Let the Magistrates Revolt: A Review of Search Warrant Applications for Electronic Information Possessed by Online Services

*Reid Day**

I. INTRODUCTION

Every day, millions of Americans send and receive email, update social media statuses, post blogs, and otherwise enjoy Internet services that enrich their lives in countless ways. These Internet users are increasingly aware that the companies providing their beloved Internet services maintain records about customers' activity online.[1] While some Americans are ambivalent about the decrease of privacy online, many Americans consider privacy important and struggle to understand the changing online privacy landscape.[2] It is difficult to know how much data is collected online and how that information is used.[3] An astonishingly revealing trail of digital information results from synthesizing records about every email, Facebook post, or tweet.[4] That

---

* J.D. Candidate, May 2016, University of Kansas School of Law; B.A., 2009, University of Kansas. I would like to thank my Note & Comment Editor, Patrick Springer, and Faculty Reader, Dean Melanie D. Wilson, for their invaluable support throughout this process. The University of Kansas School of Law misses Dean Wilson, but the University of Tennessee School of Law is fortunate to have a spectacular new Dean. I would like to thank Bryce Langford, Nicki Rose, and the entire *University of Kansas Law Review* board and staff for their help with this article and all the good times on Green Hall's fifth floor. Rock Chalk Jayhawk.

1. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

2. *Id.*

3. *Online Tracking and Behavioral Profiling*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/consumer/online_tracking_and_behavioral.html (last visited Oct. 14, 2015); *see also Privacy and Consumer Profiling*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/profiling/default.html (last visited Oct. 14, 2015) (discussing types of data collected and data collectors).

4. *See, e.g.*, Kashmir Hill, *Here's a Tool to See What Your Email Metadata Reveals About You*, FORBES (July 10, 2013, 2:20 PM), http://www.forbes.com/sites/kashmirhill/2013/07/10/heres-a-tool-to-see-what-your-email-metadata-reveals-about-you/ (discussing amount of data stored in metadata that many do not know exists); Elizabeth Dwoskin, *In a Single Tweet, as Many Pieces of Metadata as There Are Characters*, WALL ST. J.: DIGITS (June 6, 2014, 4:46 PM), http://blogs.wsj.com/digits/2014/06/06/in-a-single-tweet-as-many-pieces-of-metadata-as-there-are-characters/ (explaining that a single 140 character Tweet contains "150 separate points of so-called

information can be—and often is—stored indefinitely by service providers.[5]

Unfortunately, criminals also utilize the wide range of services offered by Internet companies to facilitate criminal activities. Internet services provide a quick way to share information and organize criminal activity, allowing a user to create an account by only providing basic information such as a username and password.[6] Though a criminal may provide a fake name or address, the digital information generated from the criminal's online activity is more difficult to manipulate and can reveal personal details including, with the help of an Internet Service Provider, a user's physical location.[7] Understandably, investigators are interested in obtaining digital information that paints a detailed picture of an individual's daily activities.[8] As a result, Apple, Google, and other online services are quickly becoming a go-to source for law-enforcement investigations.[9] The amount and type of information gathered from searching and seizing an entire online account is invaluable to government investigators because that information tells a precise and objective story about the user's activity online and offline. An investigator can piece together a compelling theory of a crime by searching an email or social media account and finding information pertaining to an individual's activity.[10]

Government investigators obtain electronic information in a number

---

metadata").

5. *E.g.*, Nate Anderson, *Why Google Keeps Your Data Forever, Tracks You with Ads*, ARS TECHNICA (Mar. 8, 2010, 8:20 AM), http://arstechnica.com/tech-policy/2010/03/google-keeps-your-data-to-learn-from-good-guys-fight-off-bad-guys/.

6. The website Fake Name Generator, for instance, automatically creates a false e-mail address and a completely false identity to go along with it, including name, age, address, and height. FAKE NAME GENERATOR, www.fakenamegenerator.com (last visited Oct. 7, 2015).

7. Cale Guthrie Weissman, *What Is an IP Address and What Can It Reveal About You?*, BUSINESS INSIDER (May 18, 2015, 4:45 PM), http://www.businessinsider.com/ip-address-what-they-can-reveal-about-you-2015-5.

8. *See* G.W. Schulz & Daniel Zwerdling, *Easily Obtained Subpoenas Turn Your Personal Information Against You*, THE CTR. FOR INVESTIGATIVE REPORTING (Sept. 30, 2013), http://cironline.org/reports/easily-obtained-subpoenas-turn-your-personal-information-against-you-5104 (explaining various ways that investigators can gather electronic information with relative ease).

9. *See* Tim Cushing, *Judge John Facciola on Today's Law Enforcement: I'd Go Weeks Without Seeing a Warrant for Anything 'Tactile'*, TECHDIRT (Mar. 3, 2015, 2:34 PM), https://www.techdirt.com/articles/20150221/13433030098/judge-john-facciola-todays-law-enforcement-id-go-weeks-without-seeing-warrant-anything-tactile.shtml (describing law enforcement's preference for digital searches rather than tactile searches).

10. *See, e.g.*, *In re* Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis, 21 F. Supp. 3d 1, 3–6 (D.D.C. 2013) (describing the government's request to compel Facebook to disclose an entire account belonging to the alleged shooter in a 2013 incident at Washington, D.C.'s Navy Yard facility).

of ways.[11] This Comment focuses on investigations where a warrant is sought to compel the company providing an Internet service to disclose the records of an individual user. Investigators rely on a two-step process from the Federal Rules of Criminal Procedure Rule 41 that is specifically designed for this purpose. A lack of guidance regarding limits on the type and amount of electronic information that government investigators can compel an Internet service provider to disclose leads to Rule 41's use as a tool to obtain the entirety of an individual's activity on a particular online service.

Although government investigations necessarily must seek electronic data to effectively fight crime, the Fourth Amendment must protect the vast amount of electronic information generated by Internet users. The data generated from our online activities must be protected because it reveals the innermost private and intimate aspects of our lives.[12] But the law today is murky, confusing, and outdated.[13] While not always statutorily required, a warrant is increasingly required in federal investigations.[14] The problem becomes not whether the government must seek a warrant in a particular investigation, but whether the government's warrant application for electronic information using Rule 41's two-step process ensures Americans are protected by the Fourth Amendment in today's digital world. When law enforcement utilizes Rule 41's two-step process, the search warrant applications are often overbroad and lacking specificity.[15] As a result, a Fourth Amendment violation can occur if the government exceeds the scope of the search warrant or indefinitely retains electronic data to conduct searches not covered by the original search warrant.[16]

---

11. *See* Theodoric Meyer, *No Warrant, No Problem: How the Government Can Get Your Digital Data*, PROPUBLICA (June 27, 2014, 10:29 AM), https://www.propublica.org/special/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data (explaining the ways in which investigators can retrieve electronic information, including ways investigators can get the information without going through the normal warrant process).

12. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (citing Rios v. United States, 364 U.S. 253, 260–61(1960); *Ex parte* Jackson, 96 U.S. 727, 733 (1877))); Riley v. California, 134 S. Ct. 2473, 2488–91 (2014) (discussing the immense storage capacity of modern cell phones, which implicates privacy concerns with regard to the extent of information that could be accessed on the cell phone).

13. *See infra* Part II.B.1.

14. *See infra* Part II.B.2.

15. *See, e.g.*, *In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@Gmail.com, 33 F. Supp. 3d 386, 388 (S.D.N.Y. 2014) ("The search warrant directs Google to provide to the Government 'all content and other information within the Provider's possession, custody, or control associated with' the email account . . . .").

16. *See, e.g.*, United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006–07 (9th

To ensure that Americans' Fourth Amendment rights are protected, Rule 41's two-step process should require government investigators, or a reviewing magistrate judge, to include limitations on the search and seizure of electronic information. The limitations recommended by this Comment address concerns about whether government investigators using Rule 41's two-step process have shown sufficient probable cause and stated what information they seek to retrieve with particularity.

Currently, Rule 41's two-step process allows government investigators to request an expansive amount of data, but the Rule does not require safeguards and limitations that ensure electronic information is not collected in an overbroad manner that violates an individual's Fourth Amendment rights.[17] Magistrate judges are well suited to address this issue because Rule 41 requires a magistrate's approval of the government's search warrant application. These judges can impose limitations on government searches and seizures that strike a balance between the government's interest in fighting crime and an individual's Fourth Amendment rights. While no two investigations are identical, there are reasonable concerns regarding the sufficiency of search warrants for online accounts. These concerns may be addressed by the imposition of modest limitations on the government's acquisition and use of electronic information prior to or after the execution of a search warrant. In the absence of congressional guidance on warrant procedures for electronic information or privacy-protective amendments to Rule 41, magistrate judges are best positioned to address this gap in Fourth Amendment law by imposing limitations on warrant applications that utilize Rule 41's two-step process for electronic information.

This Comment proceeds in two parts. Part II explains the extent of information held by service providers on individual users and details the difficulty of applying Fourth Amendment law to electronic information. Part II also explains current law governing search warrants for electronic information, finding that a warrant is increasingly the tool relied upon by government investigators. Part II then describes Rule 41's procedural steps to obtain a search warrant for electronic information and concludes by examining decisions in three cases involving overbroad warrant applications. Part III explains the inadequacy of Rule 41's two-step

---

Cir. 2009) (describing violations of search warrants related to the government's investigation of a company allegedly providing steroids to Major League Baseball players), *vacated*, 621 F.3d 1162 (9th Cir. 2010); United States v. Ganias, 755 F.3d 125, 137–38 (2d Cir. 2014) (finding the government violated the defendant's Fourth Amendment rights by retaining records outside the scope of a warrant for more than two and a half years), *reh'g granted*, 791 F.3d 290 (2d Cir. 2015).

