984)).

26. United States v. Salvucci, 448 U.S. 83, 85 (1980).

27. Smith v. Maryland, 442 U.S. 735, 740 (1979) (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

28. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting United States v. Jones, 565 U.S. 400, 405, 406 n.3 (2012)).

instead protects people.[29] Thus, a warrant supported by probable cause is required whenever the government seeks to search an item that a person has tried to make private, and when that privacy expectation is one that society recognizes to be reasonable.[30]

In *Riley v. California*,[31] the U.S. Supreme Court recognized that people have a reasonable expectation of privacy in their cell phones and corresponding digital data, given that these devices and remote servers contain "the privacies of life."[32] The Court observed that cell phones are essentially minicomputers with immense storage capacities whose data is not even connected to the actual cell phone device, but to a remote server called a "cloud."[33] In that same decision, the Court noted that within cell phones and associated digital data are applications that contain "detailed information about all aspects of a person's life."[34]

By contrast, whether a person has a reasonable expectation of privacy in his social media account depends on whether he made some effort to keep the information in his account private.[35] This is because a social media user can set his account to be available publicly or to be completely private. A Facebook user, for example, can share his profile only with "friends," with "friends of friends," or with the public at large.[36] "When a social media user disseminates his postings and information to the public, [these postings] are not protected by the Fourth Amendment" because anyone can view them; thus, a search warrant is not necessary to seize those messages.[37] On the other hand,

29. *Id.* (quoting *Katz*, 389 U.S. at 351).

30. *Id.* (citing *Smith*, 442 U.S. at 740).

31. 573 U.S. 373 (2014).

32. *Id.* at 403 (citing Boyd v. United States, 116 U.S. 616, 630 (1886)).

33. *Id.* at 393-94, 396-97.

34. *Id.* at 396.

35. *See, e.g.*, *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 146 (E.D.N.Y. 2013).

36. United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012); *see also* United States v. Khan, No. 15-cr-00286, 2017 WL 2362572, at *8 (N.D. Ill. May 31, 2017); United States v. Adkinson, No. 4:15-cr-00025-TWP-VTW, 2017 U.S. Dist. LEXIS 54104, at *15 (S.D. Ind. Apr. 7, 2017).

37. *Meregildo*, 883 F. Supp. 2d at 525; *see also* Perry v. Montgomery, No. CV-16-03730-FMO (KES), 2017 U.S. Dist. LEXIS 95077, at *35 (C.D. Cal. June 5, 2017); United States v. Gatson, No. 13-705, 2014 WL 7182275, at *22-23 (D.N.J. Dec. 16, 2014); Palmieri v. United States, 72 F. Supp. 3d 191, 210 (D.D.C. 2014) (holding that the defendant did not have a reasonable expectation of privacy in the information he made available to "friends" on his Facebook page); Rosario v. Clark Cty. Sch. Dist., No. 2:13-cv-362 JCM (PAL), 2013 WL 3679375, at *5-7 (D. Nev. July 3, 2013) ("When a person tweets on Twitter to his or her friends, that person takes the risk that the friend will turn the information over to the government."); Juror No. One v. Superior Court, 142 Cal. Rptr. 3d 151, 159 (Cal. Ct. App. 2012); Everett v. State, 186 A.3d 1224, 1230 (Del. 2018) ("[A] Facebook user does not have a reasonable expectation that information that he shares online with his 'friends' will not be revealed by them.").

when someone posts using a more secure privacy setting on social media, this reflects an intent to keep information private, and so that information may be constitutionally protected.[38] One court even noted that private Facebook messages are "inherently private" because they "are not readily accessible to the general public."[39]

III. OBTAINING A SEARCH WARRANT TO SEARCH A CELL PHONE OR SOCIAL MEDIA ACCOUNT

To obtain a search warrant for a social media account or a digital storage device, the government must establish a "specific and concrete" nexus between what is being searched and criminal activity.[40] Given the multi-functional uses and ubiquity of social media, it should not be difficult for the government to articulate why a social media search warrant is necessary.[41] Social media provides crucial evidence in criminal cases because, by its very nature, it connects people to each other by allowing connected parties to view private postings and to send and receive private messages, including videos and photographs.[42] For instance, in *United States v. Arnold*, a motion to controvert a search warrant for over three dozen Facebook accounts was denied.[43] The government argued that there was a nexus between the accounts and criminal activity because, inter alia, the account users had publicly posted photographs of themselves wearing gang clothing, statements acknowledging the existence of the gang, and references to individuals by their gang names.[44] Naturally, the court found that such evidence

38. *Meregildo*, 883 F. Supp. 2d at 525; *see also* Commonwealth v. Jenkins, No. 229 EDA 2015, 2016 Pa. Super. Unpub. LEXIS 780, at *5 n.4 (Pa. Super. Ct. Mar. 8, 2016).

39. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010); *see also* R.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012) (quoting *Crispin*, 717 F. Supp. 2d at 991).

40. United States v. Johnson, 725 F. App'x 393, 402-03 (6th Cir. 2018); United States v. Whitt, No. 1:17cr060, 2018 WL 447586, at *1 (S.D. Ohio Jan. 17, 2018) (citing United States v. Brown, 828 F.3d 375, 382 (6th Cir. 2016)).

41. *See, e.g.*, United States v. Arnold, No. 15-20652, 2017 U.S. Dist. LEXIS 148120, at *4, *7, *10 (E.D. Mich. Sept. 13, 2017) (denying motion to suppress Facebook evidence in drug conspiracy case where affidavit cited information from defendants' publicly available profile including a post accusing another individual of being a "federal informant"); United States v. Yelizarov, No. MJG-16-0309, 2017 WL 3022927, at *1-2 (D. Md. July 17, 2017) (denying motion to suppress Facebook evidence where the affidavit cited information from suspect's publicly available Facebook profile and a statement that "[d]efendant has a history of boasting about his crimes to others"); United States v. Ortiz-Salazar, No. 4:13CR67, 2015 WL 2089366, at *1-4 (E.D. Tex. May 4, 2015) (recommending denial of motion to suppress Facebook evidence where the detective cited information gleaned from defendant's publicly available Facebook profile).

42. *Arnold*, 2017 U.S. Dist. LEXIS 148120, at *9-10.

43. *Id.* at *3.

44. *Id.* at *9-10.

could be used to establish that all the individuals were involved in a criminal enterprise.[45]

Likewise, it is not difficult to draw a nexus between a cell phone and allegations of criminal activity. As the Supreme Court observed, "[c]ell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information . . . ."[46] The Nebraska Supreme Court found that because a defendant worked with at least one other person in committing a series of crimes, it was reasonable to infer that the defendant's cell phone "was used to communicate with others" before, during, and after committing the crimes.[47] Similarly, in drug cases, courts have found a sufficient nexus between cell phones and criminal activity by virtue of the fact that, as a general matter, drug traffickers communicate about their businesses through cell phones.[48]

IV. TREATING SEARCH WARRANTS FOR DIGITAL STORAGE DEVICES AND SOCIAL MEDIA ACCOUNTS SIMILARLY

As the Supreme Court observed, cell phones are essentially "minicomputers" that happen to be used as telephones.[49] Thus, search warrants for cell phones should be written and executed as if the devices are computers. As Professor Orin S. Kerr observed, although the Supreme Court in *Riley* was dealing with cases in which cell phones had been searched, its analysis was "really about computers generally . . . ."[50] What this means is that courts should analyze digital storage devices—whether they be cell phones, tablets, or actual computers—in a similar manner. Consequently, when courts analyze searches of files on cell phone devices, courts should not think of them as items in which files are discretely stored like a filing cabinet. As the Second Circuit observed in *United States v. Ganias*,[51] unlike filing cabinets, files in a digital storage device are not discretely divided amongst each other.[52] Instead,

45. *Id.*

46. Riley v. California, 573 U.S. 373, 385 (2014).

47. State v. Henderson, 854 N.W.2d 616, 632 (Neb. 2014).

48. *See, e.g.*, United States v. Fisher, No. RDB-14-413, 2015 WL 1862329, at *2-3 (D. Md. Apr. 22, 2015); United States v. Herevia, No. RDB-13-639, 2014 WL 4784321, at *8-9 (D. Md. Sept. 23, 2014); United States v. Eiland, No. 04-379 (RCL), 2006 WL 516743, at *11-13 (D.D.C. Mar. 2, 2006).

