St. John's Law Review

Volume 90
Number 2 *Volume 90, Summer 2016, Number 2*

Article 8

A Balancing Act: Fourth Amendment Protections and the Reasonable Scope of Government Investigatory Access to E-Mail Accounts

Joseph P. Gryzlo

A BALANCING ACT: FOURTH AMENDMENT PROTECTIONS AND THE REASONABLE SCOPE OF GOVERNMENT INVESTIGATORY ACCESS TO E-MAIL ACCOUNTS

JOSEPH P. GRYZLO[†]

> Applying 18th Century notions about searches and seizures to modern technology, however, is easier said than done, as we are asked to measure Government actions taken in the "computer age" against Fourth Amendment frameworks crafted long before this technology existed. As we do so, we must keep in mind that "the ultimate touchstone of the Fourth Amendment is reasonableness."[1]

INTRODUCTION

Imagine an individual—let's call him Steven—owned and operated a business.[2] Steven was convicted on counts stemming from the business conducting a scheme to defraud its customers through false advertising, as well as fabricated customer satisfaction and product effectiveness statistics.[3] He received a twenty-five-year sentence for his conduct, had to pay a fine of about $100,000, and was forced to surrender hundreds of millions of dollars.[4]

Part of the government's evidence against Steven came from information derived from thousands of e-mails he had sent and received involving one particular e-mail account he had with an Internet Service Provider ("ISP").[5] Early on in the investigation,

---

[†] Senior Staff, *St. John's Law Review*; J.D., 2016, St. John's University School of Law.

[1] United States v. Ganias, 755 F.3d 125, 133–34 (2d Cir. 2014) (footnote omitted) (quoting Missouri v. McNeely, 133 S. Ct. 1552, 1569 (2013) (Roberts, C.J., concurring in part and dissenting in part)).

[2] The following facts come from *United States. v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

[3] *Id.* at 277, 281.

[4] *Id.* at 281–82.

[5] *Id.* at 282–83. The ISP provided and hosted the e-mail account involved in this case. *Id.*

the government had requested the ISP save copies of all future e-mails involving Steven's account, which the ISP did.[6] Later in the investigation, the government required the ISP to provide the preserved e-mails, once by subpoena and once by an ex parte court order.[7] At no time did the government obtain, nor even apply for, a warrant to search Steven's e-mails.[8] Before trial, Steven moved to exclude the e-mails, alleging a Fourth Amendment violation; however, this motion was denied.[9] The foregoing facts come from an actual case, *United States v. Warshak*, which was ultimately appealed to the United States Court of Appeals for the Sixth Circuit.[10]

On appeal, the Sixth Circuit held that the government had violated Steven's Fourth Amendment rights by obtaining access to his e-mails through the ISP without a warrant.[11] In its analysis, the court concluded that Steven's subjective expectation of privacy in the content of his e-mails stored, sent, and received through the ISP was objectively reasonable.[12] This is important because if an individual's subjective expectation of privacy is unreasonable, Fourth Amendment protections do not apply.[13] As

---

[6] *Id.* at 283.

[7] *Id.*

[8] *Id.* at 274.

[9] *Id.* at 281.

[10] *Id.* at 266.

[11] *Id.* at 288. However, the court ultimately upheld the government's use of information stemming from this e-mail account because the government had relied in good faith on provisions of the Stored Communications Act ("SCA"). *Id.* at 292. The SCA authorized the steps the government took in preserving and directing disclosure of the copies of Steven's e-mail account, and the government had used the SCA in good faith as a guide, as the SCA had yet to be declared unconstitutional to the extent it permitted warrantless seizure of e-mails. *Id.* at 289. As a result, the information the government obtained from the account could be used as evidence, and Steven did not get the benefit of the holding. *Id.* at 289–90. But, because the court found that the government's conduct was a violation of Fourth Amendment protections, the court further held the SCA unconstitutional in this context. *Id.* at 288. Therefore, good faith reliance on the SCA going forward will not exist, and such conduct in the future will result in the exclusion of such evidence. *Id.*

[12] *Id.* at 286. The *Warshak* court pointed out that neither the ability of a third party to access the contents of communication, nor the right of access to the communication of the company providing the service necessarily defeats the reasonable expectation of privacy. *Id.* at 286–87.

[13] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The Fourth Amendment protects individuals from "unreasonable searches and seizures." U.S. CONST. amend. IV. Whether a person has a reasonable expectation of privacy is determined by a two-part test: (1) the individual must exhibit an actual expectation

a result, the court concluded that Fourth Amendment protections apply to the contents of e-mail accounts stored with third parties, such as ISPs.[14] Thus, a warrant based on probable cause is needed for the government to constitutionally compel an ISP or other e-mail service provider to provide the contents of an e-mail account.[15]

However, the determination in *Warshak* that a warrant based on probable cause is needed for the government to obtain access to an e-mail account from an e-mail service provider raises another question. If the government does have probable cause, it will most likely have probable cause to justify a warrant for some portion of an e-mail account, but will not have reason to believe that the entire account consists solely of e-mails relating to the investigation.[16] If the government applies for a warrant requesting access to an entire e-mail account from an e-mail service provider, will a showing of probable cause for some of the account enable the government to have a warrant application granted for the entire account? In such cases, there are potential complications regarding the particularity of such warrants and the reasonableness of the breadth of the warrants.[17]

On one side, since there is probable cause for a portion of the account, the warrant request should be granted so that the government can have access to the information for which it does have probable cause.[18] On the other side, since the government does not have probable cause to believe the entire account

---

of privacy, and (2) the expectation must be objectively reasonable. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[14] *Warshak*, 631 F.3d at 288.

[15] *Id.* Courts in other circuits have cited *Warshak* with approval. *E.g.*, *In re* Applications for 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 WL 4647554, at *4 (D. Kan. Aug. 27, 2013) [hereinafter *In re Target Email/Skype Accounts*]; United States v. Bode, No. ELH-12-158, 2013 WL 4501303, at *15 (D. Md. Aug. 21, 2013); United States v. Ali, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012). The United States Supreme Court has yet to address the issue.

[16] *See* United States v. Riley, 906 F.2d 841, 845 (2d. Cir. 1990) (recognizing that "few people keep documents of their criminal transactions in a folder marked 'drug records' ").

[17] U.S. CONST. amend. IV.

[18] *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 354 (1974) (noting that "restrictions upon means of law enforcement handicap society's capacity to deal with two of its most deeply disturbing problems: the fact and the fear of crime").

consists solely of evidence of criminal activity germane to the investigation, there are Fourth Amendment privacy complications regarding any e-mails not satisfying the probable cause showing.[19]

The problem lies in the unknown location of the relevant information; the location of e-mails that are relevant to an investigation is not known prior to someone examining the account and parsing responsive from unresponsive material.[20] As a result, the government will make a warrant application for the entire account. A court faced with such an application has two general choices: (1) deny the warrant application for the entire account, or (2) grant the warrant application for the entire account. Although this issue has yet to surface in the circuit courts, a number of district courts have recently been confronted with this problem and have been divided in their rulings.[21]

The two general approaches taken by the district courts recognize competing interests. Denial of such warrant applications recognizes the individual's Fourth Amendment right to privacy,[22] while granting such warrant applications recognizes the government's investigatory ability interest and the desire for safety and security.[23] With these competing interests in mind, this Note argues that, in such situations, a warrant application providing the government access to an entire e-mail account should be granted. Not granting the warrant and some of the alternatives that have been suggested in light of this position do not adequately respect the government's legitimate investigatory interest. Coupled with certain limitations and ex ante

---

[19] *See id.* (recognizing that liberty erodes when safeguards to liberty are relaxed "[i]n the face of plausible-sounding governmental claims of a need to deal with widely frightening and emotion-freighted threats to the good order of society").