17. *See infra* Part II.C.

process for electronic information and highlights crucial 2009 Amendment Advisory Committee Notes regarding searches and seizures of electronic information. This Comment finds Rule 41's two-step process does not sufficiently protect Americans' electronic information. To address this problem, this Comment argues for transparency and the imposition of one or more affirmative limitations on the government's search and seizure of electronic information as two ways that the process can be improved to ensure the Fourth Amendment adequately protects the information generated by our online activities.

II. BACKGROUND

A. Current Problem

The Fourth Amendment prohibits the issuance of a warrant that is not supported by probable cause or a particular description of the person or things to be seized. It is unclear how this prohibition applies to online services that collect and indefinitely store records that detail a user's every activity on that particular service. This information can tell an incredibly detailed story about a person's activities online and offline.[18] This section discusses the massive amounts of data that individuals create every day online and traces the history of Fourth Amendment law as it struggles to keep pace with our digital society.

1. Digital Trails Reveal Personal Tales

Austrian law student Max Schrems discovered how comprehensive his digital trail was when he forced Facebook to disclose the digital records that the company retained on Schrems's activity on the popular social networking site.[19] Although Schrems challenged Facebook under the European Union's data-protection laws, his case convinced Facebook to give all users the ability to download a copy of the company's records of their individual activities, regardless of their country's laws.[20]

---

18. *See* Robert Krulwich, *How Much Do They Know About Me in the 'Cloud'?*, NAT'L PUB. RADIO (Feb. 27, 2012, 11:10 AM), http://www.npr.org/sections/krulwich/2012/02/27/147497042/how-much-do-they-know-about-me-in-the-cloud (providing a short video on the immense amounts of data collected by online services).

19. Kashmir Hill, *Max Schrems: The Austrian Thorn in Facebook's Side*, FORBES (Feb. 7, 2012, 10:03 AM), http://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/.

20. *Id.*; *Downloading Your Info*, FACEBOOK, https://www.facebook.com/help/131112897028467/ (last visited Oct. 12, 2015).

Facebook, like many other popular Internet services, retains data on nearly every interaction a user has with the site.[21] The comprehensive range of data Facebook retains includes, but is not limited to: credit card data, friend requests,[22] Internet Protocol addresses showing a user's physical location when logging into the site, content of messages sent and received via the site's messaging service, all searches queried on the site, membership in groups, events, religious and political views, and wall posts.[23] The universe of information is often hundreds of pages thick and can provide a detailed view of an individual's life online and offline.[24]

While the extent of the collection, use, and retention of data is often unclear, Facebook's practices do not significantly differ from other companies offering services online. Amazon, Skype, Apple, Microsoft, and other popular services maintain digital dossiers on their users.[25] Additionally, many large Internet companies provide ancillary services, such as an online address book, a personal calendar, photo-sharing services, or a blogging platform.[26] Millions of Americans log in to these services every day to engage in countless activities such as communicating with friends and family, shopping online, or operating a small business. These services make our lives easier, but our online activities can be used to piece together an incredibly rich tale of our lives.

---

21. *See Data Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy (last visited Oct. 13, 2015). Facebook and similar sites are routinely vague about their data retention policies. *Id.* Facebook states, "[w]e store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services." *Id.*

22. Friend requests includes sent requests, received and pending requests, deleted requests, and removed friends. *Accessing Your Facebook Data*, FACEBOOK, https://www.facebook.com/help/405183566203254 (last visited Oct. 13, 2015).

23. *Id.*

24. Kashmir Hill, *Facebook Keeps a History of Everyone Who Has Ever Poked You, Along with a Lot of Other Data*, FORBES (Sept. 27, 2011, 4:36 PM), http://www.forbes.com/sites/kashmirhill/2011/09/27/facebook-keeps-a-history-of-everyone-who-has-ever-poked-you-along-with-a-lot-of-other-data/.

25. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084, 1089 (2002); Mary Graw Leary, *Katz on a Hot Tin Roof—Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 AM. CRIM. L. REV. 341, 343–45 (2013); Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 15 & n.117 (2013).

26. *See, e.g.*, *Products*, GOOGLE, http://www.google.com/about/products/ (last visited Oct. 13, 2015); *Products*, YAHOO, https://info.yahoo.com/privacy/us/yahoo/products.html (last visited Oct. 13, 2015).

2. Adapting the Fourth Amendment to Modern Technology

The Fourth Amendment guarantees the rights of citizens against unreasonable searches and seizures:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[27]

The purpose of the Fourth Amendment is "to safeguard the privacy and security of individuals against arbitrary invasions by government officials."[28] And, "the 'touchstone of the Fourth Amendment is reasonableness.'"[29] Whether government action is reasonable is "measured in objective terms by examining the totality of the circumstances."[30] Reasonableness requires a warrant before a search or seizure occurs unless the government's conduct is within an exception to the warrant requirement, such as exigent circumstances.[31] An investigator must present a search warrant application for approval by a magistrate judge.[32] The detached and neutral magistrate's scrutiny is "intended to eliminate altogether searches not based on probable cause."[33] The application must set forth the facts and circumstances giving rise to the government's probable cause to believe that the suspect committed, or will commit, a criminal offense, or to believe that evidence of a criminal offense will be found on the premises to be searched.[34] The application must also describe any items and areas to be searched and seized with particularity.[35] "[T]he scope of a lawful search

27. U.S. CONST. amend. IV.

28. Camara v. S.F. Mun. Ct., 387 U.S. 523, 528 (1967).

29. Ohio v. Robinette, 519 U.S. 33, 39 (1996) (quoting Florida v. Jimeno, 500 U.S. 248, 250 (1991)); *see also* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (explaining that "a person has a constitutionally protected reasonable expectation of privacy.").

30. *Robinette*, 519 U.S. at 39.

31. *Katz*, 389 U.S. at 357.

32. *See* FED. R. CRIM. P. 41(b), (d) (detailing how to obtain a warrant from a magistrate judge).

33. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971). "[A]ny intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity." *Id.* (citations omitted).

34. *See* FED. R. CRIM. P. 41(c)–(d) (listing reasons for issuing a search warrant and requiring probable cause); *see also* Illinois v. Gates, 462 U.S. 213, 237–39 (1983) (explaining the amount of evidence required for a magistrate judge to find probable cause to issue a warrant).

35. U.S. CONST. amend. IV; *see also* Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one 'particularly describing the place to be searched and the persons or things to be seized.'").

is 'defined by the object of the search and the places in which there is probable cause to believe that it may be found.'"[36] The probable cause and particularity requirements are designed to avoid issuance of a "general warrant" where the government conducts a "general, exploratory rummaging in a person's belongings."[37] The particularity requirement also "assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search."[38]

Application of the Fourth Amendment to the Internet is an unsettled area of law.[39] Technological advances and accompanying law enforcement techniques present novel issues in Fourth Amendment law. For example, the practice of wiretapping, where investigators intercept telephone conversations, was not initially considered a search or seizure under the Fourth Amendment.[40] In a dissenting opinion that stands the test of time as remarkably accurate, Justice Brandeis warned of future forms of espionage "by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[41] Nearly forty years after its decision in *Olmstead*, the Supreme Court held that a wiretap without a warrant violated the Fourth Amendment.[42] Later that same year, in *Katz v. United States*, the Supreme Court, in an

---

36. *Garrison*, 480 U.S. at 84 (quoting United States v. Ross, 456 U.S. 798, 824 (1982)). "Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase." *Id.* at 84–85 (quoting *Ross*, 456 U.S. at 824).

37. *Coolidge*, 403 U.S. at 467 (gathering cases). *See, e.g.*, Boyd v. United States, 116 U.S. 616, 624–30 (1886) (discussing history of constitutional search and seizure law); Olmstead v. United States, 277 U.S. 438, 463 (1928) (noting that the Fourth Amendment was "directed against general warrants"), *overruled on other grounds by* Katz v. United States, 389 U.S. 347, 353 (1967); *Garrison*, 480 U.S. at 84 (discussing particularity requirement of the Fourth Amendment).

38. Groh v. Ramirez, 540 U.S. 551, 561 (2004) (quoting United States v. Chadwick, 433 U.S. 1, 9 (1977)); *contra* United States v. Grubbs, 547 U.S. 90, 99 (2006) (Justice Scalia rejects the notion of particularity serving as an assurance to the property owner, arguing that "neither the Fourth Amendment nor Federal Rule of Criminal Procedure 41 imposes such a requirement" (citations omitted)).

39. Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1006 (2010) [hereinafter *Fourth Amendment*]; *see also* Riley v. California, 134 S. Ct. 2473, 2488–91 (2014) (holding that a cell-phone search presents novel issues for the Court due to the device's immense storage capacity); United States v. Jones, 132 S. Ct. 945, 949, 954–55 (2012) (finding that the warrantless use of a GPS attached to a suspect's car violated the Fourth Amendment on the basis of a trespass violation (Scalia, J., majority opinion) or a violation of the suspect's reasonable expectation of privacy (Sotamayor, J., concurring)).

