# REGULATING SEARCH WARRANT EXECUTION PROCEDURE FOR STORED ELECTRONIC COMMUNICATIONS

*Sara J. Dennis**

*Electronic communication services, from email, to social media, to messaging applications, have not only dramatically changed daily life but have also had a profound impact on criminal investigations and procedure. The often large volume of electronically stored information has led to a two-step process for search warrant execution, codified in Federal Criminal Procedure Rule 41. When conducting a search pursuant to Rule 41, law enforcement often retains both responsive items—materials that fall within the scope of the warrant—and nonresponsive materials—intermingled items that can be searched, but ultimately exceed the scope of the warrant. This possession of nonresponsive material creates a tension between the account holder's privacy interests and the government's ability to conduct an effective search.*

*Courts and scholars have implemented and proposed a range of approaches for search warrant execution in light of concerns about sweeping general searches and the practicalities of searching electronically stored information. This Note examines these approaches to regulate search warrant execution procedure in the context of stored electronic communications. This Note also discusses the strengths and shortcomings of these various mechanisms and concludes that Rule 41 should be amended to provide standards for the retention and use of nonresponsive material.*

INTRODUCTION ..... 2994

I. OBTAINING AND EXECUTING SEARCH WARRANTS FOR STORED ELECTRONIC COMMUNICATIONS ..... 2997

*A. The Stored Communications Act and Federal Criminal Procedure Rule 41* ..... 2997

*B. "Step Two" Execution: The Reasonableness Touchstone for Valid Execution Under the Fourth Amendment* ..... 3000

* J.D. Candidate, 2019, Fordham University School of Law; B.A., 2012, Brandeis University. Thank you to Professor Deborah Denno and the *Fordham Law Review* editors and staff for their invaluable advice and assistance. I would also like to thank my family and friends for their encouragement and support.

II. APPROACHES TO EXECUTING THE REVIEW OF ELECTRONICALLY STORED INFORMATION ..... 3001
*A. Ex Ante Orders Regulating Search Methodology and Execution* ..... 3001
1. Time Limits to Complete "Second-Step" Search of Materials ..... 3002
2. Deletion and Return of Nonresponsive Materials ..... 3004
3. Mandated Protocol for How the Search Must Be Completed ..... 3005
*B. Ex Post Rulings Shaping the Boundaries of Reasonableness in the Digital Context* ..... 3010
1. Establishing a Reasonable Time to Execute the Search ..... 3011
2. Considerations in Limiting the Scope of the Review or Deploying of Search Protocols ..... 3014
3. Use of Crime-Type Designations, Date Restrictions, or Data-Type Specifications to Evaluate Particularity ..... 3015
*C. The Plain View Doctrine and Regulating Use of Materials Outside the Scope of the Warrant* ..... 3017
*D. Policy Suggestions and Proposed Amendments to Rule 41* ..... 3018
III. LIMITATIONS OF AD HOC ELECTRONIC COMMUNICATIONS SEARCH WARRANT REGULATION AND PROPOSED MODIFICATION OF RULE 41 ..... 3020
*A. Limitations of the Warrant Regulation and Evaluation Status Quo* ..... 3021
*B. Modifying Rule 41 to Impose Retention Restrictions and Use-Based Procedures Instead of Execution Deadlines or Protocol Orders* ..... 3022
CONCLUSION ..... 3024
APPENDIX A ..... 3025
APPENDIX B ..... 3027
APPENDIX C ..... 3029
APPENDIX D ..... 3031

## INTRODUCTION

With the widespread use of electronic communication in personal and professional life, records maintained by electronic service providers have become a valuable source of evidence in criminal investigations and are requested in high volumes.[1] Whether in the form of email, social media, or

1. Google and Microsoft alone have produced data in response to tens of thousands of law enforcement requests from January 2014 through June 2017. *Law Enforcement Requests Report*, MICROSOFT, https://www.microsoft.com/en-us/about/corporate-responsibility/lerr [https://perma.cc/A23V-RNWE] (last visited Apr. 13, 2018); *Transparency Report*, GOOGLE, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=

mobile messages sent through downloadable applications, electronic communications can possess highly relevant evidence of criminal acts, from shedding light on a person's mens rea[2] to detailing the scope and manner of criminal conduct.[3] While electronic communications[4] are valuable sources of information, some courts and scholars have expressed concern that the procedure for searching electronic materials can turn search warrants for such information into de facto general warrants,[5] which undermines the protections of the Fourth Amendment.[6]

Compared to searches of physical locations, search warrants for electronic communications can, and frequently do, yield higher volumes of records, which then require a lengthier review process.[7] As a result, the Federal Rules of Criminal Procedure were amended to allow law enforcement to obtain a larger set of intermingled, potentially pertinent electronic materials, and subsequently search those records for items that actually fall within the scope of the warrant.[8] But this process creates a situation where the government possesses innocuous items in addition to evidence of a crime.[9] The product of Rule 41—law enforcement's ability to retain materials that are beyond the scope of a warrant—creates a conflict between practical necessities and privacy interests.

This tension is highlighted in one case where a magistrate judge considered the government's application to search a Facebook account that belonged to an individual who perpetrated a mass shooting at a military facility.[10] During

---

series:requests,accounts;authority:US&lu=user_requests_report_period [https://perma.cc/Q2PS-6SGV] (last visited Apr. 13, 2018).

2. *See, e.g.*, *In re* Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis That Is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 3 (D.D.C. 2013) (explaining the government's belief that Facebook posts would reveal information about the shooter's motivations).

3. *See, e.g.*, United States v. Kanodia, No. 15-10131-NMG, 2016 WL 3166370, at *1 (D. Mass. June 6, 2016) (involving email communications that contained wire instructions for proceeds connected to a securities fraud conspiracy).

4. This Note focuses on internet-based communication services, such as email, social media, and messaging applications, where the provider stores its customers' records. *See infra* notes 29–31 and accompanying text.

5. *See, e.g.*, *In re Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d at 8 (stating that electronic searches require the creation of minimization procedures in order to prevent them from functioning as general warrants).

6. *See* United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013) ("The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of general warrants.'" (quoting Payton v. New York, 445 U.S. 573, 583 (1980))). The general warrants involved unconstrained searches amounting to "rummag[ing] at will." *Id.* (quoting Arizona v. Gant, 556 U.S. 332, 345 (2009)).

7. *See* FED. R. CRIM. P. 41 advisory committee's notes to 2009 amendment (stating that allowing subsequent off-site review of electronically stored information is a practical necessity given the frequently large volume of stored materials).

8. *Id.*

9. *See id.* (acknowledging that the government could possess nonresponsive materials by stating that the determination of which documents fall within the scope of a warrant can be made later).

10. *See In re Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d at 1; *see also* Michael D. Shear & Michael S. Schmidt, *Gunman and 12 Victims Killed in*

the investigation, the government learned that the shooter had posted "mini-rants" on his Facebook page.[11] The government believed that access to the shooter's account would yield information indicating his motive for committing the crime and whether any coconspirators were involved in the plan.[12] While Magistrate Judge John M. Facciola recognized the importance for law enforcement to search these records accurately and effectively, he was also concerned with the privacy interests of anyone who might have communicated with the shooter during the specified date range.[13]

Search and seizure law has always sought to square these interests in a just manner. Yet courts still struggle to find the appropriate balance and procedural consistency in the context of electronically stored information (ESI).[14] The current ambiguity, paradoxically, can undermine both procedural and privacy interests by complicating reliance on ESI evidence in criminal prosecutions and threatening the privacy of account holders (and those with whom they communicate).[15] These balancing questions affect a wide array of cases as electronic communications evidence has been used to investigate occurrences of securities fraud,[16] child sex trafficking,[17] identity theft,[18] drug trafficking,[19] wire fraud,[20] and intentional damage to a protected computer,[21] among various other crimes.

This Note explores the gaps in the law governing reasonable search and seizure of stored electronic communications.[22] Part I provides background on search warrant procedure pertaining to ESI and the adaptations in criminal procedure in the digital age. Part II details the ex ante and ex post measures

---

*Shooting at D.C. Navy Yard*, N.Y. TIMES (Sept. 16, 2013), http://www.nytimes.com/2013/09/17/us/shooting-reported-at-washington-navy-yard.html [https://perma.cc/2J2R-EUJY]. For the government's proposed search warrant for Aaron Alexis's Facebook account, see *infra* Appendix A.

11. *In re Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d at 3.

12. *Id.* at 7.

13. *Id.* at 6. In light of these concerns, Judge Facciola issued an order limiting the information Facebook could provide to the government. *See infra* Appendix B.

14. *See infra* Part II.

15. *See infra* Part II (outlining the various mechanisms of regulation and review imposed by judges). Such range in approach hinders the ability to anticipate how the execution of a warrant will be analyzed. *See supra* notes 10–12 and accompanying text.

16. *See, e.g.*, United States v. Kanodia, No. 15-10131-NMG, 2016 WL 3166370, at *1 (D. Mass. June 6, 2016).

17. *See, e.g.*, United States v. Blake, 868 F.3d 960, 966 (11th Cir. 2017).

18. *See, e.g.*, *In re* Search of Info. Associated with Fifteen Email Addresses Stored at Premises Owned, Maintained, Controlled or Operated by 1&1 Media, Inc., Google, Inc., Microsoft Corp. & Yahoo! Inc., No. 2:17-CM-3152-WC, 2017 WL 4322826, at *1 (M.D. Ala. Sept. 28, 2017).

19. *See, e.g.*, United States v. Ulbricht, 858 F.3d 71, 82 (2d Cir. 2017).

20. *See, e.g.*, United States v. Patel, No. 16-cr-798 (KBF), 2017 WL 3394607, at *1 (S.D.N.Y. Aug. 8, 2017).

21. *See, e.g.*, United States v. Shah, No. 5:13-CR-328-FL, 2015 WL 72118, at *1 (E.D.N.C. Jan. 6, 2015).

22. Specifically, this Note addresses the execution of search warrants obtained with respect to 18 U.S.C. § 2703(a)–(b). It will not analyze procedures where records are obtained without a search warrant, as permitted under 18 U.S.C. § 2703(d).

that courts have implemented in the absence of clear regulations or precedent on searches in this context. Part II also describes additional procedures scholars have proposed. Finally, Part III recommends amending Federal Criminal Procedure Rule 41 to guide the proper handling of nonresponsive material.[23]

## I. OBTAINING AND EXECUTING SEARCH WARRANTS FOR STORED ELECTRONIC COMMUNICATIONS

With the rise of internet-based services that maintain and store user content on their own servers, law enforcement agencies frequently obtain records directly from electronic communications service providers rather than from the users themselves.[24] This Part describes the authorization and procedure to obtain a search warrant for ESI. Part I.A discusses how the government obtains information from an electronic communications service provider under the Stored Communications Act and the "two-step" process for seizing and searching ESI under Federal Criminal Procedure Rule 41. Part I.B then describes the constitutional baseline for the "second-step" ESI search and overarching reasonableness requirement in search warrant execution.

### *A. The Stored Communications Act and Federal Criminal Procedure Rule 41*

Since the 1980s, Congress has attempted to adapt to the proliferation of digital communication and law enforcement's use of related records in criminal investigations. The Stored Communications Act (SCA),[25] enacted in 1986, sought to both protect the privacy of electronic communications and recognize a mechanism for law enforcement to obtain such content lawfully.[26] The SCA specifically empowers a governmental entity to "require a provider of remote computing service to disclose the contents of any wire or electronic communication . . . held or maintained on that service" by obtaining a warrant conforming to the Federal Rules of Criminal Procedure or applicable state law.[27] Unlike a traditional premises search warrant, executing an SCA warrant does not require law enforcement personnel to be present for the initial gathering of communications—instead,

23. The term "nonresponsive" is used throughout this Note to refer to materials that fall beyond a search warrant's specified scope of items that may be seized.

24. *See* 18 U.S.C. § 2703 (2012).

25. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1861 (codified as amended at 18 U.S.C. §§ 2701–2712 (2012)).

26. *See* S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 (commenting that a person's privacy interest should not change when information is copied, maintained, and stored electronically and reiterating the need to balance privacy interests with law enforcement needs).