[20] *See* Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 140–41 (2011) (comparing a search for responsive electronic evidence to searching for needles in a haystack and pointing out that, to find the needles, it is necessary to look through a lot of hay).

[21] *Compare In re Target Email/Skype Accounts*, Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 WL 4647554, at *4 (D. Kan. Aug. 27, 2013) (declining to grant a warrant giving the government access to an entire e-mail account when only partial probable cause existed), *with In re A Warrant for All Content and Other Information Associated with the Email Account xxxxxxx@Gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F. Supp. 3d 386, 388 (S.D.N.Y. 2014) [hereinafter *In re Gmail Account*] (granting such a warrant).

[22] *See* Amsterdam, *supra* note 18, at 354.

[23] *Id.*

minimization procedures, a modified pro-access approach effectively strikes a balance between the competing investigatory and privacy interests.

Part I of this Note examines the Fourth Amendment particularity requirement, explains how it relates to the breadth of probable cause, and surveys how these concepts have been applied in the electronic context. Part II assesses the issue of the breadth of probable cause regarding e-mail accounts in particular and reviews the different approaches the district courts have taken in addressing this issue, as well as other proposed solutions that may be implemented in accordance with these approaches. Lastly, Part III proposes a resolution to the controversy, balancing the competing interests of privacy and the government's investigatory needs, and argues for a tempered version of permitting the government access to an entire e-mail account when probable cause only exists for a portion of the account.

I. OVERVIEW: FOURTH AMENDMENT PARTICULARITY AND BREADTH OF PROBABLE CAUSE

A. Framing the Issue

The Fourth Amendment of the United States Constitution provides:

> 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.[24]

In *Warshak*, the United States Court of Appeals for the Sixth Circuit determined that the search and seizure of e-mail content, received from an ISP without a warrant is unreasonable.[25] As a result, the warrant requirements stated in the Fourth Amendment apply in this context. These requirements are: (1) probable cause; (2) support of the probable cause by some form of affirmation; and (3) particularity in the description of what is to be searched and seized.[26] In addition, there must also

---

[24] U.S. CONST. amend. IV.

[25] *See supra* notes 11–15 and accompanying text.

[26] U.S. CONST. amend. IV.

be probable cause to support the breadth of what is being sought.[27] As this Note assumes probable cause exists for some part of an e-mail account, the discussion will focus on the particularity requirement, its meaning, and how it relates to the breadth of probable cause.

B. Reasons for the Particularity Requirement

The particularity requirement is recognized to have been included in the Fourth Amendment largely as a result of the Framers' distaste for British Writs of Assistance and, more expansively, general warrants.[28] During colonial times, the British government would issue Writs of Assistance, which essentially amounted to broad, general search warrants.[29] The goal of these warrants was to give the British government power to enforce trade and navigation laws in the Colonies by allowing officers broad permission to search for smuggled goods.[30] Neither the house to be searched, nor the type of goods to be searched for, would be specified and full discretion over the search was given to the officers conducting the search.[31]

The Fourth Amendment protects against such general warrants and general searches by requiring particularity in a warrant's description.[32] With this requirement, the officials executing the warrant are limited as to what they can search and seize and do not have unfettered discretion.[33] This recognizes the

---

[27] *See infra* note 53; *see also In re Target Email/Skype Accounts*, Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 WL 4647554, at *4 (D. Kan. Aug. 27, 2013) (listing the requirements of a search warrant: "it must be based on probable cause, meet particularity requirements, be reasonable in nature of breadth, and be supported by affidavit").

[28] Steagald v. United States, 451 U.S. 204, 220 (1981). For a twentieth-century example of a "general warrant," see Stanford v. Texas, 379 U.S. 476, 486 (1965) (characterizing a warrant that authorized any "books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments concerning the Communist Party of Texas, and the operations of the Communist Party in Texas" as "constitutionally intolerable").

[29] THOMAS N. MCINNIS, THE EVOLUTION OF THE FOURTH AMENDMENT 18 (2010).

[30] *Id.*

[31] *Id.* at 18–19.

[32] Marron v. United States, 275 U.S. 192, 196 (1927).

[33] *Id.* ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."). This statement has been interpreted to mean that the executing officer does not have discretion as a matter of

individual's interest in privacy and freedom from unreasonable governmental intrusion by restricting the scope of the government's investigation to that for which the government has probable cause.[34]

Other reasons for the particularity requirement have been noted. These reasons are closely related to the overall desire to avoid general warrants and the goal of protecting an individual's privacy as much as possible. For example, since warrant applications are granted by a magistrate—a neutral third party that operates outside the government's investigation[35]—the particularity requirement provides independent judgment on, and clarification regarding, what may be constitutionally searched and seized.[36] Particularity in a warrant's description thus gives clarity as to the warrant's scope, due to the limited authorization granted by the magistrate.[37] This helps protect an individual's interest in privacy by giving the government clear direction and authorization as to what is to be searched for and what is to be seized.[38]

Another reason given for the existence of a particularity requirement is that it helps give sharper teeth to the requirement of probable cause, not requiring it in a vague sense, but instead for a particular place and for particular things.[39] As with clarification,[40] specificity regarding probable cause helps protect an individual's privacy by limiting the scope of the government's search to that which may be reasonably expected to

---

opinion to determine whether a particular thing is covered within the parameters of the warrant, but does have discretion in determining whether a thing is covered as a matter of fact. *See* Strauss v. Stynchcombe, 165 S.E.2d 302, 307 (Ga. 1968). This interpretation implicitly recognizes that the review of some things not described under the warrant is permissible. *Id.*

[34] *See* Katz v. United States, 389 U.S. 347, 355–56 (1967). For an explanation of probable cause, see Brinegar v. United States, 338 U.S. 160, 175–76 (1949) ("Probable cause exists where the facts and circumstances within [the officers'] . . . knowledge . . . [are] sufficient in themselves to warrant a man of reasonable caution [to believe that] an offense has been or is being committed." (internal quotation mark omitted) (citation omitted)).

[35] *See* WAYNE R. LAFAVE, 2 SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.6(a) (5th ed. 2014).

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *See supra* notes 36–38 and accompanying text.

produce evidence related to the investigation.[41] As a result, the particularity requirement safeguards property of an individual by limiting the government to investigating only what may reasonably produce evidence of a crime.

C. The Meaning of Particularity

Particularity limits what places are to be searched and what objects are to be seized.[42] This requirement, along with the Fourth Amendment prohibition against unreasonable searches and seizures, restricts a search to the area necessary to find the evidence for which the government has probable cause.[43] Thus, if a warrant fails to appropriately define the scope of a search, or the resulting search extends beyond what is necessary to find what is reasonably sought, there is a violation of the Fourth Amendment.[44]

Whether a warrant's description satisfies the Fourth Amendment's particularity requirement is determined based on the language of the warrant and the facts and circumstances of the case.[45] At its core, the Fourth Amendment revolves around reasonableness.[46] To determine whether a warrant fails the particularity requirement, the focus must be on "whether there exists probable cause to support the breadth of the search that was authorized."[47] In the context of searches, a warrant is sufficiently particular if the executing officer can identify the

---

[41] *See* Groh v. Ramirez, 540 U.S. 551, 561 (2004) (explaining that one function of the particularity requirement is to assure individuals that warrants are executed under lawful authority and are appropriately limited to searching for what is needed).