40. *Olmstead*, 277 U.S. at 465–66.

41. *Id.* at 474 (Brandeis, J., dissenting).

42. Berger v. New York, 388 U.S. 41, 63–64 (1967).

attempt to adapt to new technologies, introduced a new test to determine the reasonableness of an expectation of privacy.[43] In *Katz*, the Supreme Court found that conversations in a public phone booth, when the door was shut behind the occupant, were protected by the Fourth Amendment because the occupant possessed both a subjective and objective expectation of privacy.[44]

In recent years, the Court tackled Global Positioning System (GPS) tracking,[45] thermal imaging devices,[46] and whether a warrant is required to search a cell phone seized during a lawful arrest.[47] When holding that the use of a GPS tracking device constituted a search under the Fourth Amendment, the Court grounded its reasoning in both trespass law and the *Katz* reasonable-expectation-of-privacy test.[48] These recent decisions demonstrate that the Supreme Court is worried about the Fourth Amendment rights of Americans in an era where technologies are more pervasive and susceptible to government use in espionage than previously seen.[49] As investigative techniques closely resemble the techniques Justice Brandeis warned of in *Olmstead*, the Fourth Amendment must keep pace with technological changes and protect Americans from unreasonable invasions into their online lives.

The difficulty of ensuring that the Fourth Amendment keeps pace with technological changes is evident when determining if probable cause and particularity requirements of the Fourth Amendment are met in a search warrant application for electronic information. Probable cause and particularity share an interconnected role at the outset of a search.[50] Probable cause ensures items identified for search and seizure are connected with criminal activity, and it specifically identifies the places or persons to be searched, thereby ensuring probable cause is tailored to the alleged crimes, rather than a "general, exploratory rummaging in a person's belongings."[51]

---

43. Katz v. United States, 389 U.S. 347, 353 (1967).

44. *Id.* at 353, 358–59.

45. United States v. Jones, 132 S. Ct. 945, 949 (2012).

46. Kyllo v. United States, 533 U.S. 27, 34–35 (2001).

47. Riley v. California, 134 S. Ct. 2473, 2488–89 (2014).

48. *Jones*, 132 S. Ct. at 949–53.

49. *See id.* at 956 (Sotomayor, J., concurring) (highlighting concerns that "unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse" and noting that the acquisition of "intimate information about any person . . . may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'").

50. Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored Email Surveillance*, 90 NEB. L. REV. 971, 985 (2012).

51. *Id.* at 985–86.

Traditionally, establishing probable cause requires showing a "fair probability that contraband or evidence of a crime will be found in a particular place."[52] In the digital context, probable cause is established when the electronic information "contain[s] contraband, evidence of a crime, fruits of a crime, or the instrumentality of a crime."[53] In the context of the search and seizure of an electronic account there are serious problems with Rule 41's two-step process involving probable cause. Probable cause will rarely be established to search and seize an entire electronic account unless the government is in some way able to demonstrate that the entire account is used solely for the purpose of committing the alleged crime.[54]

The particularity requirement also presents unique challenges when applied to a search warrant for electronic information. The Fourth Amendment's particularity requirement is of increased importance in the digital era when intermingled documents and files are stored in a single place.[55] Due to the potential for intermingled documents and other electronic information, "warrants for computer searches must *affirmatively limit* the search to evidence of specific federal crimes or specific types of material."[56] Thus, a search warrant application for electronic information must meet Fourth Amendment particularity requirements describing "the place to be searched, and the persons or things to be seized."[57] However, a brief review of documents to determine relevancy to an ongoing investigation is necessary.[58] As Fourth Amendment law and the search warrant application process is applied to new technologies, a proper balance must be found between the

52. Illinois v. Gates, 462 U.S. 213, 238 (1983).

53. Friess, *supra* note 50, at 982 (citing FED. R. CRIM. P. 41(c)).

54. *See, e.g.*, *In re* Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, Nos. 13-MJ-8163-JPO; 13-MJ-8164-DJW, 13-MJ-8165-DJW; 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 U.S. Dist. LEXIS 123129, at *27 (D. Kan. Aug. 27, 2013) ("The target accounts may contain large numbers of emails and files unrelated to the alleged crimes being investigated or for which the government has no probable cause to search and seize."); *In re* Search of Info. Associated with @mac.com, 13 F. Supp. 3d 145, 152 (D.D.C. 2014) ("Here, the warrant describes only certain emails that are to be seized—and the government has only established probable cause for those emails. Yet it seeks to seize all e-mails by having them 'disclosed' by Apple."), *vacated*, 13 F. Supp. 3d 157 (D.D.C. 2014).

55. *See, e.g.*, United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (noting the difficulties presented by the "modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers").

56. *Id.* (quoting United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005)).

57. U.S. CONST. amend. IV.

58. *See In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@Gmail.com, 33 F. Supp. 3d 386, 393 (S.D.N.Y. 2014) (citing precedent recognizing need to review information seized in a valid search to determine relevancy to investigation).

interconnected concepts of probable cause and particularity.

B. Current Law

Investigators are not always required to obtain a search warrant for some types of electronic information. However, compelled disclosure of the contents of communications—allowing investigators to read user conversations—often requires a warrant. This section describes the law currently governing the compelled disclosure of electronic information—the Stored Communications Act. The law's structure and outdated nature often result in the decision to obtain electronic information by applying for a search warrant, rather than a subpoena, which is available with a lesser showing from the government. This section concludes by showing that search warrant applications for electronic information are a tool increasingly relied upon for two reasons. First, there are concerns about the constitutionality of obtaining the contents of communications without obtaining a warrant. Second, companies that provide Internet services require a warrant before an individual's records are disclosed.

1. Stored Communications Act

Government access to Americans' electronic information is governed by the Stored Communications Act (SCA).[59] Congress enacted the law in 1986 when it "had little idea of how the Fourth Amendment might apply to the Internet."[60] Although the SCA provided a workable approach to accessing electronic content in 1986, the way email systems operate and how Internet users handle email changed significantly following the SCA's passage.[61] Consequently, the SCA presents a confusing rubric that does not stand the test of time because it is difficult to apply to modern technologies.

The focus of this paper is SCA section 2703, which provides a "code

---

59. 18 U.S.C. §§ 2701–12 (2012). The statute has many nicknames, but is commonly called the SCA. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 n.1 (2004) [hereinafter *User's Guide*]; *see also* NATHAN JUDISH ET AL., OFFICE OF LEGAL EDUC., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 115 n.1 (2009), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

60. *Fourth Amendment*, *supra* note 39, at 1043; *see also* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored Email*, 2008 U. CHI. LEGAL F. 121, 123 ("[D]espite the explosion in use of electronic communications technologies since the SCA's passage, Congress has not updated its terms or significantly changed its structure.").

61. Melissa Medina, Note, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267, 271–73 (2013).

of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications from network service providers."[62] In other words, SCA section 2703 governs situations where investigators desire content and electronic information held by a company such as Facebook or Google. A wide range of information can be obtained by investigators without requesting a warrant; however, obtaining a search warrant is the most efficient way for government investigators to obtain the type and amount of information they desire.[63] Although the government can compel disclosure of some types of information with only a subpoena, the government is able to obtain every type of information sought—including the contents of private emails, messages, and other communications—if the request is accompanied by a search warrant.[64] Professor Orin Kerr explains the value of the "'greater includes the lesser' rule" by explaining that "[SCA] 2703 allows the government to obtain only one court order—whatever process is greatest—and compel all of the information in one order all at once."[65] This approach, where the government requests a warrant for all information maintained by a company on an individual, is utilized in the search warrant applications this Comment examines.[66]

a. Understanding the SCA Decision Making Process

An investigating officer has two important decisions to make when attempting to compel disclosure of a suspect's electronic information from an Internet service. First, the officer must determine the type of service provider in order to determine how to access the communications. Second, the officer must determine the type of information sought in order to determine what tools the officer must use to compel the information. These two decisions are important because the ease with which the government may access electronic information is dependent on the officer's decisions. This section briefly explains these two decisions and how the answer affects the government's ability to access electronic information.

62. JUDISH, *supra* note 59, at 115 (describing "three main substantive components" and noting section 2703's purpose).

63. *See User's Guide*, *supra* note 59, at 1219–20.

64. *Id.* at 1223 (displaying a chart that "summarizes the basic rules of the SCA").

65. *Id.* at 1220.

66. *See infra* Part II.C.2.

i. The Type of Service Provider Determines Access to Contents of Communications

According to the SCA, an agent must first determine what type of service provider holds the information.[67] The statute provides two options.[68] One option is an electronic communication service, defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[69] The second option is a remote computing service, defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[70] The distinction between an electronic communication service (ECS) and a remote computing service (RCS) is of the utmost importance because the ease of access to the contents of emails and other messages hinges on that classification. Investigators can obtain communications stored with an RCS if they obtain a search warrant under Rule 41 or utilize the subpoena procedure set forth in SCA section 2703(b)(1)(B).[71] Communications in electronic storage, held by an ECS provider for *less than 180 days*, may only be accessed with a warrant obtained pursuant to Rule 41.[72] If an email or other communication is held in electronic storage by an ECS provider for *181 days or more*, the communication is treated like content stored with an RCS.[73]

Applied to modern technology and services, it is not readily apparent how a particular service is construed.[74] In fact, many modern services can be construed as both an ECS and an RCS.[75] Facebook is capable of

---

67. JUDISH, *supra* note 59, at 117.

68. *Id.*

69. 18 U.S.C. § 2510(15) (2012); *see also* Medina, *supra* note 61, at 271–74 (explaining that an electronic communications service is analogous to early email systems in which messages were stored by the service until the user retrieved and removed the message from the service via a dial-up connection).