27. 18 U.S.C. § 2703(b). While the SCA also permits seizure of certain evidence without a warrant through a court order under subsection (d) of this Section, this Note only addresses electronic communications obtained pursuant to search warrants.

the service provider may turn over copies of the described items from its servers.[28]

This provision covers a range of electronic service providers, including email providers,[29] social media companies,[30] and messaging application services.[31] While the availability of specific content depends on the provider and the type of electronic account,[32] a warrant generally specifies the account from which communications are sought and may also include a pertinent date range or specific types of data.[33] For example, in the case of a Facebook account, a warrant description may include any public posts made to a page and any private messages, and it may exclude photos of the subject posted by another user.[34]

---

28. *See, e.g.*, United States v. Patel, No. 16-cr-798 (KBF), 2017 WL 3394607, at *1 (S.D.N.Y. Aug. 8, 2017); *In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014).

29. *See, e.g.*, *Legal Process for User Data Requests FAQ*, GOOGLE, https://support.google.com/transparencyreport/answer/7381738?hl=en [https://perma.cc/8RKG-DGEU] (last visited Apr. 13, 2018).

30. *See, e.g.*, *Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines [https://perma.cc/NTM4-3F9P] (last visited Apr. 13, 2018) ("A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, timeline posts, and location information.").

31. *See, e.g.*, *Snapchat Law Enforcement Guide*, SNAPCHAT 3 (Oct. 11, 2016), https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf [https://perma.cc/E75B-3KTR] (acknowledging that Snapchat's ability to provide user information is dictated by 18 U.S.C. §§ 2701–2712); *see also* United States v. Price, No. 17-CR-301 (NGG), 2017 WL 4838307, at *8 (E.D.N.Y. Oct. 23, 2017) (rejecting the defendant's motion to suppress a search warrant for the defendant's Snapchat account).

32. *See, e.g.*, *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php [https://perma.cc/4B8W-G4DG] (last visited Apr. 13, 2018) (listing the types of information Facebook collects on account holders, including the account holder's communications, content others provide to or about the account holder, financial transactions, and device information); *Guidelines for Law Enforcement*, TWITTER, https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#3 [https://perma.cc/XM2M-A4LD] (last visited Apr. 13, 2018) (describing the account content available pursuant to an SCA warrant and data retention limitations); *Legal Process for User Data Requests FAQs*, *supra* note 29 (listing the content available in response to search warrants for Gmail, YouTube, Google Voice, and Blogger products); *Legal Process Guidelines*, APPLE 7–12 (Mar. 23, 2018), https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/JQQ6-B9ST] (delineating the customer and account information Apple maintains, including content that may be available in an iCloud account).

33. *See, e.g.*, *In re* Search of Info. Associated with Fifteen Email Addresses Stored at Premises Owned, Maintained, Controlled or Operated by 1&1 Media, Inc., Google, Inc., Microsoft Corp. & Yahoo! Inc., No. 2:17-CM-3152-WC, 2017 WL 4322826, at *1–2 (M.D. Ala. Sept. 28, 2017) (describing the warrant applications at issue which detailed specific types of content, pertinent record date ranges, and "fruits, evidence, and instrumentalities of violations of" specified criminal statutes).

34. *See, e.g.*, *infra* Appendices A–B (exhibiting proposed warrants to Facebook, Inc. that parse account content to the specific types of user activity that are stored by the service provider); *see also* Brief of Appellant at 42–43, *In re* 381 Search Warrants Directed to Facebook, Inc. & Dated July 23, 2013, 78 N.E.3d 141 (N.Y. 2017) (APL-2015-00318) (indicating that Facebook could withhold certain categories of content associated with an

To better accommodate the practical necessities that arise from reviewing voluminous data sets, the 2009 amendments to the Federal Rules of Criminal Procedure allow for a different process to obtain and search ESI.[35] This procedure authorizes "a later review of the media or information" pursuant to the warrant, essentially creating a two-step process[36] where law enforcement first obtains a broad set of ESI from the location where it is stored[37] and then conducts a review of the ESI for material "consistent with the warrant."[38] As the Advisory Committee stated, the impracticality of reviewing a large volume of ESI on site motivated this two-step process.[39] While Rule 41 states that the ESI warrant execution deadline specifically pertains to the "seizure or on-site copying of the media or information, and not to any later off-site copying or review," it does not mandate or suggest a time frame or methodology to conduct the second step of the search.[40] The Advisory Committee explains this intentional omission by noting that "the practical reality is that there is no basis for a 'one size fits all' presumptive period."[41] Although the hesitation to codify universal standards is consistent

account such as "Friends, Likes, [and] Groups" and asserting that warrants should omit data types that are not relevant).

35. Under the Federal Rules of Criminal Procedure, ESI includes "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained." FED. R. CRIM. P. 41 advisory committee's notes to 2009 amendment (adopting the definition stated in Rule 34(a) of the Federal Rules of Civil Procedure). The Advisory Committee noted that Rule 34's broad description, "intend[ing] to cover all current types of computer-based information and to encompass future changes and developments," applies to Rule 41 as well. *Id.* While case law pertaining to the execution of this Rule also addresses the context of computers or digital storage devices seized during warrant execution at a physical location, this Rule applies to seizures pursuant to the Stored Communications Act. 18 U.S.C. § 2703(b)(1)(A) (2012) (requiring a provider to disclose the contents of electronic communication "if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction"); *see, e.g.*, *In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 393 (S.D.N.Y. 2014).

36. FED. R. CRIM. P. 41(e)(2)(B).

37. This consists of obtaining records from a service provider or, alternatively, the initial seizure of a hard drive or computer. *See, e.g.*, *In re* Search of Google Email Accounts, 99 F. Supp. 3d 992, 994 (D. Alaska 2015) (describing the search warrant execution process, during which Google was directed to provide the government with email content for six accounts).

38. FED. R. CRIM. P. 41(e)(2)(B). In practice, courts recognized this practice as valid and necessary prior to the amendment of the Rule. *See, e.g.*, United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999); *In re* Search of: 3817 W.W. End, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004); *see also* Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 87–88 (2005) (describing the need for criminal procedure to adapt to the necessity of two-step searches); Kaitlyn R. O'Leary, Note, *What the Founders Did Not See Coming: The Fourth Amendment, Digital Evidence, and the Plain View Doctrine*, 46 SUFFOLK U. L. REV. 211, 217 (2013).

39. FED. R. CRIM. P. 41 advisory committee's notes to 2009 amendment.

40. *Id.* r. 41(e)(2)(B).

41. *Id.* r. 41 advisory committee's notes to 2009 amendment. As detailed in Part II, Rule 41 does not preclude a judge from imposing a deadline for the return of the ESI at the time the warrant is issued but does not "arbitrarily set a presumptive time period for the return." *Id.*

with the fact-specific nature of search warrant evaluation, the absence of a clear standard has led to a wide variety of results across cases.[42]

### *B. "Step Two" Execution: The Reasonableness Touchstone for Valid Execution Under the Fourth Amendment*

Search warrants for ESI, like other searches subject to the Fourth Amendment, are governed by "the general touchstone of reasonableness."[43] Although the mechanics of reviewing digital materials differ considerably from searching physical items, there is no separate procedural rule or law that regulates how this second step should be conducted.[44] The "details of how best to proceed" with warrant execution have largely been left to the discretion of law enforcement officials.[45]

For warrants authorizing searches of physical locations, developed case law provides benchmarks for reasonable execution.[46] However, the contours of ESI searches are largely undeveloped and vary considerably among appellate courts, trial courts, and magistrate judges.[47] This ambiguity is a natural quality in a still-developing area of law. However, the lack of basic unifying standards for execution leaves law enforcement with little guidance. Law enforcement officers might be prohibited from executing a warrant in a manner that might be ultimately considered constitutionally reasonable[48] or might be uncertain whether their execution methodology will cause the suppression of the evidence at trial.[49] Similarly, the privacy interests of

---

42. *See infra* Parts II.A–B.

43. United States v. Ganias, 755 F.3d 125, 136 (2d Cir. 2014) (quoting United States v. Ramirez, 523 U.S. 65, 71 (1998)), *rev'd en banc*, 824 F.3d 199 (2d Cir. 2016); *see also* United States v. Matias, 836 F.2d 744, 747 (2d Cir. 1988) (holding that officers cannot seize and retain items outside the scope of the warrant); United States v. Scully, 108 F. Supp. 3d 59, 100 (E.D.N.Y. 2015) (applying the touchstone of reasonableness to the context of search warrants for ESI); United States v. Lustyik, 57 F. Supp. 3d 213, 230 (S.D.N.Y. 2014) ("Like all activities governed by the Fourth Amendment, the execution of a search warrant must be reasonable.").

44. *See* FED. R. CRIM. P. 41 advisory committee's notes to 2009 amendment (delegating search execution details to judicial regulation).

45. Dalia v. United States, 441 U.S. 238, 257 (1979); *see also Ganias*, 755 F.3d at 136; *In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 396 (S.D.N.Y. 2014).

46. *See* United States v. Grubbs, 547 U.S. 90, 95–97 (2006) (discussing anticipatory warrant validity); Richards v. Wisconsin, 520 U.S. 385, 394 (1997) (addressing knock-and-announce requirements and exceptions); United States v. Ross, 456 U.S. 798, 822–24 (1982) (discussing limitations on searching closed containers).

47. *See infra* Part II; *see also* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1244 (2010).

48. Kerr, *supra* note 47, at 1246 (arguing that "[p]redictions of reasonableness are highly error-prone" in the absence of sufficient facts to make the determination in each respective case).

49. *See id.* at 1280 (stating that repeated ex post judicial review of search reasonableness leads to the development of general standards that law enforcement can follow). It follows that in the absence of such standards, there is greater uncertainty about future judicial evaluations. The variation in judicial response, detailed in Part II, heightens this uncertainty.

individual account holders also suffer as the government might retain personal data unrelated to the case.[50]

Even with the 2009 amendment to the Federal Rules of Criminal Procedure, questions debated over ten years ago about the process of searching digital materials remain unanswered today. Does reasonableness govern the timing of the subsequent search, and, if so, what length of time is reasonable?[51] What procedures and protocols, if any, are necessary to ensure warrant particularity or reasonable search execution?[52] And finally, is ESI so different that it requires distinct modifications to established search and seizure doctrine?[53]

## II. APPROACHES TO EXECUTING THE REVIEW OF ELECTRONICALLY STORED INFORMATION

In response to the lack of procedural guidelines, courts have responded at the magistrate level when the warrant is granted or denied and subsequently in trial courts during the consideration of suppression motions. Part II.A details the ex ante requirements some magistrate judges have implemented to regulate the scope, duration, and method of search execution. Part II.B examines ex post rulings on reasonability of the search and discusses the extent to which these rulings provide adequate guidance for subsequent cases. Next, Part II.C discusses the divergent approaches to the plain view doctrine in the context of ESI and Part II.D analyzes suggested policy responses.

### *A. Ex Ante Orders Regulating Search Methodology and Execution*

Magistrate judges have issued ex ante orders with the objective of curtailing the breadth of the warrant. Though far from universally applied by magistrates who review warrant applications, those who have required secondary orders or specific provisions to be written into the warrant itself express concern about granting warrants for ESI that might effectively

50. *See In re* Search of Premises Known As: Three Hotmail Email Accounts: [redacted]@hotmail.com, [redacted]@hotmail.com, [redacted]@hotmail.com Belonging to & Seized from [redacted], No. 16-MJ-8036-DJW, 2016 WL 1239916, at *13 (D. Kan. Mar. 28, 2016) ("The search of an email account 'would typically expose to the government far *more* than the most exhaustive search of a house: [an email account] not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form.'" (quoting Riley v. California, 134 S. Ct. 2473, 2491 (2014))), *aff'd in part sub nom. In re* Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp., 212 F. Supp. 3d 1023 (D. Kan. 2016); Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. BRIEF 1, 6–7 (2011) (noting that widespread use of email services and social media has led to unprecedented large-scale storage of communications and highlighting that "[e]ven when we aren't hoarding, our computers are").

51. *See* Kerr, *supra* note 38, at 117–24 (discussing the divergence between courts in evaluating whether searches for ESI within a certain time period are constitutional).

52. *See id.* at 113–14.

53. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 554–57 (2005).

become unconstitutional general warrants.[54] These magistrates impose such ex ante requirements under the belief that they enhance the particularity of the warrant in detailing items to be seized or, alternatively, provide safeguards for their reasonable execution.[55]

While concerns about issuing general warrants are the basis for such ex ante action, magistrate-issued orders have addressed differing aspects of the search by (1) instituting time limits on completion, (2) mandating return or deletion of nonresponsive materials, or (3) enumerating specific search protocol to be utilized during execution.