[42] U.S. CONST. amend. IV.

[43] *See* LAFAVE, *supra* note 36 ("Knowledge that some objects connected with criminal activity are to be found on certain premises is no basis for permitting an unrestricted search of those premises . . . the described premises may only be searched as long and as intensely as is reasonable to find the things described in the warrant.").

[44] *Id.*

[45] *See* Martha Applebaum, Note, *"Wrong But Reasonable": The Fourth Amendment Particularity Requirement After* United States v. Leon, 16 FORDHAM URB. L.J. 577, 580–81 (1987); *see also* Go-Bart Importing Co. v. United States, 282 U.S. 344, 357 (1931) ("There is no formula for the determination of reasonableness.").

[46] Riley v. California, 134 S. Ct. 2473, 2482 (2014).

[47] United States v. Zemlyansky, 945 F. Supp. 2d 438, 464 (S.D.N.Y. 2013) (quoting United States v. Hernandez, No. 09 CR 625(HB), 2010 WL 26544, at *8 (S.D.N.Y. Jan. 6, 2010)).

place the warrant directs the officer to search with reasonable certainty.[48] Regarding seizures, the determination is ultimately based on what discretion is given to the officer executing the warrant.[49] The officer must be able to determine whether a particular thing is covered under the warrant, not as a matter of opinion, but as a matter of fact.[50] If the officer can determine whether a particular thing is covered under the warrant as a matter of fact with reasonable certainty, the warrant is sufficiently particular.[51] The underlying rationale is that the warrant, and not the executing officer, dictates where to search, what to search for, and what to seize.

1. Particularity and the Breadth of Probable Cause

A concept closely tied to the particularity requirement in the language of a warrant is the breadth of probable cause.[52] The standard for sufficient probable cause is, given the situation set forth in the affidavit, whether there is a "fair probability" that evidence of criminality relating to the investigation will be found in the particular place specified in the affidavit.[53] As the issuance of a warrant is contingent upon a probable cause showing, the government must have probable cause to search for and seize the items described in the warrant and must have

---

[48] Steele v. United States, 267 U.S. 498, 503 (1925).

[49] *See* Applebaum, *supra* note 45, at 580; *see also supra* note 33 and accompanying text.

[50] *See supra* note 33 and accompanying text.

[51] *See supra* note 33 and accompanying text.

[52] The Fourth Amendment requires "probable cause . . . particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. Therefore, for a warrant to be issued, the government must have probable cause for the particular description contained in the warrant. *Id.*

[53] Illinois v. Gates, 462 U.S. 213, 214 (1983); *see* United States v. Hernandez, No. 09 CR 625(HB), 2010 WL 26544, at *7 (S.D.N.Y. Jan. 6, 2010) (explaining that one particularity-related inquiry is "whether the items listed as 'to be seized' in the warrant were overbroad because they lacked probable cause"). In *Hernandez*, the court pointed out that particularity in the language of the warrant is a closely related, but distinct, legal issue from the breadth of probable cause. *Id.* In the latter instance, the court referred to the analysis as one into the breadth of the warrant, whereas in the former instance, the inquiry is into the particularity of the language of the warrant. *Id.*

probable cause to justify the breadth of the search.[54] Whether the breadth of the search is justified is based on the specific circumstances of a case.[55]

This concept is best illustrated by example.[56] Imagine the police observe an individual leaving an apartment, one that was known by the police to contain marijuana. The police observe the individual holding a large brown paper bag the size of marijuana packages that the police had seen earlier. They watch as the individual walks from the apartment to his car, places the bag in his car, and drives away. As the individual drives off, the police pull him over. They search both the bag the individual was observed carrying from the apartment to his car and the rest of his car, as well.[57]

Under the facts of this example, the police had probable cause to search the bag; their prior knowledge regarding the apartment the individual was seen leaving, as well as their observance of the size of the bag and how it was similar in size to previously seen marijuana packages, gave the police probable cause to believe the bag contained evidence.[58] However, the police did not have probable cause to search the rest of the car.[59] No evidence existed for the government to believe the rest of the car contained any evidence, and, as a result, the police searching

---

[54] U.S. CONST. amend. IV. The Supreme Court has recognized that this requirement is not absolute: "In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976). In particular, this requirement is relaxed when the location of the relevant information is not known with exactness:

> Where proof of wrongdoing depends upon documents . . . whose precise nature cannot be known in advance, law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence which is properly specified in the warrant.

In re Gmail Account, 33 F. Supp. 3d 386, 392 (S.D.N.Y. July 18, 2014) (alteration in original) (quoting United States v. Scarfo, 180 F. Supp. 2d 572, 578 (D.N.J. 2001)).

[55] *Gates*, 462 U.S. at 238–39.

[56] The facts of this example are based on *California v. Acevedo*, 500 U.S. 565 (1991).

[57] In *Acevedo*, the officers did not need a warrant because the "automobile exception" to the Fourth Amendment warrant requirement applied. *Id.* at 566, 573. However, as the court recognized, even if a warrant is not necessary due to an exception, the government must still have probable cause to justify the breadth of a search. *Id.* at 579–80.

[58] *Id.* at 566–67, 572–73.

[59] *Id.* at 579–80.

the rest of the individual's car amounted to an overbroad search outside of the scope of their probable cause.[60] Under the Fourth Amendment, the search of the car is impermissible.[61]

2. The Plain View Exception

Although the Fourth Amendment requires particularity in the language of the warrant and the scope of probable cause, courts have recognized instances where items that are not described in the warrant can be seized. One exception involves items not specified in a warrant, but in "plain view" of officers executing a valid warrant.[62] Under this exception, for example, if officials have a warrant to search for certain evidence in a particular area and come across other evidence reflecting criminality not within the parameters of the warrant but in "plain view," this evidence may be seized by the officials.[63] Importantly, the officers who seize the items in plain view must have a legal right—a warrant, for example—to be in the area in which the items in plain view were found.[64] Absent some legal justification to be in the particular place, even if an item clearly reflects criminality, the officers cannot invoke the plain view exception and seize the item.[65] In addition, it must be immediately apparent to the officials that the item in plain view constitutes evidence of a crime.[66] Despite these limitations, the particularity required of the language of a warrant and the corresponding particularity required regarding the scope of probable cause are circumvented by this exception.

---

[60] *Id.*

[61] *Id.*

[62] Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971). The plain view exception also applies in instances in which officials are lawfully in a particular area, even absent a warrant. 68 GEORGE L. BLUM ET AL., AM. JUR. 2D *Searches and Seizures* § 241 (2014).

[63] *Coolidge*, 403 U.S. at 465; *see also, e.g.*, Horton v. California, 496 U.S. 128, 142 (1990) (determining that a police officer who had a warrant authorizing the search of an individual's home for stolen property could seize weapons observed in plain view, even though the weapons were not included in the warrant).