70. 18 U.S.C. § 2711(2). An electronic communications system is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id.* § 2510(14); *see also* Medina, *supra* note 61, at 271–74 (noting modern examples of remote-computing services are Dropbox and any modern web-based email provider).

71. 18 U.S.C. § 2703(b). Section 2703(b)(1)(B) allows the government to obtain information if it utilizes the SCA special-warrant procedure or an administrative subpoena so long as prior notice is given to a subscriber. But, if the government requests it, notice may be delayed in additional ninety-day increments. *Id.* § 2703(b)(1)(B)(ii); *id.* § 2705(a)(1).

72. *Id.* § 2703(a).

73. *Id.*

74. *See* JUDISH, *supra* note 59, at 117–20 (discussing different ways to determine whether a service is ECS or RCS).

75. *Id.* at 120; *see also User's Guide*, *supra* note 59, at 1215 (noting that many network service

being both an ECS and RCS, as is almost every other service commonly used today.[76] Thus, the government has flexibility to define many services in a manner that is favorable to its effort to compel disclosure of emails regardless of the number of days since the original transmission of the communication.

ii. The Type of Information Sought Determines the Tool Needed to Compel Disclosure

Next, after determining what type of service provider possesses the desired information, an agent must determine the proper classification for the information sought.[77] There are three classifications:[78] "basic subscriber and session information,"[79] information that is "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of the communications),"[80] and "any information concerning the substance, purport, or meaning of that communication."[81] Depending on the classification, the SCA provides varying degrees of requirements on government access to the electronic information sought.[82]

One potential classification is "basic subscriber and session information," a statutorily defined set of non-content records such as the name, physical address, IP address, payment method, and other items related to the user's identity.[83] Here, the government cannot obtain a copy of an email or message, but it can compel a provider to disclose a user's location and other identifying information associated with the

providers are "multifunctional").

76. Allen D. Hankins, Note, *Compelling Disclosure of Facebook Content Under the Stored Communications Act*, 17 SUFFOLK J. TRIAL & APP. ADVOC. 295, 310 (2012) (discussing *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010), in which a court found Facebook to be both an ECS and RCS); *see* Eric P. Mandel, *A Hurdle to Obtaining Electronic Evidence*, LAW360 (July 11, 2013, 11:44 AM), http://www.law360.com/articles/455225/a-hurdle-to-obtaining-electronic-evidence ("In the practical sense, email, text messages and instant messages go through ECS providers, while RCS providers offer storage and processing services. While there might have been a greater distinction in 1986, all ECS providers are now essentially RCS providers as well. Yet there are some pure RCS providers, such as Dropbox and Amazon Web Services.").

77. JUDISH, *supra* note 59, at 121.

78. *Id.*

79. *Id.*

80. 18 U.S.C. § 2703(c)(1).

81. *Id.* § 2510(8).

82. JUDISH, *supra* note 59, at 127–34 (discussing the forms of compelled disclosure used with each classification of data).

83. 18 U.S.C. § 2703(c)(2); *see also* JUDISH, *supra* note 59, at 121.

user's activity on the site.[84] A provider of either an ECS or RCS is required to disclose this basic, non-content type of information to a government entity after receiving a properly obtained subpoena.[85]

Information can also be classified as "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of the communications)."[86] As the statute explicitly provides, contents of communications are not accessible here. However, this category serves as a catchall, including a wide variety of non-content information such as transactional records, cell-site data for cellular phone calls, lists of Internet sites accessed, and email addresses the account holder corresponds with.[87] As with basic subscriber and session information, this classification does not include the contents of a communication.[88] Importantly, Congress intended basic subscriber and session information to be distinguishable from the section 2703(c)(1) information that could reveal a "person's entire on-line profile."[89] This classification allows a more comprehensive compilation of a user's activity by including information that more fully details an individual's online activity. The information in this classification is available to an investigator if a warrant is obtained pursuant to Rule 41.[90] Or the government may obtain a special warrant[91] under SCA section 2703(d) to compel disclosure of this information.[92]

The third classification of information is content-based.[93] In relation to "any wire, oral, or electronic communication," contents include "any information concerning the substance, purport, or meaning of that communication."[94] Investigators with a search warrant may obtain "everything that can be obtained using a § 2703(d) court order with

84. *Id.* § 2703(c)(1)–(2).

85. *Id.* § 2703(c)(2). The government can also secure this information by other means. *See id.* § 2703(c)(1).

86. *Id.* § 2703(c)(1).

87. JUDISH, *supra* note 59, at 122.

88. 18 U.S.C. § 2703(c)(1).

89. JUDISH, *supra* note 59, at 122 (quoting H.R. REP. NO. 103-827, at 17, 31–32 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3497, 3511–12).

90. 18 U.S.C. § 2703(c)(1)(A).

91. The SCA provides a special warrant procedure in which the government is not required to establish probable cause but rather may compel disclosure of non-content information by showing "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d).

92. 18 U.S.C. § 2703(c)(1)(B). Section 2703 also provides two other ways to obtain this information, but these procedures are not applicable to the procedures discussed in this paper.

93. JUDISH, *supra* note 59, at 121.

94. 18 U.S.C. § 2510(8).

notice"[95] and "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less."[96] This classification includes the contents of every communication a user has stored on a service.[97]

While the SCA created divisions based on the type of provider and type of information involved in an investigation, a search warrant is the tool that allows the government to compel disclosure of everything associated with a user account. As Professor Orin Kerr suggests, the efficiency of using a single tool—a search warrant application—is evident given the SCA's structure.[98] Though a search warrant requires judicial approval, government investigators can obtain every classification of information with a single search warrant application. [99]

2. *Warshak* Precedent and Online Services Require Search Warrants

Although the SCA does not always require a search warrant before the government may compel disclosure of our most sensitive records, two additional factors may force a government investigator to obtain a search warrant before accessing electronic information. First, concerns about the constitutionality of electronic searches may cause an investigator to request a search warrant.[100] Second, the company providing the Internet service may demand a warrant before it will disclose information on its users.[101] As this section explains, these factors suggest that investigations utilizing search warrants for electronic information will likely increase in frequency. The judiciary is well positioned to determine the sufficiency and boundaries of search warrants for electronic information when faced with this increasingly common issue.

a. *United States v. Warshak* Raises Concerns About the SCA's Constitutionality

An investigator might obtain a warrant if there is concern that a

95. JUDISH, *supra* note 59, at 133.
96. *Id.* (quoting 18 U.S.C. § 2703(a)).
97. *Id.* at 122–23.
98. *User's Guide*, *supra* note 59, at 1220.
99. *Id.*
100. *See infra* Section II.B.2.a.
101. NATE CARDOZO ET AL., ELEC. FRONTIER FOUND., WHO HAS YOUR BACK? PROTECTING YOUR DATA FROM GOVERNMENT REQUESTS 8 (2014), https://www.eff.org/files/2014/05/15/who-has-your-back-2014-govt-data-requests.pdf.

court may later invalidate a search and seizure made via subpoena as unconstitutional. The Supreme Court has not ruled on the reasonableness of privacy expectations in electronic communications.[102] But provisions of the SCA that require disclosure of content-information without a warrant were found unconstitutional in 2010 in a landmark Sixth Circuit decision, *United States v. Warshak*.[103] Embracing petitioner Warshak's argument that "the government's warrantless, *ex parte* seizure of approximately 27,000 of his private emails"[104] was an unreasonable search and seizure in violation of the Fourth Amendment, the Sixth Circuit invalidated SCA section 2703(b)(1)(B).[105] Although no other federal circuit court has adopted *Warshak*'s rule, various courts have extended *Warshak*'s reasoning to other online and electronic content information.[106] If additional jurisdictions adopt the *Warshak* holding, or extend it to online content information held by social media companies, investigators will be required to obtain a warrant before compelling disclosure of content information.

b. Online Services Require Search Warrants Before Disclosing User Information

The second reason an investigator might obtain a warrant is because of company policies that mandate a warrant before disclosing content information. Following the *Warshak* decision, a growing number of service providers are demanding investigators obtain a warrant before disclosing content information.[107] The Electronic Frontier Foundation's

---

102. In fact, the Court has rarely decided issues of constitutionality relating to modern surveillance laws in general. *See* Friess, *supra* note 50, at 984 (citing *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967), as two notable exceptions); *see also* Riley v. California, 134 S. Ct. 2473, 2485 (2014) (holding that police must obtain a warrant to search a cell phone incident to a lawful arrest).

103. 631 F.3d 266, 282–88 (6th Cir. 2010) (finding a reasonable expectation of privacy in emails stored with third-party email provider); *see also The Courts Boldly Go Fourth: Rulings Validate Digital Due Process*, CTR. FOR DEMOCRACY & TECH.: BLOG (Dec. 16, 2010) (discussing *Warshak* and a related case), https://cdt.org/blog/the-courts-boldly-go-fourth-rulings-validate-digital-due-process/.

104. *Warshak*, 631 F.3d at 282.

105. *Id.* at 288 ("[T]o the extent that the SCA purports to permit the government to obtain . . . emails warrantlessly, the SCA is unconstitutional.").