1. Time Limits to Complete "Second-Step" Search of Materials

The amendment to Rule 41, which formally authorizes the two-step process, clarifies that the fourteen-day execution requirement applies only to the initial seizure of the materials, which leaves the timing of the subsequent review open to judicial analysis.[56] As a result, some magistrates have regulated the warrant process by ordering a deadline for search completion in the absence of a statutory requirement.[57] Magistrates have imposed this deadline at the time the warrant is granted, with the possibility of requesting an extension,[58] or after the initial seizure of materials.[59]

---

54. *See, e.g.*, *In re* Search of Info. Associated with Fifteen Email Addresses Stored at Premises Owned, Maintained, Controlled or Operated by 1&1 Media, Inc., Google, Inc., Microsoft Corp. & Yahoo! Inc., No. 2:17-CM-3152-WC, 2017 WL 4322826, at *10 (M.D. Ala. Sept. 28, 2017) (ruling that the warrant should be issued with an accompanying order that the accounts should be searched using keywords to limit "the universe of data"); *In re Three Hotmail Email Accounts*, 2016 WL 1239916, at *23 (requiring ex ante instructions limiting search execution methods); *see also In re* Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis That Is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 10–11 (D.D.C. 2013) (describing the court's use of secondary orders to bring search warrants under constitutional standards).

55. *See supra* note 54.

56. FED. R. CRIM. P. 41 advisory committee's notes to 2009 amendment. This time frame applies to the seizure of computers or other storage devices pursuant to a search of a physical location. For warrants on an electronic communications service provider pursuant to 18 U.S.C. § 2703(b), this time period best corresponds to when the warrant is served on the provider as it is analogous to the initial seizure of a computer or hard drive.

57. *See* United States v. Brunette, 76 F. Supp. 2d 30, 42 (D. Me. 1999) (suppressing material obtained as a result of a search after the magistrate-issued thirty-day deadline and subsequent thirty-day extension). The magistrate judge's decision to impose a thirty-day limit on the execution of the search in this case, like many other decisions on whether to grant a search warrant and under what limitations, is unwritten and unpublished. Therefore, a specific rationale behind imposing the limitation on the search time frame is unknown. *See* Reid Day, Note, *Let the Magistrates Revolt: A Review of Search Warrant Applications for Electronic Information Possessed by Online Services*, 64 U. KAN. L. REV. 491, 520 (2015) (acknowledging the small number of decisions addressing the sufficiency of warrant applications).

58. *See Brunette*, 76 F. Supp. 2d at 42.

59. *See, e.g.*, *In re* Search of Premises Known as 1406 N. 2nd Ave., No. 2:05-MJ-28, 2006 WL 709036, at *1 (W.D. Mich. Mar. 17, 2006) (ordering law enforcement to submit a return to the court within thirty days of the warrant execution, prior to review of all computer storage media, along with an estimate of "the time necessary to conduct a forensics examination of the materials seized and the computer search protocol to be utilized").

However, this practice is far from universal. Other courts, while acknowledging the power of magistrate courts to impose limitations on the search execution, have declined to do so on the grounds that the Fourth Amendment does not require it and that the issue is better suited to ex post review for reasonableness.[60] A central argument against imposing restrictions at the time the warrant is granted involves the government's "need to retain materials as an investigation unfolds for the purpose of retrieving material that is authorized by the warrant."[61] This argument asserts that the benefit of an unrestrained review of the ESI is maintained while the individual's privacy interests are protected through a "reasonableness" ex post inquiry of the search.[62]

Even in a number of cases where a magistrate imposed a deadline for the review, some trial courts have not given effect to such orders and have refused to penalize noncompliance when the additional time taken was deemed to be reasonable.[63] The determination of reasonability in this context, sufficient to abandon the magistrate's restrictions, is in part made under the rationale that the government did not exhibit "reckless disregard for proper procedure" or that the defendant was not prejudiced.[64] Beyond the issue of whether ex ante restrictions should be enforced, some question the authority of magistrate judges to issue such deadlines without explicit legislative or procedural mandate.[65] Although ex ante orders are generally accepted, and not precluded by the Federal Rules of Criminal Procedure,[66]

60. *See, e.g.*, *In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 396 (S.D.N.Y. 2014) (citing United States v. Grubbs, 547 U.S. 90, 99 (2006)).

61. *Id.* at 398. Magistrate Judge Gabriel W. Gorenstein also noted the legitimate need to maintain a copy of records for the purpose of authentication at trial. *Id.* at 399.

62. *Id.* at 398. The court additionally notes that Rule 41(g) offers a remedy for the return of property and even the destruction of copies of seized material. *Id.*

63. *See* United States v. Filippi, No. 5:15-CR-133 (BKS), 2015 WL 5789846, at *9 (N.D.N.Y. Sept. 9, 2015) ("[T]he Supreme Court has held that a search in violation of a Magistrate Judge's directives regarding the execution of a warrant does not violate the Fourth Amendment, so long as the search was reasonable under the circumstances." (citing Richards v. Wisconsin, 520 U.S. 385, 117 (1997))); United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *29 (D. Ariz. May 8, 2013) (holding that the execution of the search was reasonable even though completion of the review violated the magistrate judge's thirty-day deadline); United States v. Hernandez, 183 F. Supp. 2d 468, 481 (D.P.R. 2002) (holding that it was "perfectly reasonable for the Government to take a longer time to search and inspect" ESI, especially after already discovering some evidence of a crime).

64. United States v. Beckmann, 786 F.3d 672, 680–81 (8th Cir. 2015) (holding that the defendant in this case was not prejudiced as "probable cause continued to exist and the evidence did not become stale").

65. *See* Kerr, *supra* note 47, at 1260–78 (arguing that neither the rules nor case law permit an active role for magistrate judges and even when ex ante orders are issued, they are frequently unenforced). Kerr relies, in part, on Supreme Court precedent that states that the Fourth Amendment only requires probable cause and particularity. *Id.* at 1267–68 (citing *Grubbs*, 547 U.S. 90). *But see* Ohm, *supra* note 50, at 4 (criticizing Kerr's presumption that magistrate orders that set deadlines or require certain procedures address reasonableness rather than particularity concerns).

66. FED. R. CRIM. P. 41 advisory committee's notes to 2009 amendment ("The rule does not prevent a judge from imposing a deadline for the return of the storage media or access to the electronically stored information at the time the warrant is issued. However, to arbitrarily

the arguments calling a magistrate's power into question are perhaps useful to evaluate whether these orders are effective.

### 2. Deletion and Return of Nonresponsive Materials

In addition to the varying time restrictions, some magistrates have required the government to return or destroy any material deemed nonresponsive to the warrant. By imposing this requirement, courts seek to address the issue of overbreadth in part through limiting the possibility of any future use of materials that are beyond the scope of the warrant.[67] Despite the authority given to conduct a subsequent search for responsive materials under Rule 41, courts have expressed discomfort in allowing these searches without (1) showing probable cause to seize the entire account or (2) requiring the government to return or destroy any materials that constitute an "over-seizure."[68] Courts have contemplated a range of these types of restrictions; some have mandated assurances that "the information will be returned or, if copies, destroyed within a prompt period of time,"[69] while others have not expressed any temporal indicator for when the materials must be deleted.[70]

In contrast to magistrate judges who impose these restrictions ex ante (or make comments to this effect when rejecting an application on other grounds), others challenge the idea of putting a return or deletion requirement tied to a specific timeline up front. While acknowledging that it was

---

set a presumptive time period for the return could result in frequent petitions to the court for additional time.").

67. *See In re* Search of Black iPhone 4, 27 F. Supp. 3d 74, 80 (D.D.C. 2014) (indicating that a revised warrant application must stipulate that nonresponsive seized documents will be returned or destroyed "within a prompt period of time" or it will be denied); *In re* Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis That Is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 9–10 (D.D.C. 2013); *see also In re* Search of Premises Known as: Three Hotmail Email Accounts: [redacted]@hotmail.com, [redacted]@hotmail.com, [redacted]@hotmail.com Belonging to & Seized from [redacted], No. 16-MJ-8036-DJW, 2016 WL 1239916, at *23 (D. Kan. Mar. 28, 2016) (stating generally that retention limits are an "easily enforceable tool" to protect Fourth Amendment rights); *In re* [REDACTED]@gmail.com, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (denying a warrant due to a lack of particularity and expressing concern over the absence of "any kind of commitment to return or destroy evidence"). This concern precedes the digital context in cases involving the seizure of a large amount of documents, including those outside the scope of the warrant. *See* United States v. Tamura, 694 F.2d 591, 597 (9th Cir. 1982) (finding that the government's retention of master volumes of seized documents for a period longer than six months, absent the need for the complete copy for authentication purposes, was "unreasonable and therefore [an] unconstitutional manner of executing the warrant").

68. *In re Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d at 9–10.

69. *In re Search of Black iPhone*, 27 F. Supp. 3d at 80. In this case, the court stated that the government must include a description of "what will occur with [the nonresponsive] data," and an application would likely be denied if it included any statement other than the text quoted above. *Id.*; *see also* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1168–69 (9th Cir. 2010) (en banc) (per curiam) (requiring the government to return nonresponsive items "within a reasonable period of time not to exceed 60 days from the date of the seizure unless further authorization [was] obtained from the Court").

70. *See, e.g.*, *In re Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d at 9–10.

unacceptable to retain nonresponsive material indefinitely,[71] courts have determined that retaining materials while proceedings are ongoing, without intent to use them in a subsequent investigation, is reasonable.[72] Similar to the rationale for opposing search execution deadlines,[73] judges have resisted imposing rigid retention limits during the course of a case because they believe that they could hinder law enforcement's ability to execute a thorough search and that better remedies exist to address impropriety.[74]

3. Mandated Protocol for How the Search Must Be Completed

In light of privacy concerns regarding ESI searches, magistrate judges have also considered imposing restrictions on review procedure, with the objective to either narrow the particularity of items to be seized or to ensure that the search is conducted in a reasonable manner. A range of options have been considered and implemented, including (1) requiring an independent review team,[75] (2) utilizing targeted search terms,[76] and (3) requesting an initial keyword screening by service providers.[77] These measures all seek to prevent or curtail the case team from coming into contact with nonresponsive material.

While approving search warrant applications, magistrates have mandated that an independent party or "taint team" review the electronic search warrant materials in order to limit law enforcement's exposure to nonresponsive material.[78] Although there are variations in the exact approach,[79] this

71. *See* United States v. Ganias, 755 F.3d 125, 137–38 (2d Cir. 2014) (finding that allowing the government to retain nonresponsive materials and subsequently search them pursuant to a different warrant would amount to a general search), *rev'd en banc*, 824 F.3d 199 (2d Cir. 2016); *see also* Kelsey Joy Smith, Note, *The Constitutional Right to Deletion: The Latest Battle in the War of Technology v. Privacy*, 42 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 121, 139–42 (2016) (analyzing perceived circumvention of Rule 41(g)'s remedy to return seized materials and calling for Congress to issue a clear rule on government retention of digital property to better protect privacy rights).

72. *See* United States v. Carpenter, No. 3:13-CR-226-RNC, 2015 WL 9461496, at *6–7 (D. Conn. Dec. 24, 2015).

73. *See supra* Part II.A.1.

74. *See In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 397–98 (S.D.N.Y. 2014) (arguing that an execution and retention deadline would hinder the government's ability to review materials effectively, especially considering the possibility for relevant coded language being discovered later on in time).

75. *See infra* notes 78–86 and accompanying text.

76. *See infra* notes 87–92 and accompanying text.

77. *See infra* notes 93–96 and accompanying text.

78. *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1168–69 (9th Cir. 2010) (en banc) (per curiam) (describing the search restrictions that the magistrate judge imposed); Preventive Med. Assocs., Inc. v. Commonwealth, 992 N.E.2d 257, 263 (Mass. 2013) (describing the motion judge's order that the search utilize a "taint team" consisting of attorney general's office employees who were not involved in the investigation or prosecution, in order to remove potentially privileged information); *In re* Search Warrant, 71 A.3d 1158, 1176 (Vt. 2012) (describing a judicial officer's instructions that only the materials deemed relevant should be accessed by the case investigators).