[64] *Coolidge*, 403 U.S. at 466.

[65] *Id.*

[66] *Id.*; *see also Horton*, 496 U.S. at 137 (noting that an officer must also lawfully be able to access the object intended to be seized under the plain view exception).

D. The Fourth Amendment in the Electronic Context

1. Early Developments

A starting point in consideration of the Fourth Amendment in the electronic context is that "the Fourth Amendment protects people, not places."[67] This means that the Fourth Amendment may apply not only to searches and seizures in a tangible sense, but also to searches and seizures in the electronic world of information in which persons may reasonably have an expectation of privacy.[68]

For example, in *Katz v. United States*, the government conducted an investigation of an individual suspected of passing bets across state lines, a violation of a federal statute.[69] As part of its investigation, the government placed a listening and recording device on the side of a public telephone booth where the individual made his phone calls.[70] During trial, the government used these conversations as evidence.[71] The defendant argued that the government's listening to and recording of his phone calls were a violation of the Fourth Amendment.[72] Both the defendant and the government focused their arguments on whether the telephone booth was a "constitutionally protected area" and whether physical invasion of such an area was required for a Fourth Amendment violation.[73]

The United States Supreme Court agreed with the defendant in finding a Fourth Amendment violation in the government's surveillance, but explained that the parties' arguments were misplaced.[74] Instead of focusing on the location of the defendant, the appropriate consideration involves the person—whether the government violated an expectation of privacy upon which an individual justifiably relied.[75] And, the Court held, since the

---

[67] Katz v. United States, 389 U.S. 347, 351 (1967).

[68] *Id.* at 351–52; *see also* Berger v. New York, 388 U.S. 41, 64 (1967) (holding a New York statute, which authorized eavesdropping through warrants requiring less than the Fourth Amendment, unconstitutional).

[69] *Katz*, 389 U.S. at 348.

[70] *Id.*

[71] *Id.*

[72] *Id.* at 348–49.

[73] *Id.* at 349–52.

[74] *Id.* at 351–52, 358.

[75] *Id.* at 351, 353; *see also supra* note 13 and accompanying text.

defendant justifiably relied on the privacy of his conversations within the phone booth, Fourth Amendment protections applied to the defendant's telephone conversations therein.[76]

In a similar vein, *Berger v. New York*[77] recognized that conversations can be "seized" within the meaning of the Fourth Amendment.[78] *Berger* involved the examination of a New York state statute authorizing electronic eavesdropping and whether its requirements were in accordance with the Fourth Amendment.[79] The Court ultimately found that the statute ran afoul of Fourth Amendment protections by authorizing searches and seizures that fell short of the Fourth Amendment's requirements, thereby characterizing the New York statute as plainly overbroad.[80] Implicit in this conclusion is that Fourth Amendment protection can apply to conversations in which persons have a reasonable expectation of privacy, including electronically transmitted conversation.[81]

2. Recent Developments in the Electronic Context

Katz and *Berger* establish that Fourth Amendment protections can apply to nontangible electronic things, such as phone conversation. Later cases have also affirmed this idea,[82] including in the context of e-mail accounts.[83] Yet, these cases do not confront the Fourth Amendment requirements of particularity and limited breadth in seeking access to electronic information. More recent developments provide some guidance on these issues.[84]

---

[76] *Katz*, 389 U.S. at 353.

[77] 388 U.S. 41 (1967).

[78] *Id.* at 59.

[79] *Id.* at 43–44.

[80] *Id.* at 62–64.

[81] *See supra* Introduction (explaining that, in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), Fourth Amendment protections were extended to e-mail accounts).

[82] *E.g.*, Riley v. California, 134 S. Ct. 2473, 2495 (2014) (holding that, under the Fourth Amendment, a warrant is required to search the contents of a cell phone).

[83] *Warshak*, 631 F.3d at 288.

[84] Language from the recent Ninth Circuit case, *United States v. Comprehensive Drug Testing, Inc.*, presents the issue well:

> This pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant. The problem can be stated very simply: There is no way to be sure exactly what an electronic file contains without

For example, in the context of computer hard drive searches, courts will often permit off-site review.[85] This involves the creation of a mirror-image copy of the hard drive, which impacts the target's use of his computer as little as possible, and in return provides a more convenient means for the government to search the target's information.[86] This procedure allows the government to obtain the data on the hard drive for which it has probable cause, but, in so doing, it also provides the government access to data on the hard drive for which it does not have probable cause. However, after obtaining the hard drive, the subsequent search of the hard drive must still be conducted in accordance with the Fourth Amendment's rule of reasonableness.[87] Reasonableness is considered on a case-by-case basis.[88]

The parameters of reasonableness have been shaped in recent years regarding warrants for electronic information. Search warrants authorizing the wholesale search of "computers and computer equipment" and "computer records or data" have been upheld as reasonable.[89] The Tenth Circuit has also noted that a search of the contents of a hard drive may extend as far as necessary to find the items specified to be seized under the warrant.[90] In one case, the court upheld a warrant that permitted the search of " 'any [computer] equipment' that can create or display computer data" and "any and all computer software."[91] Because the government agent who conducted the

---

> somehow examining its contents—either by opening it and looking, using specialized forensic software, keyword searching or some other such technique. . . . By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there.

621 F.3d 1162, 1176 (9th Cir. 2010).

[85] United States v. Ganias, 755 F.3d 125, 135–36 (2d Cir. 2014).

[86] *Id.*

[87] *Id.* at 136.

[88] *Id.*

[89] *See* United States v. Farlow, 681 F.3d 15, 16–19 (1st Cir. 2012); s*ee also* United States v. Richards, 659 F.3d 527, 539–40 (6th Cir. 2011) ("Applying a reasonableness analysis on a case-by-case basis, the federal courts have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers."); United States v. Stabile, 633 F.3d 219, 234 (3d Cir. 2011) (holding seizure of six entire hard drives reasonable).

[90] United States v. Grimmett, 439 F.3d 1263, 1270 (10th Cir. 2006); s*ee also* United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009) (stating that, as a practical matter, finding relevant information may often involve the government looking at many folders and documents contained on a computer hard drive).

[91] *Grimmett*, 439 F.3d at 1270 (alteration in original).

search testified that he limited the search to certain types of files likely to reveal the type of information described in the warrant, the court upheld the warrant and denied the defendant's motion to suppress.[92]

II. FOURTH AMENDMENT PROTECTIONS, PARTICULARITY, AND THE BREADTH OF PROBABLE CAUSE IN THE E-MAIL CONTEXT

In *United States v. Warshak*,[93] the United States Court of Appeals for the Sixth Circuit Court of Appeals held that Fourth Amendment protections extend to the content of e-mail accounts and that it is constitutionally impermissible for the government to obtain access to an individual's e-mails from a service provider without a warrant based upon probable cause.[94] As a result, the government must obtain a warrant to have access to an individual's e-mails. Part of the government's burden in obtaining a warrant requires the affidavit in support of the warrant to particularly describe what is sought—this applies to both the place to be searched and the things to be seized—and that the breadth of the warrant's scope is reasonable.[95] Due to the nature of e-mail,[96] however, the concepts of particularity and breadth in this context have proven problematic and there is currently a lack of consensus in the district courts as to what these requirements entail.[97]

The basic approaches fall into two camps, with one side denying warrant applications for an individual's entire e-mail account, and the other granting such warrants.[98] Both courts and commentators have offered suggestions and adjustments regarding these approaches.[99] The following sections explain the two approaches, their rationales, and the suggestions that have been proposed in accordance with these approaches, which aim to balance the competing interests of the government and the individual.