49. *Riley*, 573 U.S. at 393.

50. Kerr, *supra* note 4, at 10 n.68.

51. 824 F.3d 199 (2d Cir. 2016).

52. *Id.* at 213 (first citing Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. PITT. J. TECH. L. & POL'Y 1, 13 (2007); and then quoting Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 127-

on digital storage devices, files will typically be "fragmented" in various physical locations.[53] In other words, "[b]ecause of the manner in which data is written to the hard drive," files "are stored in multiple locations and in multiple forms . . . ."[54] When analyzing a digital storage device, forensic examiners could discover evidence that a file was deleted, and they could even reconstruct a deleted file with evidence found in an "unallocated" space on a hard drive.[55] Still more complicated, various versions of the same file may exist in different parts of the same drive.[56]

The Second Circuit found, moreover, that forensic examiners may need to examine the entirety of a digital storage device to rebut a defendant's claim that a virus or hack caused a file to appear in the device.[57] To determine that a virus was not on the device, forensic examiners must analyze the entirety of the hard drive.[58] This is significant because even with regard to cell phones, a defendant can argue that photographs, videos, and text messages were placed on his phone by others. A thorough and complete search of the device can rule out this theory by showing, for instance, that the cell phone was never corrupted, or even that the defendant represented that the phone belonged to him throughout the time the phone was used—such as by taking photographs of himself or acknowledging the receipt of a text message.

Courts are divided as to whether to view social media search warrants similarly or differently than warrants for digital data in storage devices. In *United States v. Blake*,[59] the Eleventh Circuit found a search warrant for a Facebook account to be unconstitutional because the warrant requested that Facebook provide "virtually every kind of data that could be found in a social media account."[60] The Eleventh Circuit noted that the government could have limited its request from Facebook to a search of the private messages between those suspected of being involved in the offense, and the court supported limiting the warrant to "the period of time during which [the defendant] was suspected of taking part in the prostitution conspiracy."[61] But in *United States v. Ulbricht*,[62]

---

28 (2011)).

53. *Id.* (quoting Jekot, *supra* note 52, at 13).

54. *Id.* (first quoting Jekot, *supra* note 52, at 13; and then citing Goldfoot, *supra* note 52, at 127-28) (quotation marks omitted).

55. *Id.* at 213-14.

56. *Id.* at 213.

57. *Id.* at 214.

58. *Id.* (quoting Goldfoot, *supra* note 52, at 141).

59. 868 F.3d 960 (11th Cir. 2017).

60. *Id.* at 973-75.

61. *Id.* at 974.

in its review of a search warrant for a laptop, the Second Circuit rejected the defendant's argument that the warrant should have been more specific because "[f]iles and documents can easily be given misleading or coded names . . . ."[63] In rejecting the defendant's challenges to Facebook warrants, the Second Circuit simply stated that it found the Facebook search warrants valid for the same reasons that it found the laptop search warrant valid.[64]

The distinction some courts have drawn between digital storage devices and social media accounts appears to be based on the belief that the government can clearly communicate to the social media company precisely what it needs—and by doing so, receive discrete messages, photographs, videos, etc.[65] The Eleventh Circuit in *Blake* was under the impression that the government could request that Facebook provide certain conversations between the target account and those the government suspected of complicity in the crimes, thereby omitting conversations between the target account and others.[66] But it is not clear why the Eleventh Circuit thought this. Indeed, as the government could have no way of knowing every single account involved in the crimes in that case, it is unclear why the Eleventh Circuit even addressed the matter.

In any event, and for several reasons, the Eleventh Circuit in *Blake* was mistaken in requiring that Facebook only provide a limited response to the target account, and the flaws in the court's reasoning illustrate why the same legal analysis should apply to the scope of search warrants for digital storage devices and social media accounts.[67] First, whereas a digital storage device is typically found on or near a suspect (thereby supporting an inference of possession), a social media account will be identified as belonging to a person because the account name or "handle" is similar to the person's name, the person's photograph is shown on the social media account, or others have claimed the person's social media account. Consequently, the person the government believes is connected with the social media account can argue that it is not her account. To account for this—by establishing that the person had control over the social media account during the time period of the criminal activity—the government must examine an expansive version of the

62. 858 F.3d 71 (2d Cir. 2017).