79. This idea encompasses the use of independent third-party reviewers, where the individuals looking through the materials for responsive items are not members of the law

mechanism is generally aimed at preserving the confidentiality of materials for which the government does not have probable cause to seize or retain.[80] Courts that require this procedure do so on the basis that they promote either warrant particularity or overall reasonableness of the search.[81] While the reasoning that underpins each decision to grant or deny a search warrant is at times imprecise, some courts have explicitly indicated that a particularity objective is served by limiting the case team to view only those materials that the warrant authorized.[82] Courts do this to prevent the overbreadth that would otherwise occur during the two-step process.[83] Concerned with the possibility that search warrants for electronic communications may become unconstitutional general warrants, appellate and trial court judges have urged their magistrate colleagues to restrict the review of electronic materials to those without affiliation with the case.[84] As one circuit judge noted,

> [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.[85]

Although this measure could conceivably serve either justification, Judge Alex Kozinski articulated that these procedures enhance reasonableness by

---

enforcement agency conducting the investigation. *See In re* Search of Premises Known as: Three Hotmail Accounts: [redacted]@hotmail.com, [redacted]@hotmail.com, [redacted]@hotmail.com Belonging to & Seized from [redacted], No. 16-MJ-8036-DJW, 2016 WL 1239916, at *22 (D. Kan. Mar. 28, 2016), *aff'd in part sub nom. In re* Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp., 212 F. Supp. 3d 1023 (D. Kan. 2016). Additionally, it includes the use of a "taint team," which consists of individuals within the organization but not assigned to work on the case. *See* United States v. Sealed Search Warrant, No. 2:17-CR-103-VEH-TMP-1, 2017 WL 3396441, at *2 (N.D. Ala. Aug. 8, 2017). In both of these circumstances, the reviewing group would identify and provide only the materials falling under the scope of the warrant to the case team. This technique is also commonly employed in the context of separating privileged information. *See, e.g.*, United States v. Wey, 256 F. Supp. 3d 355, 374 (S.D.N.Y. 2017) (finding that the case agent and Assistant U.S. Attorney organized an FBI "wall team" to "segregate non-privileged from potentially privileged documents in advance of the case team's substantive review of the material").

80. *See In re Three Hotmail Email Accounts*, 2016 WL 1239916, at *21.

81. *See, e.g.*, *id.* at *8, *21 (emphasizing the commitment to halt the issuance of general warrants for ESI and ultimately recommending the implementation of search protocol to offer protection from the threat of general warrants).

82. *In re Search Warrant*, 71 A.3d at 1175 (stating that "[t]he separation and screening instructions are the judicial officer's attempt to remedy this lack of particularity," while also acknowledging that ex ante procedures are never required).

83. *Id.*

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

85. *Id.*

ensuring that seizure does not exceed the bounds supported by probable cause.[86]

The requirement to utilize specific keyword queries or filtering tools[87] has been similarly implemented in order to ensure the particularity of the warrant, characterized as a way to describe the particular place to be searched.[88] This procedure could either require a search by category, naming general areas or file paths that can be searched,[89] or a free text search of items, including "names, usernames, email addresses, credit card numbers, dates, social security numbers" or general terms and phrases.[90] While this may already occur for practical reasons during the review of voluminous warrant materials,[91] imposing an ex ante requirement as an assurance of particularity could force law enforcement to generate a keyword list without knowledge of how large the initial seizure would be and could prevent further tailoring of the search to hone in on relevant results.[92]

Another option involves mandating service providers to conduct an initial screening.[93] This idea maintains the function of the keyword search—with

86. *Id.* at 1178 (stating that a magistrate's mandate of an independent review team would "increase the likelihood that the searches and seizures of electronic storage that they authorize will be deemed reasonable and lawful").

87. This entails the utilization of review platform tools to identify and focus on a subset of documents based on common characteristics. For the purposes of this Note, this phrase includes (1) running searches for specific words or phrases that are present in a document, (2) filtering categories about the communication, such as by recipients or senders, dates or times, or associated IP addresses, or (3) utilizing advanced metrics to identify documents that fall under a common pattern.

88. *See In re* Search of Info. Associated with Fifteen Email Addresses Stored at Premises Owned, Maintained, Controlled or Operated by 1&1 Media, Inc., Google, Inc., Microsoft Corp. & Yahoo! Inc., No. 2:17-CM-3152-WC, 2017 WL 4322826, at *7 (M.D. Ala. Sept. 28, 2017) ("Often the way to specify particular objects or spaces will not be by describing their physical coordinates but by describing how to locate them. This is especially true in the world of electronic information, where physical notions of particularity are metaphorical at best." (quoting *In re* Search Warrant, 71 A.3d 1158, 1170–71 (Vt. 2012))).

89. This is generally more applicable in the context of searches of computers or storage devices, although it may still be relevant in the review of cloud storage materials.

90. *In re* Search of Premises Known as: Three Hotmail Accounts: [redacted]@hotmail.com, [redacted]@hotmail.com, [redacted]@hotmail.com Belonging to & Seized from [redacted], No. 16-MJ-8036-DJW, 2016 WL 1239916, at *20 (D. Kan. Mar. 28, 2016), *aff'd in part sub nom. In re* Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp., 212 F. Supp. 3d 1023 (D. Kan. 2016) (finding that "*ex ante* instructions, as whole, are not per se unreasonable" but declining to decide whether the instructions suggested by Magistrate Judge David Waxse are reasonable).

91. *Id.* at *8; *see, e.g.*, United States v. Ganias, 824 F.3d 199, 202 (2d Cir. 2016) (en banc) (describing the procedure by which the records were reviewed and noting that new keywords were created and utilized when previous ones generated too many hits).

92. For example, if a review of materials using an individual's name reveals a code word utilized in connection with the criminal conduct which was unknown at the time of warrant execution and not specified therein but would be more effective in identifying responsive items. *See In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 398–99 (S.D.N.Y. 2014).

93. *See In re Three Hotmail Email Accounts*, 2016 WL 1239916, at *19; *In re* Search of Info. Associated with [redacted]@mac.com That Is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1, 8–9 (D.D.C. 2014) ("[H]aving an electronic communication service

the exception that the records holder would perform the search instead of law enforcement—to limit the amount of data turned over to the government in the first place.[94] Judge Facciola has suggested that the balance between law enforcement's interests and an individual's expectation of privacy can be achieved by requiring service providers to conduct an initial screening of the material for pertinent indicators.[95] This argument is based on the premise that the "government surely knows how it intends to ultimately sort through the information [provided]" and that service providers are "technologically sophisticated actors" capable of executing that search themselves.[96]

As some judges have imposed one of these mechanisms specifically, others have indicated that law enforcement could choose which of these ex ante measures to implement so long as some limitation is place.[97] By providing the opportunity to choose which search limitation to exercise, the benefit from greater particularity or reasonableness arguably can be achieved while allowing law enforcement the traditional deference regarding the details of warrant execution.[98]

Other courts have resisted requiring specific search protocol on the ground that the Fourth Amendment does not require a warrant to contain more than a particularized description of places to be searched and items to be seized, supported by probable cause.[99] Courts have cited long-standing law enforcement discretion in determining execution details while rejecting an "attempt to constitutionalize document review procedures," and they have even noted that the duty to review and identify responsive material did not

---

provider perform a search, using a methodology based on search terms . . . suggested by the government and approved by the Court seems to be the only way to enforce the particularity requirement commanded by the Fourth Amendment."). While theoretically this idea could be separated from keyword searches, requiring that level of review would be overly burdensome for service providers.

94. *In re Search of Info. Associated with [redacted]@mac.com*, 25 F. Supp. 3d at 7.

95. *Id.* at 8.

96. *Id.* The court noted that, in fact, Google has already proven this capability as it "created an entire business model around searching the contents of e-mail in order to deliver targeted advertising, and it has done so for a decade." *Id.*

97. *In re Three Hotmail Email Accounts*, 2016 WL 1239916, at *20 (stating that the government must only "educate the Court as to how it intends to minimize the discovery of ESI outside the scope of the warrant").

98. *See also* Riley v. California, 134 S. Ct. 2473, 2491 (2014) (commending the government's suggestion in its brief that law enforcement should "'develop protocols to address' concerns raised by cloud computing" (quoting Reply Brief for the United States at 14–15, *Riley*, 134 S. Ct. 2473 (No. 13-212))).

99. *See* United States v. Kanodia, No. 15-10131-NMG, 2016 WL 3166370, at *7 (D. Mass. June 6, 2016) ("In overseeing the warrant process, the Court is 'primarily concerned with identifying *what* may be searched or seized—not how,' . . . and generally will not interfere with the discretion of law enforcement in determining 'how best to proceed with the performance of a search authorized by warrant.'" (first quoting United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999); then quoting United States v. Tsarnaev, 53 F. Supp. 3d 450, 464 (D. Mass. 2014))); *In re* Search of Info. Associated with [redacted]@mac.com That Is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157, 165 (D.D.C. 2014) ("[B]ecause the government's proposed procedures comply with the Fourth Amendment and are authorized by Rule 41, there is no need for Apple to search through e-mails and electronic records related to the target account and determine which e-mails are responsive to the search warrant.").

require a particular process for memorialization.[100] Rather than utilizing protocols as a method to gain particularity, courts can instead rely on a description of the nature and character of the content to be seized, apart from how it can be located.[101]

Further, some argue the protocols described above are too restrictive and hinder the ability to identify responsive materials.[102] As the volume of items that a service provider might have is frequently unknown when a judge grants a warrant, these ex ante requirements can prevent the government from implementing the most effective search procedure when they are in a better position to evaluate what that would be.[103]

These protocols also face criticism on an individual level. Mandating the use of keyword searches to limit the results can substantially restrict the effectiveness of the search, as communications clearly covered in the warrant might not utilize the exact language anticipated, and the process eliminates the use of context and other traditional methods of identifying relevant evidence.[104] Judge Kozinski explains that limiting an electronic search by a suspect's specific language would be "like saying police may not seize a plastic bag containing a powdery white substance if it is labeled 'flour' or 'talcum powder.'"[105] Although keyword searches could be useful in identifying pertinent documents in certain circumstances, their utility can become more strained in the case of media or text-embedded images.[106] Along these lines, the use of keyword searching may hinder the ability to identify responsive material by eliminating the context of these

100. United States v. Lumiere, No. 16-CR-483, 2016 WL 7188149, at *5 (S.D.N.Y. Nov. 29, 2016).

101. United States v. Lee, No. 1:14-CR-227-TCB-2, 2015 WL 5667102, at *9 (N.D. Ga. Sept. 25, 2015). In this case, the warrant enumerated specific crimes rather than allowing a search based on general criminal activity and "thus properly constrained the discretion of the executing agents." *Id.* To this point, there is a difference between legal seizure of a broad array of items and failure to meet the particularity requirement. *See* United States v. Sugar, 606 F. Supp. 1134, 1151 (S.D.N.Y. 1985); *see also* United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars & Fifty-Seven Cents, 307 F.3d 137, 149 (3d Cir. 2002) ("Although the scope of the warrant was certainly extensive, the warrant was not general.").

102. *See also* Kerr, *supra* note 47, at 1284–87 (discussing why ex ante measures are not required by the Fourth Amendment and how their implementation is unworkable and unwise given the high rate of constitutional error).

103. *See generally* FED. R. CRIM. P. 41 advisory committee's notes to 2009 amendment (discussing the hesitancy to impose a "one size fits all" requirement).

104. *See* Brief for the United States at 51, United States v. Blake, 868 F.3d 960 (11th Cir. 2017) (No. 15-13395-FF) ("[C]riminals may misspell words, intentionally or unintentionally use different terminology than the key words, or use coded or generally evasive language, such as 'I did that thing you asked.'").

105. United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) (quoting United States v. Hill, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004) (Kozinski, J., sitting by designation)); *accord* United States v. Crespo-Rios, 645 F.3d 37, 43 (1st Cir. 2011).

106. United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009) (recognizing that search methods "must remain dynamic" due to the difficulty in outlining a satisfactory structure prospectively); *see also* United States v. Loera, 59 F. Supp. 3d 1089, 1137 (D.N.M. 2014) (acknowledging that search warrants for ESI do not need to include specific search protocols since such searches are "inherent[ly] complex[] and unpredictab[le]"), *appeal docketed*, No. 17-2180 (10th Cir. Oct. 16, 2017).

communications along with the ability to make connections that may not be apparent in isolation.