---

[92] *Id.*
[93] 631 F.3d 266 (6th Cir. 2010).
[94] *Id.* at 288.
[95] U.S. CONST. amend. IV.
[96] *See supra* note 20 and accompanying text.
[97] *See infra* Sections II.A, B.
[98] *See infra* Sections II.A, B.
[99] *See infra* Sections II.A, B.

A. *Approach One: Deny the Warrant Application*

One approach is to deny a warrant application providing the government access to an entire e-mail account when probable cause has not been established for the entire account. For example, in *In re Applications for Search Warrants for Information Associated With Target Email Accounts/Skype Accounts* ("*In re Target Email/Skype Accounts*"),[100] the United States District Court for the District of Kansas denied such a request.[101]

In that case, the targets of the search were alleged to have stolen computer equipment and transported it across the country.[102] The government argued that the targets' e-mail accounts were used to facilitate the criminal activity and sought search warrants[103] to search for evidence of criminal activity in the accounts.[104] In denying the search warrant applications, the court concluded that the content listed on the applications, if handed over, would amount to a violation of the Fourth Amendment, as the warrants failed to place any restrictions whatsoever on which communications and information were to be handed over.[105] This was problematic in the eyes of the court

---

[100] Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 WL 4647554 (D. Kan. Aug. 27, 2013).

[101] *Id.* at *10. The District of Kansas has taken this position in other similar cases as well. *See, e.g.*, *In re* Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Info. Associated with 12-MJ-8191-DJW Target Email Address, Nos. 12-MJ-8119-DJW, 12-MJ-8191-DJW, 2012 WL 4383917, at *11 (D. Kan. Sept. 21, 2012).

[102] 2013 WL 4647554, at *1.

[103] The following language is illustrative of the breadth of the warrants:

> [The service provider shall disclose] [t]he 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 . . . .

Id.

[104] *Id.* The procedure of requesting the content and information from the service providers was governed by The Stored Communications Act, 18 U.S.C. § 2701 *et seq*. *Id.* at *2. Section 2703 authorizes the government's ability to request electronically stored or held communications, such as e-mail, pursuant to a search warrant under Rule 41 of the Federal Rules of Criminal Procedure. *Id.*

[105] *Id.* at *8. "The warrants as currently proposed give the government virtual carte blanche to review the content of all electronic communications associated with

because the warrants failed to establish probable cause to search all of the account information.[106] Comparing the government's warrant applications to one requesting that a post office provide copies of the contents of all mail to and from a certain address, which would not pass constitutional muster, the court concluded that the same attempt in the electronic context should likewise not be held constitutional.[107]

The United States District Court for the Northern District of California has taken the same approach when faced with such an application. In the case *In re: [REDACTED]@gmail.com*,[108] the court took particular issue with a warrant application's lack of a date range for the desired e-mails, and a lack of language indicating that the government would return or destroy nonresponsive information.[109]

In response to the above concens, some suggestions have been made as potential solutions to the problem. For example, although the court in *In re Target Email/Skype Accounts* did not advocate for any particular procedural mechanism that could be utilized to avoid overbroad warrant applications while still providing the government with access to portions of an e-mail account, the court did provide a few suggestions[110]: (1) asking the service provider to limit the amount of content requested by restricting the information to e-mails with certain terms, or mail only to and from certain recipients; (2) appointing someone to hire an independent vendor to use computerized search techniques to review the information for relevance; or (3) establishing a filter group to review the information for relevance.[111]

---

the accounts and fail to adequately limit the discretion of the government-authorized agents executing the warrants." *Id.* at *9.

[106] *Id.* at *8.

[107] *Id.* The court noted that while neither the Federal Rules of Criminal Procedure, nor the Stored Communications Act placed this limitation on the government, the Fourth Amendment did. *Id.* at *9 ("To comport with the Fourth Amendment, the warrants must contain sufficient limits or boundaries so that the government-authorized agent reviewing the communications can ascertain which email communications and information the agent is authorized to review.").

[108] 62 F. Supp. 3d 1100 (N.D. Cal. 2014).

[109] *Id.* at 1104 ("This unrestricted right to retain and use every bit [the e-mail account] coughs up undermines the entire effort the application otherwise makes to limit the obvious impact under the plain view doctrine of providing such unfettered government access.").

[110] *In re Target Email/Skype Accounts*, 2013 WL 4647554, at *10.

[111] *Id.*

Others have advocated for similar approaches. For example, one scholar suggests that, in the event it is impossible for the government to describe which e-mails and other content are sought by the government, the appropriate solution would be to have the e-mail service provider sift through the content and only provide the government with the relevant information.[112] In the event e-mail service providers resist this burden, she proposes a filter-team "consisting of agents or specially-trained computer personnel who are not involved in the investigation" do the sifting.[113] Through this mechanism, it is argued, the Fourth Amendment particularity and breadth requirements would be satisfied.[114]

B. Approach Two: Grant the Warrant Application

A contrasting approach some courts have taken when faced with a warrant application to search an entire e-mail account where evidence of a crime is located only in individual messages, is to grant the request. The United States District Courts for the District of Maine[115] and the District of Nevada[116] have granted such requests.[117] In addition, in *In re A Warrant for All Content and Other Information Associated with the Email Account*

---

[112] Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored Email Surveillance*, 90 NEB. L. REV. 971, 1013 (2010).

[113] *Id.* at 1014–15.

[114] *Id.* at 1016.

[115] United States v. Taylor, 764 F. Supp. 2d 230, 236–37 (D. Me. 2011). In that case, the magistrate judge issued a warrant that permitted the government to search all information relating to an e-mail account of the defendants and to seize information evidencing the violation of a certain federal statute. *Id.* at 232. The District Court denied the defendant's later Motion to Suppress: "The Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching." *Id.* at 237.

[116] United States v. Bickle, No. 2:10-cr-00565-RLH-PAL, 2011 WL 3798225, at *20 (D. Nev. July 21, 2011) (agreeing that a prescreening method is not required to separate irrelevant material from relevant material before providing the government with access to an e-mail account).