63. *Id.* at 102.

64. *Id.* at 104.

65. *See Blake*, 868 F.3d at 974 ("[W]hen it comes to Facebook account searches, the government need only send a request with the specific data sought and Facebook will respond with precisely that data.").

66. *Id.*

67. *See id.*

account to determine how often the person identified himself to be the owner of the account and provided identifying information to others, such as telephone numbers, addresses, and photographs.

Second, just like cell phones or other digital storage devices, it is possible for someone to hack into a Facebook account or other social media accounts and send messages as if they are the account holder.[68] The government will thus need to acquire a large scope of the account to show—through IP logins, conversations, postings, etc.—that the suspect not only created the account but also retained control over it.

Third, it will often be difficult for the government to know the exact time that a person began to engage in the criminal activity in question. If someone is suspected of drug dealing, for instance, it will be challenging to pinpoint the exact date when the person began acting in furtherance of that crime. A more expansive search warrant for a social media provider will provide greater insight into how long the person has been engaged in the particular criminal activity that the government is investigating or prosecuting.

Fourth, the social media account may demonstrate that the owner of the account deleted specific incriminating private messages—evidence probative of a guilty mind. To establish that the account owner did not delete innocuous conversations, but rather only inculpatory messages, the government would need access to a significant range of activity on the account.

Finally, the Eleventh Circuit's approach would give Facebook and other social media providers too much discretion in determining the appropriate response to the government's search warrant.[69] Such power could lead to concerns that the social media provider is a state agent, acting as an arm of law enforcement, and that it is not providing a fully responsive return to the warrant. The concern would be multifold, including the fact that the social media provider did not adhere to the search warrant. A comprehensive examination of a target's social media account, consequently, is often necessary to connect the suspect to the account and to obtain a complete sense of the criminal activity.

---

68. *See* Emily Erickson, *Cut Bait or Phish*, CREDIT UNION MGMT., Dec. 1, 2018, at 36, 36 ("It's important to remember that your friends' social media accounts can be hacked, and those hacked accounts can be used to post links to malicious websites."); *see also Oculus CEO is Latest Tech Boss Hacked in Embarrassing Account Takeover*, GUARDIAN (June 30, 2016, 6:24 AM), https://www.theguardian.com/technology/2016/jun/30/oculus-ceo-is-latest-tech-boss-hacked-in-embarrassing-account-takeover.

69. *See Blake*, 868 F.3d at 966-67, 974.

V. PLAIN-VIEW DOCTRINE AS APPLIED TO ELECTRONIC EVIDENCE

Another significant question is what happens when a search of digital storage data or a social media account reveals that a person has engaged in a number of other crimes unrelated to the crimes underpinning the search warrant. This question implicates the "plain-view doctrine," which allows law enforcement to seize an item when: (1) the officer was lawfully in the place from where the seized item was in plain-view, (2) the item's incriminating nature was "immediately apparent," and (3) the officer had "a lawful right of access to the object itself."[70]

Application of this doctrine in the virtual context is a challenging question because of the volume of information through which law enforcement must search through when executing a warrant for a digital storage device or social media account. One court observed that a commercially available digital storage device can hold data "roughly equal to 16 billion thick books."[71] As discussed above, unlike physical objects that can be readily identified, digital storage device files may be manipulated such that files are hidden, disguised, or even deleted.[72] Permitting law enforcement to review every file and message—and then to claim that even those unrelated to the scope of the search warrant but that demonstrate other crimes, fall into the plain-view exception—creates "a serious risk" that all electronic search warrants will become general search warrants, essentially "rendering the Fourth Amendment irrelevant."[73]

The majority of federal courts have taken the position that, as long as the search of digital storage data is "reasonably required to locate the items described in the warrant based on probable cause," unrelated evidence can be seized under the plain-view doctrine.[74] Departing from

70. Horton v. California, 496 U.S. 128, 136-37 (1990) (quotation marks omitted).

71. United States v. Ganias, 824 F.3d 199, 218 (2d Cir. 2016) (quoting Quentin Hardy, *As the Data Deluge Grows, Companies Are Rethinking Storage*, N.Y. TIMES, Mar. 15, 2016, at B3, https://www.nytimes.com/2016/03/15/technology/as-a-data-deluge-grows-companies-rethink-storage.html) (quotation marks omitted).