Requirements calling for service providers to perform an initial search are similarly criticized. In addition to problems with the specific keywords utilized, such protocols are condemned for placing too much of a burden on service providers.[107] Indeed, one court noted that it is "unrealistic to believe that Google or any other email host could be expected to produce the materials responsive to categories listed in a search warrant."[108] In addition to the burden of reviewing ESI content, and potentially duplicating the government's efforts, service provider employees may not be capable of "interpret[ing] the significance of particular emails without having been trained in the substance of the investigation"[109] and could miss "[s]eemingly innocuous or commonplace messages [that] could be the direct evidence of illegality the Government had hoped to uncover."[110]

Between requiring execution deadlines, retention limits, independent party review, keyword searches, service provider screening, or some combination of these approaches,[111] magistrates seek to balance the governmental interest in obtaining the information with the privacy interests particularly with respect to the nonresponsive materials. Such mechanisms seek to compensate for the two-step process by limiting the government's access to nonresponsive material through search protocol and deadlines. However, in addition to the concerns about each requirement individually, the range of measures as a whole leaves the application and execution of ESI search warrants inconsistent and unclear.

### *B. Ex Post Rulings Shaping the Boundaries of Reasonableness in the Digital Context*

While their magistrate counterparts try to anticipate reasonableness at the time the warrant is issued, trial courts have also sought to define the

107. *See* United States v. Deppish, 994 F. Supp. 2d 1211, 1220 (D. Kan. 2014) (finding that requiring the service provider to conduct a review of the material would be unreasonable and less effective than allowing "government agents to determine the relevance of particular emails"). While service providers have expertise in navigating their own systems to identify and retrieve the specified types of data stored therein, they may not have the experience or resources to identify materials that constitute the evidence described in the warrant. *See In re* Search of Info. Associated with Fifteen Email Addresses Stored at Premises Owned, Maintained, Controlled or Operated by 1&1 Media, Inc., Google, Inc., Microsoft Corp. & Yahoo! Inc., No. 2:17-CM-3152-WC, 2017 WL 4322826, at *9 (M.D. Ala. Sept. 28, 2017) (stating that it would "generally be unrealistic to expect Google or another email provider to conduct the search for the Government").

108. *In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014).

109. *Id.* at 395 (rejecting analogies between ESI warrants and subpoenas, as a service provider "typically searches only its own records, of which it is expected to have a full understanding of the source and content" and usually "is not called upon to search another party's records"). In this respect, knowledge of the organization and storage of customer data is distinct from familiarity with the actual data content. *See id.*

110. *Id.*

111. See Appendix C for a summary of the various mechanisms described in this Part.

boundaries of ESI searches in specific cases, driven by the specific set of facts at hand after the search is executed.[112]

In evaluating the reasonableness of an ESI search, judges have considered the following areas: (1) the duration of search execution, (2) implementation of search protocols, and (3) limitations in the warrant based on crime type, date range, or data type.

### 1. Establishing a Reasonable Time to Execute the Search

The reasonableness of electronic search duration and retention of digital materials have been disputed in the courts even prior to the 2009 amendment to Rule 41.[113] While the amendment resolved one issue (by stating that the required fourteen-day deadline for execution only applied to the first step), Rule 41 still leaves the timing of the second-step search to the discretion of the courts.[114] The Advisory Committee delegated this determination to the courts due to the case-specific factors, including the technological effort involved, size of the return, and resources available, which can create varying standards for when completion of a search is possible.[115] Yet the void has created significant variation in what courts have found to be a permissible amount of time to execute the second-step search, which makes it difficult to anticipate what will be considered reasonable in subsequent cases.

Decisions on whether the duration of the review of ESI is reasonable have ranged from disapproval of a fifteen-month period[116] to acceptance of subsequent searches after five years had elapsed.[117] This variation can be partially attributed to fact-specific situations,[118] but it also belies the lack of consistent guiding principles to evaluate the reasonableness of search

---

112. Reasonableness evaluations of search warrants are generally fact-specific exercises. This Part discusses decisions in this area, which do not provide much assistance for future determinations of reasonableness absent any benchmarks.

113. *See supra* note 38 and accompanying text.

114. *See* FED. R. CRIM. P. 41 advisory committee's notes to 2009 amendment (indicating that the Committee considered but did not implement a presumptive or universal time period for subsequent off-site review because "the practical reality is that there is no basis for a 'one size fits all' presumptive period").

115. *Id.* ("A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs.").

116. *See* United States v. Johnston, 789 F.3d 934, 941–43 (9th Cir. 2015) (finding that an exhaustive search five years after the initial seizure was reasonable).

117. *See* United States v. Metter, 860 F. Supp. 2d 205, 215 (E.D.N.Y. 2012) (holding that a fifteen-month delay in the government's review of seized devices violated the Fourth Amendment); *see also* United States v. Jarman, 847 F.3d 259, 266–67 (5th Cir. 2017) (holding that a twenty-three month review of seized ESI was reasonable due to the complexity of the search and a time-consuming privilege review process); United States v. Gorrell, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) (holding that a ten-month delay in retrieving data from a seized computer did not warrant suppression, although it made note of the "lengthy" process).

118. *Johnston*, 789 F.3d at 942 (where an initial "bare minimum" search preceded a more thorough examination five years later when plea negotiations broke down); United States v. Christie, 717 F.3d 1156, 1163 (10th Cir. 2013) (finding that the delay in the search was reasonable where the agent was assigned to assist on other matters out of town in the intervening time).

duration going forward.[119] Courts have independently contemplated factors while evaluating reasonableness in the timeliness of execution, but they have not established how these factors should be applied to future instances. One of these factors involves the government's delay in first initiating the review of the electronic materials, or, whether the government has evinced a "blatant disregard for its responsibility."[120] While the court recognized that there is no established deadline for the completion of a search, the government's retention of "*all* imaged electronic documents, including personal emails, without *any* review whatsoever to determine not only their relevance to this case, but also to determine whether any recognized legal privileges attached to them, is unreasonable and disturbing."[121]

Another factor bearing on the reasonableness of the review period is whether the government subjected the materials to subsequent searches based on new information and theories developed about the case.[122] In these instances, courts have expressed concern about continued searches for evidence under new theories of the case or more expansive areas not initially included in the warrant.[123]

Beyond the question of what constitutes a reasonable time, courts and scholars disagree on whether a constitutional requirement that the review be conducted in a "reasonable time" exists. The courts cited above, along with others, posit that the reasonableness standard permeates all aspects of the search, including the time frame to conduct the subsequent review.[124]

---

119. This challenge of the ability to predict "how long is too long" raises the question of whether the exclusionary rule would even apply if conduct is not "sufficiently deliberate that exclusion can meaningfully deter it." United States v. Filippi, No. 5:15-CR-133 (BKS), 2015 WL 5789846, at *9 (N.D.N.Y. Sept. 9, 2015) (quoting Herring v. United States, 555 U.S. 135, 144 (2009)).

120. *Metter*, 860 F. Supp. 2d at 212, 215 (stressing that the delay in the start of the review was unreasonable and thus a violation of the Fourth Amendment, while acknowledging that "there is no established upper limit as to when the government must review seized electronic data"); *see also* State v. Zinck, Nos. 03-S-1000-1024, 04-S-2393-2444, 2005 WL 551447, at *2–3 (N.H. Super. Ct. Feb. 4, 2005) (holding the search of a computer's contents to be unreasonable where the state "offered no justifiable reason for waiting approximately a year and one half to begin a search of the defendant's computer").

121. *Metter*, 860 F. Supp. 2d at 215.

122. *See, e.g.*, United States v. Wey, 256 F. Supp. 3d 355, 406 (S.D.N.Y. 2017).

123. *See id.* at 406 (stating that there is "no authority suggesting that simply because it has retained all originally searchable electronic materials, the Government is permitted to return to the proverbial well months or years after the relevant Warrant has expired to make another sweep for relevant evidence, armed with newly refined search criteria and novel case theories"); *see also* People v. Thompson, 28 N.Y.S.3d 237, 255 (Sup. Ct. 2016) (expressing concern with government officials searching "at their leisure" or when "some new issue in this case might arise").

124. *See* United States v. Place, 462 U.S. 696, 709 (1983) (holding that the length of time for which property is seized is a factor that bears directly on the reasonableness of that seizure); United States v. Lustyik, 57 F. Supp. 3d 213, 230 (S.D.N.Y. 2014) (noting that "[l]ike all activities governed by the Fourth Amendment, the execution of a search warrant must be reasonable" and "[l]aw enforcement officers therefore must execute a search warrant," including, when applicable, review of recovered electronic communications "within a reasonable time").

However, the nature of an off-site review of copied materials differs from the initial execution of a warrant in ways that cut against close review of search execution timeliness. The purpose of the mandatory fourteen-day time frame, to "prevent the execution of a stale warrant,"[125] is not relevant in the context of a review of ESI materials. Since warrant staleness pertains to a temporal relationship between the acknowledged existence of probable cause and the likelihood that the evidence sought is still located in the place to be searched,[126] it is less of a concern in the subsequent review of ESI, whose contents remain static once received from the service provider.[127] Additionally, the review duration does not impact or inconvenience any need the owner may have to use the materials, as would be the case for other types of warrants, and therefore lessens the need for a speedy return.[128]

A close counterpart to search execution timeliness is regulation of the government's retention of materials deemed to be nonresponsive. In a given case, the two concepts can be intertwined as the retention of materials not covered under the warrant can be subject to subsequent or ongoing search during that time.[129] There is a distinction, however, between the execution of a search during the span of the case and later retention of all materials, nonresponsive items along with evidence of crime, beyond the closing of an investigation or culmination of prosecution. The concern over "indefinite" retention of such voluminous records relates to the possibility that they may be accessed in future investigations. As contemplated in *United States v. Ganias*,[130] this would transform a specific warrant into "the equivalent of a general warrant" after the fact.[131]

In that case, Judge Denny Chin mused that, while there is practical need for the two-step process to search electronic materials, the accommodations afforded to electronic searches do not justify indefinite retention nor the

125. United States v. Brewer, 588 F.3d 1165, 1172 (8th Cir. 2009) (quoting United States v. Syphers, 426 F.3d 461, 469 (1st Cir. 2005)).

126. *Id.* ("[A] warrant becomes stale if the information supporting the warrant is not 'sufficiently close in time to the issuance of the warrant and the subsequent search conducted so that probable cause can be said to exist as of the time of the search.'" (quoting United States v. Palega, 556 F.3d 709, 715 (8th Cir. 2009))); *see also* United States v. Mutschelknaus, 592 F.3d 826, 830 (8th Cir. 2010) ("The computer media at issue here were electronically-stored files in the custody of law enforcement. Because of the nature of this evidence, the . . . delay in searching the media did not alter the probable cause analysis." (alteration in original) (quoting *Brewer*, 588 F.3d at 1173)).

127. This concern is ameliorated as the records will not be altered after the service provider produces them. This situation is distinguishable from a physical location where someone may alter or move the items of interest during the time between the judge's signature and the physical search. *See* Kerr, *supra* note 38, at 103 ("While it is desirable for electronic searches to occur quickly, staleness is not a concern after the container of evidence has been seized.").

128. The materials companies provide under § 2703 are electronic copies of the data—the owner still retains the ability to access his or her account and the contents of the messages therein. This is distinct from searches of entire computers, devices, or storage drives, which prevent the device's owner from using the material contained therein for the duration of the search.

129. *See, e.g.*, United States v. Wey, 256 F. Supp. 3d 355, 404 (S.D.N.Y. 2017).

130. 755 F.3d 125 (2d Cir. 2014), *rev'd en banc*, 824 F.3d 199 (2d Cir. 2016).

131. *Id.* at 139.

ability to "search them whenever [the government] later developed probable cause" as it leads to a de facto evasion of the particularity requirement.[132] While search execution and retention of materials are two sides of the same coin, this distinction could reflect differing law enforcement justifications and therefore necessitate distinct treatment upon review.

### 2. Considerations in Limiting the Scope of the Review or Deploying of Search Protocols

In the ex post evaluation of search reasonableness, courts have diverged on whether it is reasonable for law enforcement to manually review everything provided to them in an SCA warrant or whether officials must employ some limitation to minimize access to nonresponsive information. The government's ability to search every electronic record is analogous to its ability to review physical materials: If an agent would be allowed to review all of the records when they were printed and stored in a residence, why should she be precluded when they are stored digitally?[133] In response to this rhetorical question, some answer that ESI materials are truly different—ESI requires greater restriction and procedural care.[134] Unlike searching a desk or closet, SCA warrants have the potential to yield a size and scope of data incomparable to physical materials. The data may comprise gigabytes or even terabytes of data that service providers retain in situations where the record ordinarily would not have been kept by the individual if it was generated and first used in a physical space.[135] Underlying these concerns

132. *Id.*; *see, e.g.*, United States v. Lustyik, No. 2:12-CR-645-TC, 2014 WL 1494019, at *5 (D. Utah Apr. 16, 2014) ("The Government's knowledge of the activity being investigated developed over time. As the Government learned new details, the Government would go back and conduct targeted searches in the Relativity database using search terms for additional documents responsive to the warrants. From time to time, and based on developing knowledge of the investigation, documents that were previously marked as irrelevant were re-reviewed and marked as relevant.").