[117] In both *Taylor* and *Bickle*, the courts also approved a filter process which functioned to filter out privileged material from the e-mail accounts (e.g. information between the defendant and his lawyer). However, in neither case was a filter process used to filter out irrelevant information. *Bickle*, 2011 WL 3798225, at *20; *Taylor*, 764 F. Supp. 2d at 232–33, 235.

xxxxxxx@Gmail.com Maintained at Premises Controlled by Google, Inc. ("*In re Gmail Account*"),[118] the Southern District of New York also granted such a request.[119]

In *In re Gmail Account*, the government conducted an investigation into an individual on the basis of possible unlawful money remitting, conspiracy to commit unlawful money remitting, and conspiracy to commit money laundering.[120] As part of its investigation, law enforcement made an application for a search warrant to search the contents of, and all information associated with, the target's e-mail account.[121] In its application for the warrant, the government provided probable cause to believe that the e-mail account was being used to conduct criminal activity and to believe certain information contained in the account would reveal evidence of that criminal activity.[122] The search warrant required the service provider to disclose " 'all content and other information within the Provider's possession, custody, or control associated with' the email account, including all emails sent, received, or stored in draft form, all address book information, and a variety of other information associated with the account."[123] The search warrant also directed that law enforcement officials were authorized to comb through the provided content—that is, the entire account—to locate categories of information provided for in the warrant.[124]

The court granted the search warrant application, noting first that the Fourth Amendment hinges on reasonableness.[125] The court then focused its opinion on the reasonableness of the warrant application.[126] It stressed the degree of leniency regarding which documents could be searched that courts generally permit when the government conducts a physical search for evidence.[127] This allowance is due to law enforcement's need to examine documents in order to perceive their relevance to the investigation; it is impossible to know beforehand whether

---

[118] 33 F. Supp. 3d 386 (S.D.N.Y. 2014).
[119] *Id.* at 388.
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.* at 389–90.
[126] *See id.* at 390–96.
[127] *Id.* at 391–92.

a document is pertinent to the investigation and, as a result, sometimes innocuous documents are reviewed.[128] Applying this concept to the case at hand, the court reasoned that the same logic should apply in the electronic context.[129] In addition, the court disagreed with the option of having the service provider, Google, examine the account and send over only relevant information, citing Google's lack of ability to cull responsive information, the burden this would place on service providers, and the fact service providers consist of private employees who have no constitutional responsibilities to the public as significant issues that weigh against this option.[130]

Another case in which a court granted a warrant application in similar circumstances is *In re the Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.* ("*In re Apple Account*").[131] Overturning a prior order denying a search warrant request,[132] the court held that the government's application complied with the Fourth Amendment.[133] While echoing the reasoning utilized in *In re Gmail Account* in granting the request, the court did note the increased risk of infringements on privacy with the mass of information held in undifferentiated electronic format coupled with law enforcement's ability to access such information.[134] However, the court explained that the unique challenges posed when searching for responsive electronic data to gather evidence requires a practical solution.[135] Recognizing the difficulties, if not impossibilities, created for law enforcement officials in holding otherwise, the court granted the warrant application.[136]

---

[128] *Id.*

[129] *Id.* at 392.

[130] *Id.* at 394–95.

[131] 13 F. Supp. 3d 157 (D.D.C. 2014) [hereinafter *In re Apple Account*]. In this case, the government similarly applied for a search warrant to search an e-mail account, and provided information to support a finding of probable cause for some of the information in the account. *Id.* at 160.

[132] *In re* Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 145 (D.D.C. 2014). The prior order essentially relied on the same reasoning as the court did in *In re Target Email/Skype Accounts*. *See supra* Section II.A.

[133] *In re Apple Account*, 13 F. Supp. 3d at 168.

[134] *Id.* at 163–67.

[135] *Id.* at 166.

[136] *Id.* at 166–67.

1. Ex Ante Minimization Procedures

Some courts that have granted warrant applications in the electronic context have imposed ex ante limitations regarding the handling and retention of the material listed in a warrant.[137] For example, in a case involving a search warrant for content contained on a personal computer, the Supreme Court of Vermont upheld an order imposing certain ex ante limitations in order to ensure that the Fourth Amendment's particularity and breadth requirements were not violated.[138] In that case, the court addressed concerns over the constitutional authority of the magistrate to impose such restrictions.[139] Since the restrictions on a warrant become part of the warrant, the government's nonobservance of the restrictions amounts to a constitutional violation.[140] Noting that disagreement exists as to the constitutionality of ex ante limitations,[141] the court ultimately upheld the limitations.[142] The court focused on the fact that the Fourth Amendment ultimately is based on reasonableness, pointing out that such restrictions provide one way reasonableness can be achieved.[143] In addition, in the physical, nonelectronic realm, certain ex ante limitations[144] can be, and often are, imposed.[145] As a result, although the Fourth Amendment does not require ex ante limitations be imposed on a warrant, the court held that, in appropriate circumstances, the imposition of ex ante limitations is permitted.[146]

The use of ex ante minimization procedures has not been met with universal approval. One argument against imposing such procedures is that other procedures are available that

---

[137] Examples of such limitations include limiting the permitted search methods, directing the destruction or return of nonresponsive information, and requiring the government to place a limit on the amount of time they may search and seize. *See In re* Appeal of Application for Search Warrant, 71 A.3d 1158, 1162–63 (Vt. 2012) [hereinafter *In re Search Warrant*].

[138] *Id.* at 1182.

[139] *Id.* at 1166–70.

[140] *Id.* at 1164.

[141] *See* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1242 (2010).

[142] *In re Search Warrant*, 71 A.3d at 1170.

[143] *Id.*

[144] *See supra* note 137 and accompanying text.

[145] *In re Search Warrant*, 71 A.3d at 1170.

[146] *Id.*

provide adequate relief, such as suppression motions.[147] This renders the imposition of prospective limitations unnecessary.[148] Another argument is that the imposition of prospective limitations is impermissible altogether, as magistrates do not have the authority to impose such restrictions.[149] Under this view, such restrictions are unreasonable because they judge the reasonableness of a search before the search ever takes place and impermissibly control the method by which a search must be conducted.[150]

2. Elimination of the Plain View Doctrine in the E-mail Context

Another idea that has been suggested to limit the effects of unrestricted government access to an e-mail account is to eliminate the plain view doctrine in the electronic context.[151] Doing so would allow the government broad access to content, some of which the government likely does not have probable cause for, but would prevent the government from using any information derived from this content that falls outside the scope of the warrant.[152] As a result, this suggestion grants the government discretion in conducting a search, but preempts use of seized information at trial to only what was specified in the warrant.[153] So, instead of preventing the government from seeing information outside the scope of a warrant, this method prevents the government from using that information. However, like the

---

[147] *See In re Gmail Account*, 33 F. Supp. 3d 386, 400–01 (S.D.N.Y. 2014).

[148] *Id.*

[149] *See* Kerr, *supra* note 141, at 1246.

[150] *Id.*

[151] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 582–84 (2005) [hereinafter *Searches and Seizures in a Digital World*]. However, when the article was written in 2005, Kerr noted that "[i]t is too early for courts or Congress to impose such a rule." *Id.* at 583. In a recent Washington Post article, Kerr suggested that the time may have come, at least for the e-mail context. Orin Kerr, *A Remarkable New Opinion on Search Warrants for Online Accounts – And Why I Think It's Wrong* [hereinafter *New Opinion on Search Warrants for Online Accounts*], WASH. POST (Mar. 27, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/03/27/remarkable-new-opinion-on-online-accounts.

[152] *Searches and Seizures in a Digital World*, *supra* note 151, at 582–83.