106. *E.g.*, R.S. *ex rel.* S.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F. Supp. 2d 1128, 1142–43 (D. Minn. 2012) (holding user has reasonable expectation of privacy in Facebook private messages and search of account by school official was unreasonable); State v. Clampitt, 364 S.W.3d 605, 611 (Mo. Ct. App. 2012) ("The rationale used by the *Warshak* court in establishing individuals' reasonable expectation of privacy in the contents of their email is equally applicable to cell phone users' expectation of privacy in the contents of their text messages.").

107. CARDOZO, *supra* note 101, at 13–14.

(EFF) annual "*Who has your back?*" report identifies Amazon, Apple, Verizon, and Yahoo as publicly committing, within the last year, to requiring a warrant before content information is disclosed.[108] The civil liberties group noted that its 2014 report is "encouraging" because many companies implemented additional protections for user data when compared to the group's initial report in 2011.[109] According to the EFF report, the list of Internet companies requiring a warrant before disclosing content information includes, but is not limited to: Amazon, Apple, Dropbox, Facebook, Google, Microsoft, Twitter, Verizon, Foursquare, and LinkedIn.[110]

C. Current Procedure

There are four important differences between warrants for online and offline searches and seizures: (1) the two-step process for electronic information; (2) jurisdiction to issue a search warrant; (3) notice requirements; and (4) the requirements relating to the presence of an officer during execution of the search warrant. Following a description of these differences, this section examines three cases that highlight the complexities of a search warrant for electronic information.

1. Federal Rule of Criminal Procedure 41's Two-Step Process

An investigator is required to obtain a warrant for electronic content information under the procedures detailed in Rule 41.[111] Like a warrant for a physical search or seizure, a warrant for electronic content information must meet certain fundamental criteria. A search warrant application must be based on probable cause, particularly describe the persons or items to be searched and seized, and be supported by an affidavit, whether it is for electronic content or offline search or seizure.[112] Though subject to these requirements, a warrant for electronic information has multiple features distinguishing it from a standard warrant executed in the offline world.[113] The 2009 amendments to Rule 41 specifically addressing the two-step process declined to address "the specificity of description that the Fourth Amendment may require in a

108. *Id.* at 21, 23, 59, 67.
109. *Id.* at 12.
110. *Id.* at 18.
111. 18 U.S.C. § 2703(a), (b).
112. *Id.*; FED. R. CRIM. P. 41.
113. JUDISH, *supra* note 59, at 133–34.

warrant for electronically stored information."[114] The Advisory Committee chose to "leav[e] the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development."[115] However, this is problematic because this lack of guidance leads to confusion about whether the government is sufficiently meeting Fourth Amendment standards in recent investigations.

The most important difference between a warrant in the physical world and a warrant for electronic information is Rule 41's two-step process for electronic information. This is important because it allows an officer to "seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant."[116] The process allows the government to first compel disclosure of a large universe of information and then conduct a search for items related to its investigation. In the initial step, the "warrant directs the service provider to produce all email from within the specified account or accounts."[117] In the subsequent step, the warrant allows "law enforcement to review the information produced to identify and copy information that falls within the scope of the particularized 'items to be seized' under the warrant."[118] As a practical matter, Rule 41 limits the timeframe for when the warrant must be executed to fourteen days.[119] However, no presumptive limitations are placed on the amount of time investigators may retain the data for review purposes.[120]

A second distinction involves jurisdiction. Generally, a magistrate judge has authority to issue a warrant only for items and persons within the district.[121] A magistrate judge, however, may issue a warrant "for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed."[122] These

---

114. FED R. CRIM. P. 41 committee's notes to 2009 amendment, http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-app-federalru-dup1-rule41.pdf.

115. *Id.*

116. *Id.*

117. JUDISH, *supra* note 59, at 134.

118. *Id.*

119. FED. R. CRIM. P. 41(e)(2)(A).

120. FED. R. CRIM. P. 41 committee's notes to 2009 amendments.

121. FED. R. CRIM. P. 41(b)(1).

122. FED. R. CRIM. P. 41(b)(2). Additionally, the Rule provides a magistrate judge with authority to issue a warrant for information outside the district if the investigation relates to terrorism, a tracking device, or outside jurisdictions in which the United States has a strong interest. FED. R. CRIM. P. 41(b)(3)–(5).

limitations are not sustainable in an online world where companies store user content and data on servers located throughout the world. Consequently, courts allow magistrate judges to issue a warrant for electronic information held in another jurisdiction.[123]

A third distinguishing feature of search warrants for electronic content involves the requirement of notice. Generally, after executing a warrant for a search or seizure in the physical world, an executing officer must leave a copy of the warrant with the person from whom property was seized or on the premises from which property was removed.[124] The SCA expressly negates this requirement for the online world by providing that a warrant may be served on an RCS "without required notice to the subscriber or customer."[125] Separate provisions pertaining to an administrative subpoena or a section 2703(d) court order do not expressly negate the notice requirement of Rule 41.[126] However, given the notice requirements and ability to subsequently delay notice regardless of the procedure,[127] agents can obtain electronic content information without notice to the subject of the investigation if a warrant is obtained.

A final distinguishing feature concerns the presence of an officer during the execution of the warrant. While an officer or government representative is necessarily required to be present when a search is executed in the physical world, the SCA does not require the presence of an officer for service or execution of the warrant.[128] In executing a warrant for electronic information, the provider is often served in a similar fashion to a subpoena, and the provider produces the requested information.[129]

2. Rule 41's Two-Step Process in Action

Magistrate judges are "revolting" against search warrant applications that grant the government access to the entirety of an

123. *E.g.*, United States v. Berkos, 543 F.3d 392, 396–98 (7th Cir. 2008); *In re* Yahoo, Inc., No. 07-3194-MB, 2007 U.S. Dist. LEXIS 37601, at *22 (D. Ariz. May 21, 2007); *In re* Search Warrant, No. 6:05-MC-168-Orl-31JGG, 2005 WL 3844032, at *5–6 (M.D. Fla. Feb. 13, 2006).

124. FED. R. CRIM. P. 41(f)(1)(C).

125. 18 U.S.C. § 2703(b)(1)(A).

126. *Id.* § 2703(b)(1)(B)(i)–(ii).

127. *Id.* § 2705.

128. *Id.* § 2703(g).

129. JUDISH, *supra* note 59, at 134; *see also* United States v. Bach, 310 F.3d 1063, 1068 (8th Cir. 2002) (finding that the search of email by an ISP without presence of law enforcement did not violate the Fourth Amendment).

account.[130] In the five years following the Advisory Committee's refusal to provide guidance on search warrants of this type, case law developed in a hopelessly confusing manner and no consensus emerged on how the Fourth Amendment should best protect users' online activity and electronic information. Faced with the difficult task of applying the Fourth Amendment to the digital era, magistrate judges are denying search warrant applications that seek access to vast numbers of email and vast amounts of electronic information.[131] While multiple opinions now set forth an individual magistrate judge's reasoning behind the denial or approval of a search warrant application, the legal reasoning varies across the country. Magistrate judges in Kansas and Washington, D.C. denied these overly broad warrant applications, whereas a magistrate judge for the Southern District of New York approved a similar warrant application.[132] These cases demonstrate the lack of settled standards for a search and seizure of electronic information in an online service provider's possession.

a. Examining *In re Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*

Magistrate Judge David Waxse of the United States District Court for the District of Kansas has denied multiple search warrant applications for electronic content and data. When initially approaching the issue in 2012, Judge Waxse denied a search warrant application for electronic content that sought the entirety of a Yahoo account.[133] Judge Waxse also

130. *E.g.*, Ann E. Marimow & Craig Timberg, *Low-Level Federal Judges Balking at Law Enforcement Requests for Electronic Evidence*, WASH. POST (Apr. 24, 2014), http://www.washingtonpost.com/local/crime/low-level-federal-judges-balking-at-law-enforcement-requests-for-electronic-evidence/2014/04/24/eec81748-c01b-11e3-b195-dd0c1174052c_story.html; Patrick J. Cotter, *Magistrates' Revolt: Unexpected Resistance to Federal Government Efforts to Get "General Warrants" for Electronic Information*, NAT'L L. REV. (May 15, 2014), http://www.natlawreview.com/article/magistrates-revolt-unexpected-resistance-to-federal-government-efforts-to-get-genera.

131. *E.g.*, *In re* Search of Info. Associated with @mac.com, 25 F. Supp. 3d 1, 6–7 (D.D.C. 2014), *renewed application denied*, 13 F. Supp. 3d 145 (D.D.C. 2014), *vacated*, 13 F. Supp. 3d 157 (D.D.C. 2014); *In re* Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 U.S. Dist. LEXIS 123129, *24–28 (D. Kan. Aug. 27, 2013); *In re* Cunnius, 770 F. Supp. 2d 1138, 1139 (W.D. Wash. 2011).

132. *In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com, 33 F. Supp. 3d 386, 394–96 (S.D.N.Y. 2014).