133. *See* United States v. Stabile, 633 F.3d 219, 237–40 (3d Cir. 2011) (holding that the search was reasonable since the detective "reasonably believed that [the folder] could contain evidence of financial crimes" and took measures to comply with the warrant's provisions); United States v. Williams, 592 F.3d 511, 521 (4th Cir. 2010) ("[T]he warrant impliedly authorized officers to open each file . . . and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's authorization."); United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009) ("[T]here may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders."); United States v. Sealed Search Warrant, No. 2:17-CR-103-VEH-TMP-1, 2017 WL 3396441, at *5 (N.D. Ala. Aug. 8, 2017) (holding that "'some perusal' is generally necessary to determine the 'relevance of documents to the crime'" and that "the investigative team *itself* is allowed to search despite the possibility that innocuous materials might be present" (quoting United States v. Slocum, 708 F.2d 587, 604 (11th Cir. 1983))).

134. *See* United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999); Ohm, *supra* note 50, at 6; Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 103–05 (1994) (discussing the implications of large data volumes in the context of computer storage).

135. *See* Ohm, *supra* note 50, at 6 ("Hard drives store more information about more people of a more sensitive nature than filing cabinets ever have; the comparisons aren't even close."). Even focusing specifically on materials that communications companies provide through SCA authorization, searching these accounts is arguably very different from searching physical

about the volume and breadth of the types of materials that might be included is the apprehension that access may equate to a "general exploratory rummaging" and dramatically expand beyond the warrant's authority.[136]

Even given these concerns about the volume and sensitivity of ESI searches specifically, some courts that have recognized the need for some limiting principles have left the precise protocol to the discretion of law enforcement, subject to judicial review for reasonableness ex post. For example, in the consideration of reasonableness, courts have rejected assertions that law enforcement should have employed a particular method of execution, such as utilizing an independent party to review emails,[137] recording the differentiation between "irrelevant" and "relevant" emails,[138] or requiring the use of keyword searches.[139] These courts reject these motions in part because they do not believe their role includes dictating how a search is conducted.[140]

### 3. Use of Crime-Type Designations, Date Restrictions, or Data-Type Specifications to Evaluate Particularity

Courts have also evaluated the constitutionality of a warrant ex post by examining whether the warrant was sufficiently particular with respect to the designation of a crime for which evidence can be seized, a temporal limitation on the date range of records, or the type of files sought as stated in the warrant. By considering whether a warrant describes the items to be seized as evidence pertaining to a specified crime, courts have ruled that such cases

---

materials due to gigabytes of storage available and the comingling of messages and data. *See id.*; *see also Carey*, 172 F.3d at 1275 (stating that analogizing ESI to physical record storage does not take into account the modern state of digital storage and leads to oversimplification of the law (citing Winick, *supra* note 134, at 108)).

136. *See In re* Search of Premises Known as Three Hotmail Accounts: [redacted]@hotmail.com, [redacted]@hotmail.com, [redacted]@hotmail.com Belonging to & Seized from [redacted], No. 16-MJ-8036-DJW, 2016 WL 1239916, at *4 n.10 (D. Kan. Mar. 28, 2016), *aff'd in part sub nom. In re* Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp., 212 F. Supp. 3d 1023 (D. Kan. 2016); Ohm, *supra* note 50, at 11.

137. *See* United States v. Harder, Crim. No. 15-1, 2016 WL 7647635, at *5 (E.D. Pa. Apr. 18, 2016); United States v. Shah, No. 5:13-CR-328-FL, 2015 WL 72118, at *18 (E.D.N.C. Jan. 6, 2015) (noting that "'outsiders' to an investigation may fail to recognize particular codes, concealment techniques, or other details that would not escape the notice of an officer more familiar with the circumstances of a case"); *see also* United States v. Lustyik, 57 F. Supp. 3d 213, 229 (S.D.N.Y. 2014) (finding that the government did not act in bad faith when it reviewed, among other items, the contents of defendants' email accounts without guidance of written search protocols).

138. *See* United States v. Lee, No. 1:14-cr-227-TCB-2, 2015 WL 5667102, at *1, *3–4 (N.D. Ga. Sept. 25, 2015).

139. *See* United States v. Kanodia, No. 15-10131-NMG, 2016 WL 3166370, at *6–7 (D. Mass. June 6, 2016) (rejecting the defendant's assertion that the government should have employed a keyword search or alternative procedures to limit the materials reviewed by the government).

140. *Id.* at *7 (noting that courts "generally will not interfere with the discretion of law enforcement in determining 'how best to proceed with the performance of a search authorized by warrant'" (quoting United States v. Tsarnaev, 53 F. Supp. 3d 450, 464 (D. Mass. 2014))).

have met Fourth Amendment particularity requirements.[141] The presence of a connection to specific alleged criminal activity sets these circumstances apart from searches for "general criminal activity," the latter of which may fall outside constitutional boundaries.[142]

Similarly, limiting the date range of the records sought is another recognized method to provide greater particularity.[143] Given courts' concern about the prospect of over seizing data in ESI cases, limiting the content that a service provider should deliver to materials within a specified date range limits exposure to potentially nonrelevant material at the first stage, especially if specific dates of criminal conduct are already known.[144] This is not to say that the seizure of the full date range of the account's existence is impermissible if probable cause supports the full time frame,[145] but it can similarly be a tool to achieve constitutional warrant particularity.

Further restrictions on data type, depending on the service provider and type of account sought, is another area of particularity that can be enforced at the first stage of the process. As shown in Appendices A and B, warrants to service providers commonly state the relevant time periods and enumerate the types of data subject to the warrant, including messages, profile posts and comments, page likes, and IP address information.[146] If certain types of data are not necessary or do not have a connection to the probable cause that supports the seizure of other items, there is an opportunity to add greater particularity to the warrant without affecting the mechanics of the government's subsequent review.[147] This ability to curtail the volume of results by date range and data type differentiates the particularity evaluation

141. *See* United States v. Deppish, 994 F. Supp. 2d 1211, 1221 (D. Kan. 2014) (finding that even without specified search protocol, limiting the seizure for items "with reference to a particular criminal statute" was a distinguishing factor).

142. *See Shah*, 2015 WL 72118, at *12–13 (citing United States v. Dickerson, 166 F.3d 667, 693 (4th Cir. 1999)).

143. *See, e.g.*, United States v. Blake, 868 F.3d 960, 974 (11th Cir. 2017) (holding that the warrants should have only requested records "from the period of time during which [the defendant] was suspected of taking part in [a] prostitution conspiracy").

144. *See* United States v. Henshaw, No. 15-00339-01-CR-W-BP, 2017 WL 1148469, at *6 (W.D. Mo. Feb. 24, 2017) (finding that a warrant that limited account information to a period of one year was sufficiently particular); *Shah*, 2015 WL 72118, at *14. This analysis can be conducted at the time of the warrant application. *See In re* Search of Info. Associated with Fifteen Email Addresses Stored at Premises Owned, Maintained, Controlled or Operated by 1&1 Media, Inc., Google, Inc., Microsoft Corp. & Yahoo! Inc., No. 2:17-CM-3152-WC, 2017 WL 4322826, at *5–6 (M.D. Ala. Sept. 28, 2017) (indicating that such temporal restriction is not sufficient at the second step of the search, but must be incorporated when describing the materials service providers are ordered to provide); *In re* Search of Google Email Accounts Identified in Attachment A, 92 F. Supp. 3d 944, 952–53 (D. Alaska 2015) (denying a search warrant application seeking the entire content of email accounts without providing a reason for an unrestricted time frame).

145. *See In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 391–92 (S.D.N.Y. 2014) (noting that some latitude should be given to law enforcement to make a determination about the relevance of materials after brief examination).

146. *See infra* Appendices A–B (separately listing each type of account data to seize).

147. *See Blake*, 868 F.3d at 974.

for SCA warrants, as this option is unavailable in computer or device searches where ESI is not obtained from a neutral third party.

### *C. The Plain View Doctrine and Regulating Use of Materials Outside the Scope of the Warrant*

The implications of the plain view doctrine in the context of digital searches have similarly been weighed by courts and academia in light of the two-step review of electronic materials.[148] Developed within the context of searches of physical locations, the plain view doctrine allows law enforcement officials to seize evidence they encounter inadvertently without meeting the ordinary warrant requirement.[149] The typical situation where this arises in the physical world, which is also directly applicable to the ESI context, is when law enforcement identifies "some other article of incriminating character" during the course of a search warrant execution for other specified items.[150]

Currently, circuit courts have a number of approaches to apply the plain view doctrine to electronic searches, necessitated by the two-step review process. The Fourth Circuit, in *United States v. Williams*,[151] has treated the plain view doctrine the same as it would in searches of physical locations.[152] On the other end of the spectrum, the Ninth Circuit, in *United States v. Comprehensive Drug Testing, Inc.*,[153] has suggested addressing the issue ex ante by encouraging magistrate judges to "insist that the government waive reliance upon the plain view doctrine."[154] In between these two positions,

148. *See generally* RayMing Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31 (2007) (asserting that the plain view doctrine should not be applied to ESI); Kerr, *supra* note 53 (discussing the potential need to narrow the plain view in the context of computer hard drive searches); Corey J. Mantei, Note, *Pornography and Privacy in Plain View: Applying the Plain View Doctrine to Computer Searches*, 53 ARIZ. L. REV. 985 (2011) (suggesting the development of plain view doctrine application to ESI through case law); 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 (2010) (proposing a balancing test to evaluate whether the plain view doctrine should permit evidence admission on a case-by-case basis); O'Leary, *supra* note 38 (discussing the circuit split and four varying approaches regarding the applicability of the plain view doctrine to ESI warrants); 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) (asserting that the plain view doctrine turns digital searches into general warrants).

149. Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) (plurality opinion) ("[U]nder certain circumstances the police may seize evidence in plain view without a warrant.").

150. *Id.*; *see also* Arizona v. Hicks, 480 U.S. 321, 326–28 (1987) (requiring the existence of probable cause to invoke the plain view doctrine and hazarding that the doctrine is not a tool to "extend a general exploratory search from one object to another until something incriminating at last emerges" (quoting *Coolidge*, 403 U.S. at 466)).

151. 592 F.3d 511 (4th Cir. 2010).

152. *Id.* at 523 (concluding that "the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents" and that the established requirements for seizure under the plain view doctrine apply).

153. 621 F.3d 1162 (9th Cir. 2010).

154. *Id.* at 1180 (Kozinski, C.J., concurring).

the Tenth Circuit "limits the scope of a search by permitting investigators to search only those containers that could reasonably hold items described in a warrant"[155] and the Seventh Circuit has followed a case-by-case approach to build policy incrementally.[156]

While the applicability of the plain view doctrine to search warrants for ESI may impact how magistrates review warrant applications ex ante and how judges review warrant executions ex post, the doctrine as an issue by itself largely remains outside the scope of this Note.[157] Still, it is important to recognize that ESI warrant applications are not insulated from preexisting search and seizure doctrine and concerns about the plain view doctrine can implicate a magistrate's decision when granting a warrant.[158]

### *D. Policy Suggestions and Proposed Amendments to Rule 41*

In response to these issues pertaining to the second-step execution of ESI warrants under Rule 41, scholars have suggested approaches centered on (1) encouraging magistrate judges to implement ex ante orders governing the methodology of the search, (2) relying on pure ex post reasonableness review, or (3) changing Rule 41 to impose explicit requirements regarding the time frame allowed for execution or the search protocol employed.

The first approach—encouraging magistrate judges to implement ex ante orders through the use of filter teams, keyword searches, service provider screening, and other mechanisms described in Part II.B—embraces the long-standing role of the magistrate judge as the independent evaluator of whether the constitutional requirements have been met to first authorize a warrant.[159]

---

155. O'Leary, *supra* note 38, at 238 & n.171 (quoting United States v. Ross, 456 U.S. 798, 822–24 (1982)).

156. *See* United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010).

157. For additional information about the applicability of the plain view doctrine in searches of ESI, see *supra* note 148.