72. United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010) (citing United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006)); *see also* United States v. Stabile, 633 F.3d 219, 237 (3d Cir. 2011) ("[I]t is clear that because criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity, a broad, expansive search of the hard drive may be required."); *supra* text accompanying notes 52-56.

73. United States v. Galpin, 720 F.3d 436, 447 (2d Cir. 2013) (quoting United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010)) (quotation marks omitted).

74. United States v. Richards, 659 F.3d 527, 538-39 (6th Cir. 2011) (quoting United States v. Burgess, 576 F.3d 1078, 1092 (10th Cir. 2009)) (quotation marks omitted) (adopting a "reasonableness" analysis on a case-by-case basis in analyzing the plain-view doctrine); *see also* United States v. Perez, 712 F. App'x 136, 140 (3d Cir. 2017) (explicitly refusing to adopt a Fourth

this view, in its per curiam decision in *United States v. Comprehensive Drug Testing, Inc.*, the Ninth Circuit explicitly rejected the government's plain-view doctrine argument on the basis that "everything the government chooses to seize will, under this theory, automatically come into plain view."[75] A five-judge concurrence, expressing concern with the government's ability to turn digital storage device warrants into general warrants, suggested that the government should "forswear reliance on the plain view doctrine" whenever seeking a search warrant to examine such a device.[76]

The application of the plain-view doctrine to digital storage devices taken by the majority of circuit courts makes more sense than the Ninth Circuit's seemingly blanket opposition to the plain-view doctrine. The majority's approach is persuasive because it applies the bedrock principle of the Fourth Amendment—reasonableness—to law enforcement's search of large quantities of evidence. A straightforward analysis of the plain-view doctrine under this majority approach demonstrates that both courts and law enforcement can be guided as to what is "reasonable" in this context.

United States v. Carey,[77] on the one hand, illustrates an unreasonable search of digital data.[78] In that case, a detective searched a computer pursuant to a search warrant that authorized him to look for evidence of drug trafficking.[79] At some point, while examining the files, the detective viewed the computer's "JPG" files which contained images he believed to be child pornography.[80] The detective testified that he then downloaded the rest of the JPG files because he thought it contained child pornography, not drugs.[81] The Tenth Circuit suppressed

---

Amendment search doctrine, and applying a "reasonableness" test to evaluate a digital search); *Galpin*, 720 F.3d at 447 ("Once the government has obtained authorization to search the hard drive, the government may claim that the contents of every file it chose to open were in plain view and, therefore, admissible even if they implicate the defendant in a crime not contemplated by the warrant."); *Stabile*, 633 F.3d at 241 n.16 (3d Cir. 2011) (adopting the Seventh Circuit's holding in *Mann*); *Mann*, 592 F.3d at 785 (quoting *Comprehensive Drug Testing, Inc.*, 579 F.3d at 1013 (Callahan, J., concurring in part and dissenting in part)) ("[The best approach is] to allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based case adjudication."); United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010) (applying the plain-view doctrine to a search of a digital storage device); United States v. Walser, 275 F.3d 981, 987 (10th Cir. 2001) (holding that a search was valid under the plain-view doctrine where the search was "reasonable and within the parameters of the search warrant").

75. *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1170-71.
76. *Id.* at 1178 (Kozinski, C.J., concurring).
77. 172 F.3d 1268 (10th Cir. 1999).
78. *Id.* at 1276.
79. *Id.* at 1270.
80. *Id.* at 1271.
81. *Id.* at 1273.

the seized images of child pornography as the result of an unlawful search.[82] The search in *Carey* did not satisfy the plain-view doctrine because, by the detective's admission, he was not looking for drugs in these files but rather child pornography and thus was not guided by the search warrant that authorized him to look only for drugs.[83]