133. *In re* Search Warrants for Info. Associated with Target Email Address, Nos. 12-MJ-8119-DJW, 12-MJ-8191-DJW, 2012 U.S. Dist. LEXIS 138465, at *2–4, *27–30 (D. Kan. Sept. 21, 2012) (finding that the government lacked probable cause to seize and search such a large amount of data and finding the lack of limitations on the investigative process troubling).

denied searches for electronic content in the context of a cellular phone search.[134]

In *In re Search Warrants for Information Associated with Target Email Accounts/Skype Accounts*, Judge Waxse once again denied a search warrant application for the entirety of accounts held by several Internet companies.[135] The government alleged that the suspect utilized several online services to "facilitate the purchase, receipt, and transportation" of stolen property.[136] As part of its investigation, the government sought to compel five providers—Google, GoDaddy, Verizon, Yahoo, and Skype—to disclose the contents of communications related to its investigation.[137]

The government utilized Rule 41's two-step process to compel disclosure of the electronic content.[138] In the first step, the government identified the information to be disclosed by the five providers under the SCA compelled-disclosure provisions.[139] The government's request in this first step included an astonishingly large amount of information because the government sought a comprehensive disclosure of every piece of information associated with the five separate accounts.[140] It is

---

134. *In re* Search of Three Cellphones, No. 14-MJ-8013-DJW, 2014 U.S. Dist. LEXIS 108470, at *1 (D. Kan. Aug. 4, 2014); *In re* Search of a Nextel Cellular Tel., 14-MJ-8005-DJW, 2014 U.S. Dist. LEXIS 88215, at *1 (D. Kan. June 26, 2014).

135. 2013 U.S. Dist. LEXIS 123129, at *1–2.

136. *Id.* at *2.

137. *Id.* at *1.

138. *Id.* at *2–4.

139. *Id.*

140. The government sought:

> The contents of all emails, instant messages, and chat logs/sessions associated with the account, including stored or preserved copies of emails, instant messages, and chat logs/sessions sent to and from the account; draft emails; deleted emails, instant messages, and chat logs/sessions preserved pursuant to a request made under 18 U.S.C. § 2703(f); the source and destination addresses associated with each email, instant message, and chat logs/session, as well as the date and time at which each email, instant message, and chat logs/session was sent, and the size and length of each email;
>
> All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
>
> All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
>
> All records pertaining to communications between (Provider) and any person regarding the account, including contacts with support services and records of actions taken.

Id. at *3–4.

difficult, if not impossible, to find information potentially held by one of the five providers that is outside the scope of the government's request. In this initial step, the government did not list a date range or other basic limitations on the disclosure.[141]

The second step of the government's request stated that the government would "maintain all information that constitutes fruits, evidence, and instrumentalities" of the alleged violations.[142] The government identified the types of information in a broad and imprecise manner, but the information was limited to the alleged crimes.[143] In contrast to the first step of the warrant application, the government limited the information it would maintain to only that occurring "from June 2006, when the conspiracy commenced until the date of the search warrant."[144]

After scrutinizing the SCA in relation to the Fourth Amendment, Judge Waxse denied the government's search warrant application for two reasons.[145] First, Judge Waxse found that the compelled disclosure was "too broad and too general."[146] Although not explicitly stated as such, Judge Waxse's objection was that the government did not establish probable cause for the breadth of emails and account information sought as part of its investigation. The warrants would have authorized disclosure of "all email communications in their entirety and all information about the account without restriction."[147] The sections of the warrant describing content to be disclosed by the providers was deemed the "most troubling" part because the "warrants fail to limit the universe

---

141. *Id.* The government's request also indicates it had previously requested content preservation as provided for by section 2703(f) of the SCA. *Id.* at *3. Given this aspect of the request, and lack of any date range to guide companies, there is no reason to believe that the government cannot obtain the entirety of the providers' records on an individual suspect.

142. *Id.* at *4.

143. The government sought to maintain:

> All stored electronic mail, instant message, and chat logs/session[s] sent to, from, and through (target account) and all related subscriber accounts from June 2006, when the conspiracy commenced until the date of the search warrant to include communications involving the transportation or receipt of stolen property;
>
> Records relating to who created, used, or communicated with the (target account) or identifiers, including records about their identities and whereabouts; and
>
> All records related to the subscriber account of (all target accounts), including account information, computer host names, Internet addresses, passwords, access telephone numbers, password files, and other identifying information.

Id. at *4–5.

144. *Id.* at *4.

145. *Id.* at *24–25.

146. *Id.* at *25.

147. *Id.*

of electronic communications and information to be turned over to the government to the specific crimes being investigated."[148] Judge Waxse identified the critical problem concerning probable cause, noting that "[t]he target accounts may contain large numbers of emails and files unrelated to the alleged crimes being investigated or for which the government has no probable cause to search and seize."[149] Judge Waxse noted that probable cause was not established to search and seize "all emails ever sent to or from the accounts or for all the information requested from the Providers."[150]

Judge Waxse's second objection focused on the absence of limitations set forth by the government regarding the review of the "potentially large" amount of electronic information to be disclosed.[151] The warrant applications did not include a procedure for sorting or filtering relevant information from information outside the scope of the government's investigation of the alleged conspiracy.[152] Judge Waxse analogized such an electronic request without limitations to a warrant seeking to search copies of all physical mail ever sent through a post office to or from a specific address, a request that violates the Fourth Amendment because such procedures are unreasonable.[153] Judge Waxse recognized that the Fourth Amendment does not require a particular search strategy or methodology, but he did find that "the warrants must contain some limits" to comply with the Fourth Amendment.[154]

b. Examining *In re Search of Information Associated with @mac.com*

Magistrate Judge John Facciola is a prominent member of the Magistrates' Revolt.[155] Similar to Judge Waxse, Judge Facciola denied search warrant applications for electronic information on the basis that the applications were too broad and general to meet Fourth Amendment standards.[156] Judge Facciola also denied overbroad search warrant

148. *Id.*
149. *Id.* at *27.
150. *Id.*
151. *Id.* at *25.
152. *Id.* at *25–26.
153. *Id.* at *28.
154. *Id.* at *30.
155. *See* sources cited *supra* note 130.
156. *In re* Search of Info. Associated with @mac.com, 25 F. Supp. 3d 1, 6–7 (D.D.C. 2014), *renewed application denied*, 13 F. Supp. 3d 145 (D.D.C. 2014), *vacated*, 13 F. Supp. 3d 157 (D.D.C. 2014); *see also In re* Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis, 21 F. Supp. 3d 1, 9–11 (D.D.C. 2013) (modifying warrant application to prevent wholesale disclosure of electronic content outside the scope of probable cause).

applications for cellular phone and handheld tablet investigations.[157]

One recent denial of a search warrant application by Judge Facciola is *In re Search of Information Associated with @mac.com*.[158] There, following the denial of its first application, the government renewed its motion for a search warrant application.[159] The government's renewed search warrant application contained three attachments.[160] The first attachment specified the @mac.com account at issue in the investigation.[161] This attachment also specified that the government sought information from January 2014 forward.[162] The next attachment detailed the "[p]articular things to be seized by the government."[163] Here, the government limited its seizure to information "referring or relating" to a government investigation involving a myriad list of companies the government suspected may have been involved in the crime.[164] The third attachment detailed "[p]rocedures to facilitate execution of the warrant."[165] This section was similar to Rule 41's first step where the government identifies information to be disclosed by a provider. As with search warrant applications before Judge Waxse, the government's requested disclosure was massive in scope, and it is difficult to think of information that was outside the scope of the government's request.[166] Although the universe of information disclosed

157. *In re* Search of Apple iPhone, 31 F. Supp. 3d 159, 161 (D.D.C. 2014); *In re* Search of Odys Loox Plus Tablet, 28 F. Supp. 3d 40, 41–42 (D.D.C. 2014).

158. 13 F. Supp. 3d 145, 157 (D.D.C.), *vacated*, 13 F. Supp. 3d 157 (D.D.C. 2014).

159. *Id.* at 147.

160. *Id.* at 148.

161. *Id.*

162. *Id.*

163. The government sought:

> All emails, including email content, attachments, source and destination addresses, and time and date information, that constitute evidence and instrumentalities of violations of 41 U.S.C. § 8702 (Solicitation and Receipt of Kickbacks) and 18 U.S.C. § 371 (Conspiracy), dated between [January], 2014, to the present, including emails referring or relating to a government investigation involving any or all of the following: [Redacted list of names of companies and individuals in the form of "John Smith, John Smith, Inc., any current or former John Smith employees, etc."].

Id. (alterations in original).

164. *Id.*

165. *Id.*

166. The government's broad request was phrased as follows:

> To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) [in January], 2014, the Provider is required to disclose the following information to the government for the account listed in Attachment A: all emails, including attachments, associated with the account, dating from [January], 2014, to the present, and including stored or preserved copies of emails sent to and from the account,

by a provider is similar to requests in previously described rulings, the government recommended procedures for the search and seizure after receiving the information from Apple that were not recommended in the warrants examined by Judge Waxse.[167] These procedures allowed the government to search the large universe of information disclosed by Apple and stated that the government will seal, but not return or delete, any information it found that was not within the scope of the warrant.[168]

Although this search warrant application varied in important ways from the search warrant application denied by Judge Waxse, Judge Facciola reached the same decision as Judge Waxse and found the application was too broad and too general.[169] Judge Facciola explained that he denied the previous application because the government sought to seize an entire email account without establishing probable cause for all of the emails, and the government failed to explain what would happen to data beyond the scope of the warrant following the initial seizure.[170] Once again, Judge Facciola denied the government's search warrant application.[171]

Judge Facciola disapproved of the government's use of Rule 41's two-step procedure.[172] He reasoned that the two-step procedure was only proper after a showing of practical need by the government.[173] After distinguishing a hard drive or cell phone from an email or other

---

> draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email.
>
> Apple shall deliver the information set forth above via United States mail, courier, or email to: [The Department of Justice].