158. *See In re* Search of Premises Known as: Three Hotmail Accounts: [redacted]@hotmail.com, [redacted]@hotmail.com, [redacted]@hotmail.com Belonging to & Seized from [redacted], No. 16-MJ-8036-DJW, 2016 WL 1239916, at *22 (D. Kan. Mar. 28, 2016), *aff'd in part sub nom. In re* Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp., 212 F. Supp. 3d 1023 (D. Kan. 2016); *In re* Search of Google Email Accounts Identified in Attachment A, 92 F. Supp. 3d 944, 951 (D. Alaska 2015) (expressing concern that the plain view doctrine could "transform electronic data search warrants into general warrants"); *In re* [REDACTED]@gmail.com, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014); *In re* U.S.'s Application for a Search Warrant to Seize & Search Elec. Devices from Edward Cunnius, 770 F. Supp. 2d 1138, 1144–47 (W.D. Wash. 2011) (discussing the characteristics of electronic searches that require the government to forgo use of the plain view doctrine to maintain constitutional searches).

159. *See, e.g.*, Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance*, 90 NEB. L. REV. 971, 1015 (2012); Athul K. Acharya, Note, *Semantic Searches*, 63 DUKE L.J. 393, 433 (2013); Day, *supra* note 57, at 497–98; Saylor, *supra* note 148, at 2854–57. Scholars have also suggested imposing elimination or use restrictions on the plain view doctrine. *See generally* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1 (2015) (proposing that use restrictions should apply to nonresponsive data and reserving judgment on the elimination of the plain view doctrine); Bryan K. Weir, Note, *It's (Not So) Plain to See: The Circuit Split on the Plain View Doctrine in Digital Searches*, 21

Similar to the reasoning of magistrate judges who have already issued secondary orders of this kind, this approach's focus is the "intrusiveness of searching and seizing the contents of stored e-mails and files" and the potential for coming into contact with a greater volume and range of personal materials.[160] In response to the potential differences in scope of electronic searches as well as the procedure that allows for review of these materials while in law enforcement's possession, specific methodology is necessary to ensure particularity.[161] As described in this Note, this approach is already being implemented to some extent, albeit without standardization.

Those who advocate for the second approach—relying on pure ex post reasonableness review—call for patience in letting the law develop over time to be consistent with existing search and seizure doctrine.[162] They assert that this approach will allow the justice system to reach a fair result naturally and without attempting to anticipate the methodologies that would weigh on reasonableness.[163] Given the fact-specific nature of reasonable search determinations, ex post review may have the advantage of seeing how the conduct unfolded and the implications of varying protocols in fact rather than trying to anticipate the result.[164] While suppression motions pertaining to electronic evidence are frequently reviewed, district courts and appellate judges vary considerably in their approaches to these issues.[165] Further, even when courts have chosen not to enforce measures imposed ex ante,[166] they have not precluded their continued use or alleviated the potential problems they can impose for subsequent reasonableness review.[167]

Finally, another suggestion involves amending Rule 41[168] to regulate the timing of the second-step search execution as well as to clarify the

---

GEO. MASON U. C.R.L.J. 83 (2010) (discussing the benefits of abolishing the plain view doctrine in digital searches).

160. Friess, *supra* note 159, at 1016.

161. *Id.*; *see, e.g.*, *In re Three Hotmail Email Accounts*, 2016 WL 1239916, at *24.

162. *See, e.g.*, Kerr, *supra* note 47, at 1276.

163. *See* Moshirnia, *supra* note 148, at 634 ("By implementing an ex post judicial balancing test weighing society's interest in protection against a defendant's interest in the privacy of the material searched, courts may render suppression judgments more consistently and honestly."); Samantha Trepel, Note, *Digital Searches, General Warrants, and the Case for the Courts*, 10 YALE J.L. & TECH. 120, 141 (2007).

164. Kerr, *supra* note 47, at 1293 ("The factual vacuum of ex ante and ex parte decisionmaking leads such restrictions to introduce constitutional errors that inadvertently prohibit reasonable search and seizure practices.").

165. *See supra* Part II.B.

166. *See, e.g.*, United States v. Filippi, No. 5:15-CR-133 (BKS), 2015 WL 5789846, at *4 (N.D.N.Y. Sept. 9, 2015) (choosing not to enforce the magistrate judge's "Addendum to Search Warrant," which stated that the electronic media search should be completed within sixty days of the warrant).

167. Kerr, *supra* note 47, at 1287 (arguing that "[e]x ante restrictions effectively deny courts an opportunity to announce the law in a de novo fashion").

168. There are no current proposed amendments to Rule 41. The most recent change, discussed at the last posted Committee meeting in April 2017, pertained to the 2016 amendment granting authority to issue warrants for remote electronic searches. *See* Advisory Comm. on Criminal Rules, Minutes 2 (Apr. 17, 2017), http://www.uscourts.gov/sites/default/files/spring_2017_criminal_rules_committee_meeting_minutes_final_0.pdf [https://perma.cc/ZAP6-F2HM].

particularity standards for the warrant.[169] First, this proposed rule change calls for a characterization of the device seized[170] and then applies a sliding scale for the allotted execution time.[171] Second, it proposes that warrant applications include an accompanying affidavit from the examiner stating that the methodology implemented would limit the scope of the search, such as through keyword searches, searches of stored memory, review of metadata, or searches of only selected file types.[172] These proposed amendments focus primarily on method and timeline of execution rather than directly targeting retention of nonresponsive material.

## III. LIMITATIONS OF AD HOC ELECTRONIC COMMUNICATIONS SEARCH WARRANT REGULATION AND PROPOSED MODIFICATION OF RULE 41

Although courts have responded to the gaps in the law on an ad hoc basis, the root problem is not an isolated occurrence. Due to the nature of warrants for ESI material, it is nearly guaranteed that law enforcement will obtain nonresponsive information from service providers. The issue of what to do with these materials is therefore a universal concern. Making readily workable amendments to Rule 41 would be the most appropriate and effective way of ensuring that baseline protections are met, which would provide greater guidance to law enforcement on what will be deemed a reasonable search in this context and would improve consistency in the execution of search warrants for electronic communications.[173] The changes this Note proposes encompass three main ideas: (1) separating review procedure for electronic communications under the SCA from materials seized directly from a subject (e.g., a computer, hard drive, or device from a search of a residence or other physical location), (2) establishing a cap on retention of materials deemed nonresponsive and limiting access to the case team after they have been designated as such, when technologically

169. O'Leary, *supra* note 38, at 233–34.

170. *Id.* (differentiating between a device that rises to an instrumentality of a crime and a device that is a mere storage vehicle).

171. *Id.* (proposing a range from thirty days to twelve months, with an option to apply for an extension).

172. *Id.* at 239–40. O'Leary further elaborates that in the event that the examiner sees evidence of a crime beyond the scope of the warrant, she should immediately stop her review and seek a subsequent warrant to expand the search. *Id.* at 240.

173. Inconsistency across jurisdictions may preclude obtaining a warrant or significantly curtail the effectiveness of its execution depending on which magistrate hears the application. For example, the same application that a magistrate judge in the Southern District of New York would grant could very likely be denied or subject to greater restriction if brought before Judge Waxse in the District of Kansas. *Compare In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 400 (S.D.N.Y. 2014) (refusing to impose ex ante restrictions on warrant execution), *with In re* Search of Premises Known as: Three Hotmail Email Accounts: [redacted]@hotmail.com, [redacted]@hotmail.com, [redacted]@hotmail.com Belonging to & Seized from [redacted], No. 16-MJ-8036-DJW, 2016 WL 1239916, at *24 (D. Kan. Mar. 28, 2016) (requiring ex ante restrictions on search warrant execution). While rational minds may disagree on the existence of probable cause or appropriate particularity in some cases, the variation in the context of ESI is arguably more pronounced.

feasible,[174] and (3) applying a procedural step to regulate use of nonresponsive material rather than restrict search methodology. Part III.A describes the insufficiency of the current inconsistent approaches to regulating and evaluating execution of electronic communications search warrants. Then, Part III.B details the elements of the proposed amendment to Federal Criminal Procedure Rule 41.

### *A. Limitations of the Warrant Regulation and Evaluation Status Quo*

The myriad measures discussed in Part II all generally point to the same concerns: how to mitigate the impact of nonresponsive material captured during the execution of these warrants and how to ensure that its inclusion does not turn the inquiry into an unconstitutional "general search."[175] Of the various restrictions imposed, some are not tailored to the root of the issue and collaterally affect the search for responsive data.

Efforts to impose a deadline for the execution of the second-step searches of electronic communications, or attempts to identify what length of time is no longer reasonable after the fact, do not have the same utility in this context as they do for physical items, namely, addressing issues of staleness and inconvenience to the owner of the content.[176] Absent this utility, determining that a search is unreasonable based solely on the duration of time to conduct it appears arbitrary. Although there are certainly privacy concerns implicated by the retention of materials that do not fall within the scope of a warrant, this issue could be better addressed by focusing on what is done after an item is deemed nonresponsive.[177]

Requiring specific search methodologies may also sweep too broadly and hinder the ability to conduct an effective search in the first place. Practically speaking, the use of keywords, filters, and other indicators for advanced searching are likely already employed to triage large data sets.[178] While they can have utility in terms of expediency, prohibiting a more thorough search when time and resources allow can raise concerns. Preselection of keywords

174. Depending on the file types the service provider uses to deliver data, the review platform available may not always have the technological capability to restrict access rights for items marked nonresponsive. Where it is technologically possible, such walling off should occur. Where it is not possible, the case team should make an effort not to reexamine those materials affirmatively marked nonresponsive.

175. *See supra* Part II (describing ex ante requirements that judges have imposed to ensure greater particularity and ex post review frameworks to determine warrant execution reasonableness in searches of ESI).

176. *See supra* notes 126–28 and accompanying text.

177. While delaying a search could be a mechanism to evade regulation of postsearch retention, it may prove more workable to identify cases where delay in conducting a search is a bad faith attempt to retain nonresponsive material rather than necessary to evaluate whether the search duration is reasonable. The latter is particularly complicated given the number of variables that could affect search duration and the lack of an accepted time frame. *See supra* Part II.B.1 (discussing the breadth of time periods deemed reasonable to execute the search).

178. *See* United States v. Sealed Search Warrant, No. 2:17-CR-103-VEH-TMP-1, 2017 WL 3396441, at *2 (N.D. Ala. Aug. 8, 2017) (positing that winnowing of the volume of documents may already be happening absent mandatory protocols as "Government agents generally do not manually search each and every document that is present").

can be incomplete and ineffective if coded language is employed, especially as law enforcement may not be aware of the specific language before the search execution but could ascertain from the patterns and context of the communications.[179] The suggestion that service providers conduct an initial search using such indicators and keywords is prone to the same pitfalls as initial searches run by law enforcement. In addition, it places a greater burden on the provider and delegates investigative functions to private parties.[180]

Approaches that call for the search to be conducted by an independent party, taint team, or special master could similarly prove too restrictive. The search itself might be less effective without the expertise and knowledge base of trained law enforcement officials who know the case and may be better able to identify evidentiary material.[181] In general, requiring the use of specific protocol in conducting a review of electronic communications could preclude use of constitutional search techniques and mechanisms that could identify responsive material with greater success.[182]

### *B. Modifying Rule 41 to Impose Retention Restrictions and Use-Based Procedures Instead of Execution Deadlines or Protocol Orders*

Instead of continuing with the current ad hoc approach or requiring law enforcement to select from a menu of possible restrictions ex ante, a future amendment to Rule 41 could offer rudimentary guidance without mandating specific measures that could curtail the ability to identify items within the scope of the warrant. First, the rule covering materials obtained via SCA warrants should be distinct in some ways from hard drives, computers, and devices obtained directly from the subject. While there are similarities in the volume and complexity of digital storage, there are also some important variations. For instance, duration of the execution and retention of copies of information from online accounts may have less serious implications on the subject than the seizure of a device from the home or office.[183] Additionally, the source of the materials can affect the forensic methodology necessary to access the relevant data. Significantly, in the case of SCA warrants, an additional source of particularity may be available by specifying a pertinent

179. *See supra* Part II.A.

180. *See supra* note 108 and accompanying text.

181. *See supra* note 108 and accompanying text; *see also In re* Search of Info. Associated with [redacted]@mac.com That Is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157, 165 (D.D.C. 2014) (discussing how service provider employees, "untrained in the details of the criminal investigation," are unlikely to have sufficient experience and skill to make determinations of the document's relevance to the criminal activity).