By contrast, in *United States v. Walser*,[84] the same court affirmed the denial of a motion to suppress where it found a plain-view search reasonable.[85] In that case, as the law enforcement agent lawfully searched a computer for evidence of drug trafficking, he noticed images of child pornography.[86] The agent stopped his search and obtained another search warrant that allowed him to search the computer for child pornography.[87] The Tenth Circuit made clear that the law enforcement agent had searched the computer reasonably before obtaining the subsequent search warrant because he had been looking for evidence of drug dealing.[88]

United States v. Mann[89] further illustrates the contours of reasonableness in this area.[90] *Mann* involved a search of a computer for evidence that the defendant had videotaped women in a locker room.[91] The detective executed the search by running a software program that indexed the data on the computer to reveal the exact quantity of images, videos, and documents.[92] When the detective reviewed this material on the computer, he saw images of child pornography.[93] Based on the detective's testimony, the district court found that as the detective perused the computer files and encountered child pornography, "he never abandoned his search for evidence of voyeurism" and looked only for child pornography.[94] The Seventh Circuit upheld this search as reasonable and within the scope of the warrant's authorization because

82. *Id.* at 1276.
83. *Id.* at 1273.
84. 275 F.3d 981 (10th Cir. 2001).
85. *Id.* at 983, 987.
86. *Id.* at 984-85.
87. *Id.* at 985, 987; *see also id.* at 986 ("Because computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer.").
88. *Id.* at 987.
89. 592 F.3d 779 (7th Cir. 2010).
90. *See id.* at 780-82.
91. *Id.* at 780-81.
92. *Id.* at 781.
93. *Id.*
94. *Id.* at 781-82.

the discovery of child pornography transpired while law enforcement was "conducting a systematic search for evidence of voyeurism . . . ."[95]

The plain-view analysis adopted by the majority of federal courts should apply to all digital devices and social media accounts. Just like computers, when law enforcement authorities examine the contents of a cell phone or social media account, they are opening a Pandora's box of "intermingl[ed]" information relating to an individual.[96] So long as evidence of unrelated crimes is found while executing the search warrant that provided access to the digital device or social media account, that evidence should be admissible.

Ultimately, the best practice is that law enforcement—upon observing evidence of other crimes in a cell phone or a social media account—apply for an additional search warrant that incorporates the newly-encountered crimes.[97] The new warrant will provide law enforcement with the ability to look specifically for evidence of the new crimes and will circumvent litigation about whether the initial digital device or social media search warrant was merely an improper pretext to violate the defendant's right to privacy.

VI. CONCLUSION

When the Fourth Amendment was written, there was obviously no way to envision the world that we live in today with the advent of digital devices and social media. But no doubt exists that the Fourth Amendment applies in this context because its "basic purpose . . . is to safeguard the privacy and security of individuals against arbitrary invasions by government officials."[98] In today's world, some of our most private information is contained in our cell phones, tablets, computers, and social media accounts.

With that said, the "touchstone" of Fourth Amendment analysis has always been reasonableness.[99] The proposals in this paper—namely, that the government should be allowed to have broad access to a social media

95. *Id.* at 786.

96. United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) (quotation marks omitted).

97. *See Mann*, 592 F.3d at 786 ("Although we now hold that [the detective's] actions were within the scope of the warrant, we emphasize that his failure to stop his search and request a separate warrant for child pornography is troubling."); *see also* United States v. Burgess, 576 F.3d 1078, 1094-95 (10th Cir. 2009) ("[A]s our cases seem to require, [the law enforcement agent] immediately closed the gallery view when he observed a possible criminal violation outside the scope of the warrant's search authorization and did not renew the search until he obtained a new warrant.").

98. Camara v. Mun. Court of S.F., 387 U.S. 523, 528 (1967); *see also* Riley v. California, 573 U.S. 373, 403 (2014).

99. Birchfield v. North Dakota, 136 S. Ct. 2160, 2186 (2016).

account that it has probable cause to search and that the government should be able to seize evidence found in plain view in digital storage devices and social media accounts—are premised on reasonableness.[100] Moreover, these proposals provide law enforcement with clear guidance as to how to search digital storage devices as well as social media accounts.[101] Given the ubiquity of digital data, as well as the large amounts of data law enforcement is required to peruse when executing search warrants, such reasonable guidance is clearly necessary to aid law enforcement as well as the courts.

100. *See supra* Parts IV–V.
101. *See supra* Parts IV–V.

***