Id. (alterations in original).

167. The government's suggested procedure was:

> The United States government will conduct a search of the emails produced by the Provider and determine which are within the scope of the information to be seized specified in Attachment B. Those that are within the scope of Attachment B may be copied and retained by the United States.
>
> Law enforcement personnel will then seal any information from Apple that does not fall within the scope of Attachment B and will not further review the information absent an order of the Court.

Id. at 148–49.

168. *Id.*

169. *See id.* at 149 ("[T]he government requests that Apple provide all e-mails from a certain date in January, 2014, so that the government may search them for evidence of specific crimes and keep any non-relevant e-mails under seal until further order of a court.").

170. *Id.*

171. *Id.* at 150 ("Although there are some cosmetic differences between the original application and the Renewed Application, the bottom line is that the government still gets *all* e-mails—regardless of their relevance to its investigation—and keeps them indefinitely.").

172. *Id.* at 152–53.

173. *Id.* at 153.

electronic content held by a provider, Judge Facciola suggested the extraordinary step of having Apple perform an initial search, pursuant to the warrant, then disclose only the emails that the government can establish probable cause for.[174] Judge Facciola noted that his suggestion was going into unexplored territory because it was a step beyond what other courts had done.[175] In response to his own question of whether his court could order Apple to disclose emails *outside* the warrant's scope, Judge Facciola emphatically declared, "[t]he answer is no."[176]

Like Judge Waxse's ruling, Judge Facciola rejected the search warrant application because its lack of limitations made it overbroad.[177] The government did not suggest an alternative approach in response to Judge Facciola's recommendation to utilize Apple's expertise in performing an initial disclosure narrowly tailored to the application's probable-cause showing.[178] Additionally, the government ignored previous warnings against retaining information outside the search warrant's scope and attempted to do so once again.[179] According to Judge Facciola, the government's request to indefinitely retain the entirety of a user's email account, even under seal, was "inconceivable . . . and unacceptable."[180] Although Judge Facciola did not specify a certain limitation procedure, it is clear that he believes that some limitations are needed when the government seeks, or receives, the entirety of a user's email account or other electronic content.[181]

The government responded to Judge Facciola's second denial of its search warrant application by challenging the denial order in the United States District Court for the District of Columbia.[182] The District Court ultimately vacated Judge Facciola's order and granted the search warrant.[183] The District Court cited several key reasons for doing so. First, the government's search was "constrained and limited" to the specific items listed as "to be seized" in the application's second

174. *Id*. at 153–54.

175. *Id*. at 154.

176. *Id*.

177. *See id*. at 155–56 (discussing government's failure to establish probable cause and breadth of the request).

178. *See id*. at 155 ("[T]he government is unwilling–for whatever reason–to give up its policy of seizing large quantities of emails and other Fourth Amendment protected data . . . .").

179. *Id.* at 155–56.

180. *Id.* at 155.

181. *Id.* at 155–56.

182. *In re* Search of Info Associated with @mac.com, 13 F. Supp. 3d 157 (D.D.C. 2014).

183. *Id.* at 159–60.

attachment.[184] Second, the court found the search warrant sufficiently particular, despite its breadth, because "there is a fair probability that the electronic communications and records that the government seeks . . . will be found in the particular place to be searched."[185] Finally, after examining the two-step procedure relied on by the government, the court determined that the government's application complied with Rule 41.[186]

Finally, the District Court found Judge Facciola's suggestion—use Apple to conduct an initial search to limit the scope of the disclosure—to be inadequate.[187] The District Court noted that having Apple perform an initial search was problematic for several reasons. Apple employees are not trained to determine whether particular content is relevant to an investigation, the suggested procedure is costly, time-consuming, and could "expose the government to potential security breaches."[188]

c. Examining *In re Warrant for All Content & Other Information Associated with the Email Account xxxxxxx@Gmail.com*

Judge Gorenstein, of the United States District Court for the Southern District of New York, reached a contrary decision on a similar request to those before Judges Waxse and Facciola.[189] The search warrant application utilized Rule 41's two-step process to seek the entirety of a Google account and did not limit the information to be disclosed to a specific date range.[190] Judge Gorenstein did not interpret the Fourth Amendment's probable-cause requirement narrowly and allowed the government to obtain electronic information falling outside the scope of the warrant.[191] After comparing a search of a computer hard drive with that of an email inbox, Judge Gorenstein tackled the complexity of electronic searches.[192] Ultimately, Gorenstein held that Rule 41(e)(2)(B) supported the Government's argument that the two-step procedure was proper and approved the request.[193] However, Judge Gorenstein did find Judge Facciola's suggestion to have a third-party

184. *Id.* at 164.
185. *Id.*
186. *Id.* at 165.
187. *Id.* at 165–66.
188. *Id.*
189. *In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@Gmail.com, 33 F. Supp. 3d 386, 388 (S.D.N.Y. 2014).
190. *Id.* at 388–89.
191. *Id.* at 391–92.
192. *Id.* at 392–94.
193. *Id.* at 393–94.

service provider conduct an initial review of a user's content persuasive in cases where the service provider could "produce responsive material in a manner devoid of the exercise of skill or discretion."[194]

Judge Gorenstein did not require the government to affirmatively limit its ability to retain the information obtained or to include a search protocol in the warrant application.[195] Although he noted several decisions where the government had proposed limitations in "secondary orders" that provided for the return or destruction of records not within the scope of the warrant, Judge Gorenstein did not hold the application before him to such standards.[196] Judge Gorenstein noted the potential recourse a user may take if the government acts improperly in the execution of the search warrant.[197] Finally, Judge Gorenstein noted that while it is permissible to mandate search protocols in the application, he did not find protocols "necessary to ensure particularity here."[198]

III. ANALYSIS

After examining current law and reviewing the overbroad search warrant applications described in Part II, Part III offers two suggestions for magistrate judges to consider when deciding whether a search warrant application meets Fourth Amendment standards. First, transparency is crucial to the development of Fourth Amendment law. Magistrate judges should contribute to ongoing case law by publishing opinions that explain the reasoning underlying a decision to approve or deny a search warrant application. Second, Rule 41 must be updated to require affirmative limitations on a search warrant sought using Rule 41's two-step process for electronic information. Part III suggests a number of modest limitations that a magistrate judge may impose when presented with an overbroad search warrant application. Given the varying nature of criminal investigations, no one-size-fits-all limitation should be implemented. However, modest limitations can be imposed in combination with other limitations, or as a stand-alone measure, to ensure a search warrant for electronic information does not violate a citizen's Fourth Amendment rights.

194. *Id.* at 394.

195. *See id.* at 396–401 (explaining that courts need not define the proper procedure to execute a warrant, instead analysis focuses on the reasonableness of the search).

196. *Id.* at 396, 400–01.

197. *Id.* at 398.

198. *Id.* at 400.

A. Transparency in Search Warrant Applications is Necessary

Criminal investigations are necessarily secretive. It is obvious why, when submitting a search warrant application, the government does not want its target to receive notice of the warrant or investigation. However, the sealed nature of search warrants hinders a judge's ability to tackle the issue of specificity when presented with an application for electronic information. The 2009 Advisory Committee Notes to Rule 41 explicitly declined to address the specificity of description for electronic information in a search warrant, "leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development."[199] However, case law is not readily found in many jurisdictions and there are even fewer district or circuit court decisions addressing the sufficiency of a warrant for electronic information. Magistrate judges should contribute to ongoing case law in the area of search warrants for electronic information by publishing and explaining their decisions—but only after publication would no longer threaten the government's investigation.

Faced with a search warrant application for electronic information, Judge Gorenstein approved the government's request immediately after reviewing the application.[200] However, Judge Gorenstein recognized opinions to the contrary in other jurisdictions and published a written opinion five weeks later that explained the approval of the government's request.[201] This is a positive step that helps all parties understand the nature of the government's request and the judiciary's legal reasoning. This practice is valuable to other law enforcement officials, members of the judiciary at all levels, and to attorneys representing those charged with crimes where a search warrant for electronic information was used in the government's investigation.

B. Affirmative Limitations Are Necessary to Curb Overbroad Search Warrant Applications

In denying the warrant applications before him, Judge Waxse's chief concern was the absence of limitations on the government's review of

199. FED. R. CRIM. P. 41 committee's note to 2009 amendments.

200. *See In re xxxxxxx@Gmail.com*, 33 F. Supp. 3d at 388 ("On June 11, 2014, this Court was presented with an application for a search warrant . . . . The Court granted the application on the day it was presented.").

201. *Id.* at 388.

information obtained pursuant to the search warrant.[202] Judge Facciola expressed similar concerns in denying the warrant applications before him.[203] Given the importance of ensuring Fourth Amendment protections, Judge Waxse and Judge Facciola present persuasive reasoning. Guidance provided by Rule 41 and its accompanying comments on electronic search and seizures must require search warrant applications for electronic information to affirmatively limit the Government's use and retention of information disclosed pursuant to the Rule's two-step process. Magistrate judges should mandate a minimum level of affirmative limitations when approving a warrant for disclosures pursuant to Rule 41. As the complexities of technology are numerous, setting such a limitation on the government's conduct is inherently difficult and will be dependent on the specifics of each investigation.