182. *See supra* note 102 and accompanying text.

183. *See supra* note 28 and accompanying text. As these materials are copies of records that service providers retain and do not involve removing property from the owner's possession, the subject is not deprived of his own records, documents, postings, or other communications.

date range or data type, which can limit what the service provider delivers to the government at the first step.[184]

Second, the issue of limiting access to material outside the scope of a warrant can be addressed without imposing specific ex ante requirements that require a procedure that may not be appropriate given the size and form of the materials returned. At the time of a search warrant application, it is frequently unknown how large the return will be and case-specific nuances can foreseeably lead to different redeterminations of reasonableness.[185] By focusing on the issue of retention of materials after the search has been completed rather than placing a time limitation on execution, the rule could instead restrict retention of materials deemed nonresponsive to the end of the case[186] and require the government to limit the case team's access to nonresponsive items, within technological capability. While, theoretically, mechanisms could be in place to petition the court to reaccess materials based on new information, the default procedure would limit the detrimental effect of the two-step process and mitigate the concerns expressed in cases such as *Ganias*.[187]

Third, and closely related to retention, the various protocols and procedures discussed in Part II also seek to minimize exposure to nonresponsive materials in the first place to mitigate the effects of the two-step process. However, regulation of the subsequent use of nonresponsive material—for instance, items that are evidence of a different crime—would be a better tailored approach. Regulating the use rather than the search addresses issues of nonresponsive material without undermining the practicality that the two-step process seeks to achieve. Limiting the applicability of the plain view doctrine is one such use-based approach that has been considered by courts over the last ten to fifteen years.[188] However, the purpose of the doctrine is the same irrespective of whether the search is

184. *See supra* notes 143–47 and accompanying text. While the ability to parse different types of records necessary depends on the provider, some have publicly stated the ability and willingness to limit types of data made available. *See Guidelines for Law Enforcement*, *supra* note 32 (requesting that law enforcement list the specific information sought); *Legal Process for User Data Requests FAQs*, *supra* note 32 ("In some cases we receive a request for all information associated with a Google account, and we may ask the requesting agency to limit it to a specific product or service."). Since SCA warrants require a service provider to deliver a specified set of data in its possession, this ability to limit seizure at the first step is unavailable in the case of searches of computers or devices in the subject's possession.

185. This was the advisory committee's concern with imposing additional requirements in 2009. *See supra* note 41 and accompanying text.

186. It may be necessary to retain a complete copy of the original materials provided to the government for authentication purposes and for proving the integrity of the files. *See* United States v. Scully, 108 F. Supp. 3d 59, 100 (E.D.N.Y. 2015); *In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 399 (S.D.N.Y. 2014); *see also* United States v. Tamura, 694 F.2d 591, 597 (9th Cir. 1982) (acknowledging the need, at times, to retain a complete copy of warrant materials for authentication purposes).

187. United States v. Ganias, 755 F.3d 125 (2d Cir. 2014), *rev'd en banc*, 824 F.3d 199 (2d Cir. 2016); *see supra* notes 130–32 and accompanying text.

188. *See supra* Part II.C (describing the circuit split on the applicability of the plain view doctrine to ESI searches).

for physical or electronic items.[189] Rather than be placed in an uncomfortable and counterintuitive position where the government or law enforcement agency would have to ignore evidence of another crime, requiring an additional procedural step to use items that were initially outside the scope of the warrant or to expand the search to cover those crimes prospectively could achieve a balance that is more consistent with existing search and seizure law.[190]

While recognizing that not all issues relating to the reasonableness of ESI warrants can be addressed ex ante—primarily because the Fourth Amendment reasonableness doctrine will still require case-specific determinations as to whether a given search is constitutional—the wide range of responses discussed in this Note illustrates how clarifying Rule 41's procedure can, to some extent, standardize the execution of second-step searches. Establishing baseline standards ex ante can provide more consistent privacy protection on the issue of record retention, while giving law enforcement officials greater confidence that their methodology will be effective and considered valid.

## CONCLUSION

As we move further into the digital age, search and seizure procedure for electronic content continues to develop, although in varied and inconsistent ways. The practical necessity of the two-step process—and with it the virtual guarantee that the government, at least initially, will have access to materials falling outside the scope of the warrant—will continue to raise questions of whether the nature of these searches requires additional procedural restrictions and what to do with the nonresponsive data. While it is not feasible or even advisable to escape case-specific determinations of reasonable searches ex post, amending Federal Criminal Procedure Rule 41 to address the retention and use of nonresponsive data could serve to curtail practices that undermine the efficacy of the search while also providing greater guidance on reasonableness in the ESI context and adding protection for account holders.

189. *See supra* note 152 and accompanying text.

190. *See supra* notes 169–72 (describing a proposal that would impose additional procedural steps when law enforcement encounters evidence of a crime beyond the scope of a warrant's authority).

## APPENDIX A

### *Proposed Search Warrant in the Case of the 2013 Navy Yard Shooter*[191]

Items for Facebook to provide to the government:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have been tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and other information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of the account's usage of the "Like" feature, including all Facebook posts and non-Facebook webpages and content that the user has "liked";

(i) All information about the Facebook pages that the account is or was a "fan" of;

(j) All past and present lists of friends created by the account;

(k) All records of Facebook searches performed by the account;

(l) All information about the user's access and use of Facebook Marketplace;

(m) The types of service utilized by the user;

191. *In re* Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis That Is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 3–4 (D.D.C. 2013) (alterations in original).

(n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Information that the government would seize:

(a) Records and information, and items related to violations of [18 U.S.C. §§ 1111, 1113, and 1114];

(b) Records, information, and items related to the identity of Aaron Alexis;

(c) Records, information, and items related to the Washington Navy Yard or individuals working or present there;

(d) Records, information, and items related to any targeting of, or planning to attack, the Washington Navy Yard or individuals working or present there, or any records or information related to any past attacks;

(e) Records, information, and items related to the state of mind of Alexis, or any other individuals seeking to undertake any such attack and/or the motivations for the attack;

(f) Records, information, and items related to any organization, entity, or individual in any way affiliated with Alexis;

(g) Records, information, and items related to any associates of Alexis or other individuals he communicated with about his planned violent attacks, including the one perpetrated at the Washington Navy Yard on September 16, 2013;

(h) Records, information, and items related to Alexis or his associates' schedule of travel or travel documents;

(i) Records, information, and items related to any firearms or ammunition;

(j) Records, information, and items related to any bank records, checks, credit card bills, account information, and other financial records; and

(k) Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts.

## APPENDIX B

*Court Order, Amending the Proposed Search Warrant, in the Case of the Navy Yard Shooter*[192]

(1) Facebook, Inc. is instructed to comply strictly with the terms of this Order and to provide only the following materials to the government:
   (a) All contact and personal identifying information related to the Account, including the Account holder's full name, user identification number, birth date, gender, contact e-mail addresses, Facebook login details, physical addresses (including city, state, and zip code), telephone numbers, screen names, websites, billing information, and other personal identifiers associated with the Account;
   (b) All records relating to use of the Account, including session times, login/logout times, IP addresses from which it was accessed, and the types of services used;
   (c) All records related to the Account's privacy settings;
   (d) All activity logs for the Account and all other records showing the Account's posts, messages, and other activities on Facebook;
   (e) All photos and videos uploaded by the Account;
   (f) All records—but not content—relating to the Account's list of friends, including any friend requests that were pending or rejected;
   (g) All records of communications—but not content—sent to the Account from another account or group, including the user ID of that account or group and the user name of the account or group, the date and time of the communication, whether attachments existed (subject to the limitations expressed *infra*); and
   (h) All records—including content—of communications generated by or sent from the Account to any other user or group (including postings).

(2) Facebook, Inc. is instructed to comply strictly with the terms of this Order and is PROHIBITED from providing the following materials to the government without an additional Order from this Court:
   (a) The contents of any communications sent to the Account;
   (b) Photos and videos uploaded by other users, even if Aaron Alexis is "tagged" or otherwise mentioned or identified in the photos or videos; and
   (c) Any records or details about any groups of which the Account was a member, including those that were "liked" or of which the Account was a "fan" (or other similar term) other than the user ID and name of the user or group.

192. *Id.* at 5–6.

(3) Upon receipt of the above-described records and content, the government will then conduct a search to determine which relate to the following areas of investigation, as identified in the government's application. These areas are:
   (a) Allegations that Aaron Alexis violated:
      (i) 18 U.S.C. § 1111;
      (ii) 18 U.S.C. § 1113;
      (iii) 18 U.S.C. § 1114;
   (b) Records and content related to the identity of Alexis;
   (c) Records and content related to any targeting of, or plans to attack, the Washington Navy Yard or individuals working or present there;
   (d) Records and content related to any other attacks planned or carried out by Alexis;
   (e) Records and content related to the motive of Alexis for the attack, including evidence of mental illness;
   (f) Records and content related to whether Alexis had any accomplices in planning or carrying out the attack on the Washington Navy Yard or individuals working or present there;
(4) All records and content that the government determines are NOT within the scope of the investigation, as described above, must either be returned to Facebook, Inc., or, if copies (physical or electronic), destroyed.

## APPENDIX C

*Ex Ante Protocols*

| Process | Brief Description | Policy Objective |
|---|---|---|
| **Execution Deadline** | Creates a deadline by when the second-step review of material must be completed. | Reasonableness of the search. |
| **Retention Limit** | Places a restriction on the amount of time law enforcement can retain nonresponsive material. (Usually at the end of the case.) | Reasonableness of the search. |
| **Independent Review**<br><br>**(including use of a special master or "taint team")** | The search for materials that fall under the scope of the warrant is conducted by an independent (non-law enforcement) group of reviewers, or, alternatively, by a unit not associated with the case team.<br><br>While there are differences between special masters and taint teams, they seek to achieve the same purpose of limiting case team access to nonresponsive material. Those conducting the review pass along the responsive material and do not provide any information about the items deemed nonresponsive. | Reasonableness of the search. Serves to limit law enforcement access to material not within the scope of the warrant. |

| Process | Brief Description | Policy Objective |
|---|---|---|
| **Keyword Search and Filtering**<br><br>**(applies similarly to use of other filtering parameters)** | Requires the execution of ESI warrants to utilize specified keyword searches based on the facts of the case and probable cause findings outlined in the warrant application. Law enforcement is not permitted to review every file or document. | Particularity of the warrant and reasonableness of the search. Serves to limit law enforcement access to material not within the scope of the warrant. |
| **Service Provider Screening** | Similar to the keyword search, this process requires electronic communications service providers to use search terms or filtering parameters to limit the materials provided to law enforcement at the first step. | Particularity of the warrant and reasonableness of the search. Serves to limit law enforcement access to material beyond the scope of the warrant. |

## APPENDIX D

*Ex Post Review Bases*

| Process | Brief Description | Policy Objective |
|---|---|---|
| **Execution Time Limit** | When deciding the admissibility of materials seized pursuant to ESI search warrants, the court determines whether the amount of time taken to conduct the search was reasonable. Most warrants do not state a particular deadline ex post but evaluate whether the particular length of time taken was reasonable given the circumstances. | Reasonableness of the search. (Finding that reasonableness applies to all aspects of the search.) |
| **Failure to Follow Review Protocol**<br><br>**(not specified in warrant)** | Arguments have been made by defense attorneys that the failure to employ various limitations on search methodology (even without specification in the warrant) is unreasonable. Generally, these arguments are not successful. | Reasonableness of the search. Serves to limit law enforcement access to material not within the scope of the warrant. |
| **Noncompliance with Review Protocol**<br><br>**(specified in warrant ex ante)** | Noncompliance with the search requirements in the warrant is per se unreasonable and evidence obtained pursuant to such search should not be admitted. These decisions are often framed in language of compliance with an order rather than reasonableness. | Reasonableness of the search. |

| Process | Brief Description | Policy Objective |
|---|---|---|
| **Non-Enforcement of Specified Ex Ante Protocol** | The refusal to exclude evidence obtained despite failure to follow a search methodology required in the warrant under the rationale that reasonableness of the search depends on case-specific circumstances that could change from what was anticipated ex ante. Focus is on reasonableness rather than compliance. | Reasonableness of the search. |
| **Evaluation of Data Limitations** | Consideration of whether the warrant was sufficiently particular with respect to the stated crimes to which the seized evidence should pertain as well as the date range of records and type of data sought. | Warrant particularity and whether supported by probable cause. |