[153] *Id.* at 583.

suggestion of ex ante minimization procedures, the elimination of the plain view doctrine in the electronic context has been met with some disapproval.[154]

III. THE CURRENT APPROACHES' INADEQUACIES: PROPOSED RESOLUTION

District courts have taken inconsistent approaches when faced with a warrant application that would provide the government access to an entire e-mail account when probable cause does not exist for the entire account.[155] As a result, this area of the law is muddled with conflicting views and incompatible opinions. This conflict derives from the ambiguity of the Fourth Amendment; as courts have repeatedly quoted, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.' "[156] While reasonableness has developed some definitional contours in the physical realm, it has proven difficult to shape in the cybersphere.[157]

The cases summarized in Part II of this Note provide some guidance as to what courts interpret reasonableness to mean regarding particularity in warrant applications for e-mail accounts and the appropriate breadth of e-mail account disclosure.[158] While the two general approaches agree that reasonableness involves a balance of the individual's right to privacy and the government's need to investigate criminal activity, the approaches weigh the two factors differently.[159] However, neither approach balances these competing interests adequately. While denying warrants that request full access to an individual's e-mail account or requiring e-mail service provider or third-party involvement, both which significantly restrict law enforcement,[160] granting such warrants outright fails to adequately respect the individual's right to privacy.[161] Instead, an appropriate solution would be to grant warrant applications

---

[154] *See* Alison Bonelli, Comment, *Computer Searches in Plain View: An Analysis of the Ninth Circuit's Decision in* United States v. Comprehensive Drug Testing, Inc., 13 U. PA. J. CONST. L. 759, 780–81 (2011).

[155] *See supra* Part II.

[156] Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

[157] *See supra* Part II.

[158] *See supra* Part II.

[159] *See generally supra* Part II.

[160] *See supra* note 18 and accompanying text.

[161] *See supra* note 19 and accompanying text.

giving the government full access to an e-mail account through the e-mail service provider, while imposing ex ante minimization procedures on a case-by-case basis and abolishing the plain view doctrine in this context. Through these methods, the government's role in investigating crime and the individual's right to privacy are balanced in a reasonable manner.

This section elaborates on why the current approaches are inadequate and proposes a middle ground approach, which incorporates the rationales behind the current approaches to achieve a reasonable solution. In addition, potential criticisms of the proposed solution are considered and addressed.

A. Why the Current Approaches Are Inadequate

The two current approaches each have troublesome implications. Denial of a warrant application requesting full access to an e-mail account in this context hampers the government's ability to investigate crime,[162] and therefore fight it as effectively as possible.[163] This problem is accentuated by the prevalence of the e-mail account as a means of communication, both for personal and business use.[164] Law enforcement efforts would also be burdened if, as has been suggested,[165] a court were to order the e-mail service provider or a third party to cull responsive information from an e-mail account.[166] Having an e-mail service provider produce only the responsive information would involve a number of issues. These include the substantial burden that would be placed on e-mail service providers,[167] e-mail

---

[162] *See supra* Section II.A.

[163] *See In re Gmail Account*, 33 F. Supp. 3d 386, 395–96 (S.D.N.Y. 2014); *see also* Amsterdam, *supra* note 18.

[164] The number of e-mail accounts worldwide was estimated to be 3.9 billion in 2013 and is expected to increase to over 4.7 billion by 2017. *Email Statistics Report, 2013–2017*, THE RADICATI GROUP, INC. (April 2013), http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf.

[165] *See, e.g.*, *In re Target Email/Skype Accounts*, Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 WL 4647554, at *10 (D. Kan. Aug. 27, 2013); Friess, *supra* note 112, at 1013–14.

[166] *In re Gmail Account*, 33 F. Supp. 3d at 395.

[167] *Id.* at 394–95; *see also* Friess, *supra* note 112, at 1014 (noting the possibility that e-mail service providers, such as ISPs, may be unwilling to function in this role). The potential for significant burden becomes obvious when one considers the number of users some e-mail service providers have. *See* Sean Ludwig, *Gmail Finally Blows Past Hotmail to Become the World's Largest Email Service*, VENTUREBEAT (June 28, 2012), http://venturebeat.com/2012/06/28/gmail-hotmail-

service providers' lack of skill in conducting law enforcement investigations,[168] and the problem of allowing private companies to know the details and scope of law enforcement investigations.[169] While some of these issues would not be present if a court were to instead order a third party, such as a filter team "consisting of agents or specially-trained computer personnel . . . who are not involved in the investigation" to sift through the information,[170] this approach is also not free of issues[171] and is often rejected by courts in other contexts.[172]

In addition, in the similar context of computer searches, warrants authorizing the wholesale seizure of computer records by the government have been found reasonable.[173] In so holding, courts recognize that, although probable cause does not exist for an entire computer, the government may be allowed access to the computer in order to search for relevant information.[174]

However, granting a warrant application requesting full access to an e-mail account, while imposing no subsequent restrictions on the government's ability to search and seize the

---

yahoo-email-users/ (reporting that, in June 2012, Gmail had 425 million monthly active users).

[168] *In re Gmail Account*, 33 F. Supp. 3d at 395. Of course, the government could provide the e-mail service provider with certain terms for the provider to use to search for evidence. However, this procedure oversimplifies the nature of investigations. For a simple explanation of why this is, see *New Opinion on Search Warrants for Online Accounts*, *supra* note 151:

> [T]ake the facts of this case. Maybe the suspects in this case are dumb and they wrote things in their e-mail such as, "let's engage in a conspiracy to commit a criminal kickback scheme that is a felony crime!" If so, a keyword search for terms like "conspiracy" and "kickback" will retrieve at least some of the evidence. But maybe the suspects are more savvy, and they used code words that a keyword search won't easily identify.

[169] *In re Gmail Account*, 33 F. Supp. 3d at 395.

[170] *See* Friess, *supra* note 112, at 1014 (suggesting this method).

[171] For example, this approach merely transfers the intrusiveness of the search from being an act of government to being an act of a third party working at the direction of the government. Although the Fourth Amendment is concerned with government over-intrusiveness, privacy concerns are not adequately solved by having someone else read an individual's personal information for the government.

[172] *See* United States v. Bowen, 689 F. Supp. 2d 675, 682 (S.D.N.Y. 2010) ("[T]he Fourth Amendment [does not] require the executing authorities to delegate a pre-screening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching.").

[173] *See supra* Section I.D.2.

[174] *See supra* Section I.D.2.

information contained within the account,[175] is not unproblematic. Due to the widespread use of e-mail for both personal and business communication,[176] unrestricted wholesale authorization would give the government the ability to freely examine and use large masses of information, much of which the government likely does not have probable cause for.[177] Significantly, this is questionable in light of the Fourth Amendment requirement of particularity in a warrant's description and the requisite limited breadth of a subsequent search and seizure.[178]

B. Proposed Resolution

As noted above, denying a warrant application that provides the government access to an entire e-mail account or having e-mail service provider or third-party involvement is problematic. This points towards using the other approach some courts have taken—granting such applications outright.[179] However, this approach is equally problematic because the government would have virtual carte blanche access to, and the unrestricted ability to use, all of the information contained in an e-mail account. And, as the Fourth Amendment reflects, unrestrained government investigatory capabilities are unsettling. As a result, adopting the following two restrictions in this context, while still permitting the government full access to an e-mail account upon probable cause for some of an account, achieves a reasonable balance of the government's and the individual's interests: (1) on a case-by-case basis, impose certain minimization procedures, and (2) eliminate the plain view doctrine in this context.

---

[175] *See supra* Section II.B.

[176] *See supra* note 164 and accompanying text.

[177] *In re Target Email/Skype Accounts*, Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 WL 4647554, at *8 (D. Kan. Aug. 27, 2013).