This section provides four affirmative limitations that may be imposed by magistrate judges to ensure the Fourth Amendment protects electronic information held by an online service provider. Magistrate judges could require investigators to narrow the scope of the disclosure if there is evidence that the criminal activity only occurred during a certain time period. Alternatively, magistrate judges could impose a limitation on the type of information the government obtains if there is no showing of need for that particular type of information. A filtering agent or Special Master conducting the search of an account may be a sufficient limitation on investigators' ability to search the entirety of an account. Finally, magistrate judges should not hesitate to impose limitations on the government's retention of the information received after a search warrant is executed. Although magistrate judges must balance an individual's Fourth Amendment right with the government's need to fight crime, these affirmative limitations are reasonable steps that could provide a proper level of protection for electronic information.

---

202. *See In re* Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 U.S. Dist. LEXIS 123129, at *25 (D. Kan. Aug. 27, 2013) ("[The warrants] fail to set out any limits on the government's review of the potentially large amount of electronic communications and information obtained from the electronic communications service providers."); *In re* Search Warrants for Info. Associated with Target Email Address, Nos. 12-MJ-8119-DJW, 12-MJ-8191-DJW, 2012 U.S. Dist. LEXIS 138465, at *29 (D. Kan. Sept. 21, 2012) ("[T]he Court is concerned by the lack of any limits on the government's review of the information, such as filtering procedures for emails, faxes, and information that do not fall within the scope of probable cause or contain attorney-client privileged communications.").

203. *In re* Search of Info. Associated with @mac.com, 13 F. Supp. 3d 145, 149 (D.D.C. 2014), *vacated*, 13 F. Supp. 3d 157 (D.D.C. 2014) ("[T]he government failed to explain what would occur with data that were seized but were outside the scope of the warrant application . . . ." (citing *In re* Search of Info. Associated with @mac.com, 25 F. Supp. 3d 1, 4 (D.D.C. 2014), *renewed application denied*, 13 F. Supp. 3d 157 (D.D.C. 2014))).

1. Affirmative Limitations Narrowing the Scope of the Search

Where possible and reasonable, the government should take steps to limit the initial disclosures made by an entity holding a user's electronic information. The difficulty of establishing probable cause for the entirety of electronic information in an account should not preclude agents from executing a warrant. However, the government and the reviewing magistrate judge must be cognizant of the potential for information outside that for which probable cause is established to be disclosed in a search warrant utilizing Rule 41's two-step process.

In *In re Search Warrants for Information Associated with Target Email Accounts/Skype Accounts*, the government requested an unlimited amount of information, but declared only information from June 2006 onward would be retained.[204] Although it is unclear due to the brief nature of the opinion, the government presumably had reason to believe that the alleged conspiracy, or use of electronic services to carry out the conspiracy, started in June 2006.[205] Therefore, any information prior to June 2006 is seemingly not relevant to the government's investigation. Despite this, the government's request did not limit their request to a certain time period, instead they requested *everything* ever associated with the user's account.[206] Investigators may immediately disregard any information disclosed that is prior to June 2006, and service providers can easily limit the information it delivers to investigators. Such a process ensures the government obtains information relevant to its investigation but also ensures that a potentially large amount of information from the user's account for which the government has no probable cause is not disclosed. A magistrate judge is well positioned to add this simple limitation. Though limiting the request in this manner may also exclude information the user entered when registering for the service, there is nothing to preclude investigators from seeking that information by sufficiently identifying a need in its efforts to obtain further information on the suspect. However, the government should not acquire information on a suspect when it fails to establish a fair probability that the criminal activity was occurring within the time period of requested disclosure.

204. *In re Target Email Accounts/Skype Accounts*, 2013 U.S. Dist. LEXIS 123129, at *2–5.

205. *Id.* at *4 (noting that the government warrant request included information "from June 2006, when the conspiracy commenced").

206. *Id.* at *2–5.

2. Affirmative Limitations Narrowing the Type of Information

Additionally, magistrate judges should not hesitate to modify the type of information disclosed if doing so ensures the government does not receive disclosures without fairly establishing probable cause. Following a deadly shooting at the Federal Navy Yard in Washington, D.C., government investigators requested a search warrant for the alleged shooter's Facebook account.[207] The government's initial disclosure request was expansive in scope, involving every conceivable aspect of the suspect's use of the social media site.[208] In response to concerns about the scope of the warrant application, Judge Facciola limited the information Facebook must disclose.[209] Importantly, the revised order limited the information to be disclosed to content the alleged shooter sent, excluding content of messages sent to the shooter from third parties and other third-party content and activities, such as photo "tags," that the alleged shooter had no ability to control.[210] As with a limitation on the time period, limiting the type of information disclosed is within a service provider's technical abilities. An affirmative limitation on the type of information disclosed is a great way to ensure that the government does not receive the entirety of an account, including information that is surely outside the warrant's scope. This limitation ensures that the government is more likely to receive information directly relevant to its investigation. Judicially imposed modifications and constraints on a search warrant application ensures that investigators search a set of information more closely tailored to that which it properly established probable cause.

3. Filtering Agent or Special Master Limiting Disclosures to Investigators

The use of a filtering agent or special master may be an acceptable limit on the government's search of electronic information disclosed by providers. In this procedure, the agent serves as a barrier to access for investigators that are involved in a particular case. Rather than have an investigator search the information himself, the investigator works with an agent that is not directly involved in the investigation.[211] This

207. *In re* Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis, 21 F. Supp. 3d 1, 3 (D.D.C. 2013).

208. *See id.* at 3–4 (recreating warrant request and expressing concern over its breadth).

209. *Id.* at 5.

210. *Id.* at 5–7.

211. *See* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV.

technique can be helpful because investigators can repeatedly query the electronic information for clues, but the barrier to access limits the opportunity for an investigator involved in the case to view information that is not relevant to the investigation.

In *United States v. Bickle*, the government used a filtering agent to conduct a search of the information disclosed by Microsoft.[212] This practice served the additional purpose of ensuring the government did not view or search attorney-client privileged communications.[213] Additionally, the use of a government filtering agent or special master addresses concerns that an online-content provider may not be best suited to conduct an initial search if the court were to require a third-party provider to conduct an initial search of the suspect's account before disclosing information to government investigators.[214] Such a procedure implements an additional step in the investigative process, but the additional protections ensure that the government is able to obtain the information it needs while still protecting users' Fourth Amendment rights.

4. Affirmative Limitation on Retention of Disclosed Information

Another troubling aspect to government investigations using Rule 41's two-step process is the lack of limitations on how long the government may retain information that is disclosed pursuant to a search warrant. The indefinite retention of information in this manner is unreasonable because the government may repeatedly search the information without court oversight. Currently, Rule 41 does not require limitations on the government's retention and use of electronic information following an initial disclosure by a provider.[215] The 2009 Advisory Committee Notes simply declined "to arbitrarily set a presumptive time period" for return of materials.[216] Additionally, several courts hold it unnecessary that the court impose or require a search

1241 (2010) (discussing a search protocol involving case agents that are unaffiliated with the government's investigation in the context of the decision in *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009)).

212. No. 2:10-cr-00565-RLH-PAL, 2011 U.S. Dist. LEXIS 94921, at *59 (D. Nev. July 21, 2011).

213. *Id.*

214. *See In re* Search of Info. Associated with @mac.com, 13 F. Supp. 3d 157, 165–66 (D.D.C. 2014) (arguing that training and directing third-party providers in law enforcement techniques is unsatisfactory).

215. FED. R. CRIM. P. 41 committee's note to 2009 amendment.

216. *Id.*; *see also In re* Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@Gmail.com, 33 F. Supp. 3d 386, 399 (S.D.N.Y. 2014).

protocol or retention timeframe for information seized pursuant to a search warrant.[217] However, magistrate judges should set a timeframe in which the government must destroy or return information outside the scope of the warrant. A limit on the length of time the government retains any information it receives ensures that the government cannot access the information again.

Judge Gorenstein argued that such a deadline could impede government investigations when the government must conduct additional searches after discovering new information in its investigation or must preserve information for trial purposes.[218] Although the suggestion to seal information outside the scope of the warrant was suggested in *In re Search of Information Associated with @mac.com*, the suggestion mistakenly relied on precedent relating to on-site searches.[219] Instead, Judge Facciola held the suggestion unacceptable.[220] Rather than retain the information, it is reasonable to require the government to return the seized information, or destroy it.

IV. CONCLUSION

Rule 41 must be updated in light of the government's search and seizure process for electronic information in the possession of an online service provider. The Fourth Amendment must be applied with strength to protect Americans' electronic information to ensure protections from unreasonable searches and seizures. As more investigations request electronic information from service providers, magistrate judges should impose affirmative limitations on the government's conduct. While Rule 41's two-step process is likely to continue to allow disclosure of a large universe of information in any given investigation, affirmative limitations can ensure the Fourth Amendment remains a strong protection in the digital era. The affirmative limitations in this Comment provide concrete actions magistrate judges can take to ensure search warrants for electronic information comply with Fourth Amendment protections.

---

217. *See In re Email Account xxxxxxx@Gmail.com*, 33 F. Supp. 3d at 396–97 (discussing cases).

218. *Id.* at 398–99.

219. *In re Info. Associated with @mac.com*, 13 F. Supp. 3d at 156 (discussing *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982)).

220. *Id.*