[178] U.S. CONST. amend. IV. Indeed, for example, although in the context of computer hard drive searches, courts have found the seizure of entire hard drives reasonable, the subsequent search of the hard drives is still subject to a reasonableness examination. *See* United States v. Ganias, 755 F.3d 125, 136 (2d Cir. 2014).

[179] *See supra* Section II.B.

1. Ex Ante Minimization Procedures

One way in which the government's and the individual's interests can be balanced is the imposition of certain ex ante minimization procedures, if necessary, to limit government overintrusiveness when conducting searches of e-mail accounts.[180] Examples of potentially effective minimization procedures include instructions "requiring police to use focused search techniques and prohibiting the use of specialized search tools without prior court authorization," as well as instructions "pertaining to the copying, destruction and return of data."[181] The procedures to be imposed, if any, depend upon the nature and facts of an investigation; however, it is important that courts consider implementing them to limit the potential for government overintrusiveness.[182]

Against this suggestion, some would argue that ex ante restrictions should be proscribed because they determine the reasonableness of a search before the search takes place.[183] Another argument against the restrictions is that other procedures, such as suppression motions, provide adequate relief in themselves.[184] However, some courts have recognized the utility of such restrictions and that some jurisdictions even statutorily require minimization procedures in the context of warrants for electronic surveillance.[185] While imposing ex ante minimization procedures is not a flawless solution, the procedures may provide an effective tool in preventing government investigatory overreach and should be considered to provide balance to the competing interests of the individual and the government.

2. Elimination of the Plain View Doctrine in This Context

Additionally, to combat the fear of general warrant issuance in the e-mail context, the government's ability to use information found in an e-mail account should be limited to the information that is specified in the warrant; in other words, the plain view

---

[180] *See supra* note 137 and accompanying text.
[181] *In re Search Warrant*, 71 A.3d 1158, 1172 (Vt. 2012).
[182] *See supra* Section II.B.1.
[183] *E.g.*, Kerr, *supra* note 141, at 1246.
[184] *In re Gmail Account*, 33 F. Supp. 3d 386, 401 (S.D.N.Y. 2014).
[185] *In re Search Warrant*, 71 A.3d at 1170.

doctrine should be eliminated in this context.[186] Any information that may be potentially incriminating but falls outside of the scope of information to be seized should be subject to exclusion at trial. This position recognizes the interests of both the government and the individual. While the government has latitude in accessing an individual's entire e-mail account, its ability to use any information uncovered is limited in scope to the information sought before the government started looking into the account, and to the information for which the government already had probable cause to believe was in the account.

Despite the advantages this approach has in balancing the interests of the government and the individual, it comes with the significant drawback that it could lead to undesirable results due to its broad and inflexible nature.[187] As a disturbing illustration:

> [T]he evidence in plain view could be profoundly serious, ranging from photographs of a kidnapped child to plans to commit acts of terrorism. The judicial directive to forswear in advance the plain view doctrine, placed in a different context, is equivalent to demanding that a DEA investigative team engaged in the search of a residence for drugs promise to ignore screams from a closet or a victim tied to a chair.[188]

As a result, it has been argued that abolishing the plain view exception is inadvisable because it prevents the government from prosecuting individuals who are known to have committed crimes outside the scope of the current investigation.[189]

---

[186] Professor Orin Kerr has advocated for this abolition in the general electronic context. *See* Kerr, *supra* note 151, at 582–83. This position has also found some support in the Ninth Circuit. *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178 (2010) (Kozinski, C.J., concurring) ("When the government wishes to obtain a warrant to examine a computer hard drive or electronic storage medium to search for certain incriminating files, or when a search for evidence could result in the seizure of a computer . . . magistrate judges should insist that the government forswear reliance on the plain view doctrine." (citation omitted)). *But see id.* at 1184 (Callahan, J., concurring) ("The more prudent course would be to allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based case adjudication."). The elimination of the plain view doctrine is technically a type of *ex ante* minimization procedure, as the procedure prospectively imposes a restriction on the government's capabilities. *In re Search Warrant*, 71 A.3d at 1172.

[187] Eric Yeager, Note, *Looking for Trouble: An Exploration of How to Regulate Digital Searches*, 66 VAND. L. REV. 685, 714–15 (2013).

[188] *Id.* at 714 (quoting United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *7 n.3. (D. Me. Dec. 3, 2009)).

[189] *Id.* at 715–16.

Despite the fact that the abolition of the plain view doctrine may sometimes lead to perverse and undesirable results, there are a couple of important points to mention in support of abolishing the plain view doctrine in the context of e-mail. For example, this approach does not necessarily prevent the government from prosecuting individuals for crime X when the warrant is directed toward crime Y. Rather, this abolition only prohibits the government from prosecuting those individuals for crime X based on information learned from the warrant seeking evidence of crime Y. This means that if the government has probable cause at a later point for the same individual relating to the crime, which was previously in plain view but not within the scope of the warrant, the government may still prosecute that individual for that crime. Additionally, at least in the e-mail context, absent granting the government broad access to an e-mail account, the government would never come across this evidence now in "plain view."

Lastly, if the plain view exception is not abolished in the e-mail context, it is possible that the rationale behind the concepts of particularity and overbreadth, which are at the core of the Fourth Amendment, will be rendered irrelevant.[190] E-mails, like other forms of electronic storage and communication, can store an incredible amount of personal information. Absent eliminating the plain view doctrine, allowing the government access to an entire e-mail account, which is preferable compared to the alternatives that have been suggested,[191] would mean that no restrictions would exist as to the information the government could use against an individual.[192] This result would run counter to the Fourth Amendment and could very well have the effect of rendering the particularity and breadth requirements immaterial.[193]

CONCLUSION

The protections of the Fourth Amendment in the electronic context have started to take shape in recent years.[194] Specific to the context of e-mail accounts, one circuit court has held that

---

[190] *Searches and Seizures in a Digital World*, *supra* note 151, at 566.
[191] *See supra* Section III.A.
[192] *Searches and Seizures in a Digital World*, *supra* note 151, at 566.
[193] *Id.*
[194] *See supra* Section I.D and Part II.

Fourth Amendment protections apply to e-mail accounts stored with e-mail service providers.[195] Courts in other circuits have cited this opinion with approval.[196] However, even if this position is universally adopted, it would simply mean that a warrant is required for the government to access an e-mail account stored with a third party. It does not answer the more specific question of what portion of an account may constitutionally be provided to the government under a warrant granting access to the account, given that the government will likely not have probable cause for the entire account.[197] This issue has been faced by several district courts, and there is disagreement as to the correct resolution.[198]

Ultimately, the approaches of simply granting or denying such an application fail to adequately account for and balance the competing interests of the government's role in investigating crime and the individual's Fourth Amendment right to privacy. As a result, a middle ground approach is best tailored to fairly respect both interests: Courts should grant the government warrants that provide access to an entire e-mail account, even though probable cause may not exist for the entire account, but should also, if necessary, impose certain minimization procedures depending on the specific facts and circumstances of the case. In addition, the plain view exception that applies to physical searches and seizures should not apply in this context. Through these methods, the competing interests of the government and the individual can effectively be balanced and courts can achieve what has been often explained to be the core of the Fourth Amendment: reasonableness.

---

[195] United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010).
[196] *See supra* note 15 and accompanying text.
[197] *See supra* note 16 and accompanying text.
[198] *See supra* Part II.