DIGITAL SEARCHES, THE FOURTH AMENDMENT, AND THE MAGISTRATES' REVOLT

Emily Berman[*]

ABSTRACT

Searches of electronically stored information present a Fourth Amendment challenge. It is often impossible for investigators to identify and collect, at the time a warrant is executed, only the specific data whose seizure is authorized. Instead, the government must seize the entire storage medium—e.g., a hard drive or a cell phone—and extract responsive information later. But investigators conducting that subsequent search inevitably will encounter vast amounts of non-responsive (and often intensely personal) information contained on the device. The challenge thus becomes how to balance the resulting privacy concerns with law enforcement's legitimate need to investigate crime. Some magistrate judges have begun including in their warrants for digital searches limits on how those searches may be carried out—a development that some have referred to as a "magistrates' revolt," and which has both supporters and detractors. This Article argues that the magistrates' "revolt" was actually no revolt at all. Instead, these judges simply adopted a time-honored tool—minimization—that is used to address a conceptually analogous privacy threat posed by foreign intelligence collection. This Article further argues that embracing both the practice and the label of "minimization" will yield at least two benefits: First, it will recast magistrates' actions as a new instantiation of a legitimate judicial role, rather than a novel, potentially illegitimate practice. Second, it will allow magistrates to draw on lessons learned from the Foreign Intelligence Surveillance Court's creative use of minimization to safeguard Fourth Amendment rights in the intelligence-collection context.

[*] Assistant Professor of Law, University of Houston Law Center. Thanks go to participants in the "Courts at War" Conference at the University of Texas Law School, D. Theodore Rave, David Kwok, Dave Fagundes, Kellen Zale, Renee Knake, Gina Warren, James Nelson, and Lonnie Hoffman.

INTRODUCTION

In the 1967 Supreme Court case *Berger v. New York*, Justice Clark wrote that, "law, though jealous of individual privacy, has not kept pace with . . . advances in scientific knowledge."[1] In the half-century since he wrote those words, the gap between technological advancement and the legal regime has only grown wider. The pace of technological change has accelerated. The role of technology in Americans' daily lives has swelled. Yet even in this twenty-first century world, the speed at which legal change moves remains much as it has been since the eighteenth century.

When it comes to the Fourth Amendment—which protects against unreasonable searches and seizures of our "persons, houses, papers, and effects"—this sluggish pace has proved particularly problematic.[2] The information age has generated an avalanche of Fourth Amendment-law dilemmas[3]—whether the same rules that apply to searching suitcases at the border apply to a traveler's laptop computer;[4] whether mapping an individual's life 24/7 for days on end using cell phone location records requires a warrant;[5] whether the results of predictive algorithms generated using massive databases can form the basis of reasonable suspicion;[6] whether and how the warrant requirement's exception for searches incident to arrest should apply to the contents of an arrestee's cell phone.[7] It is up to courts in the first instance to resolve these questions.[8]

---

[1] 388 U.S. 41, 49 (1967).

[2] U.S. CONST. amend. IV ("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.").

[3] *See, e.g.*, United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring) (noting that "[d]ramatic technological change" creates legal uncertainty); *United States v. Ganias*, 755 F.3d 125, 134 (2d Cir. 2014), *rev'd en banc on other grounds*, 824 F.3d 199 (2d Cir. 2016) ("Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools."); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 808 (2004) [hereinafter Kerr, *The Fourth Amendment and New Technologies*] (discussing impact of changing technologies on Fourth Amendment doctrine).

[4] *See* United States v. Saboonchi, 990 F. Supp. 2d 536, 539 (D. Md. 2014) (answering in the affirmative).

[5] *See* Carpenter v. United States, No. 16-402 (U.S. June 22, 2018) (answering in the affirmative).

[6] *See* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 376–88 (2015).

[7] *See* Riley v. California, 134 S. Ct. 2473, 2477–78 (2014) (holding that the warrant exception for searches incident to arrest does not permit a search of a cellphone's contents).

[8] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 40–41 (2001) (considering whether use of thermal imaging devices to scan a private home was a search requiring Fourth Amendment protection); Katz v. United States, 389 U.S. 347, 351–53 (1967) (holding that placing an electronic listening device on a public telephone

Searches and seizures of electronic media, such as computers and smart phones, present judges with a particularly thorny example of this phenomenon. For a traditional analog search or seizure to pass Fourth Amendment muster, the government must (1) apply to a neutral magistrate for a search warrant, (2) satisfy that magistrate that there is probable cause to believe that the search will lead to evidence of a crime, and (3) identify with particularity the places to be searched and the evidence to be seized.[9] The magistrate then memorializes that information in a warrant, which authorizes law enforcement officials to execute a search of those places and to seize that evidence. These rules are designed to constrain government discretion, ensuring both that law enforcement officials have sufficient justification for infringing on a citizen's privacy and that the infringement is no more significant than necessary.[10]

When it comes to digital evidence, however, it is often impossible at the time of seizure to locate and segregate data that is responsive to a warrant from the vast amount of non-responsive (and often intensely personal) data stored on the same device. Imagine, for example, that Harry is suspected of tax fraud, and law enforcement gets a warrant to seize tax-related documents from his home computer. While looking through Harry's computer files for evidence of tax fraud, investigators are likely to come across quite a few non-tax-related files, which could be private items such as personal correspondence or detailed medical information. Similarly, investigators seeking evidence that a computer was used to view child pornography might discover (lawful) intimate photographs or an Internet search history suggesting a substance-abuse problem. In other words, the search might result in exactly the kind of intrusive search that warrants are supposed to prevent.[11]

Rule 41 of the Federal Rules of Criminal Procedure was amended in 2009 to recognize the unique nature of digital searches and offers as a partial solution a two-step process.[12] First, when it comes to digital searches, investigators may

booth qualified as a search because "the Fourth Amendment protects people, not places"); Olmstead v. United States, 277 U.S. 438, 464–65 (1928) (requiring a physical intrusion into a constitutionally protected area to trigger the Fourth Amendment), *overruled by Katz*, 389 U.S. 347, *and* Berger v. New York, 388 U.S. 41 (1967); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 494–525 (2011) (providing examples of courts adjusting Fourth Amendment doctrine in response to technology to maintain the balance of power between would-be criminals and law enforcement). Arguably, *Katz* added to the *Olmstead*-era rules rather than replacing them. *See* United States v. Jones, 565 U.S. 400, 405–07 (2012) (holding that *Katz* was not intended to withdraw any of the protection that the Fourth Amendment provides to private property).

[9] Dalia v. United States, 441 U.S. 238, 255 (1979).

[10] *See infra* notes 59–61 and accompanying text.

[11] *See infra* note 60 and accompanying text.

[12] FED. R. CRIM. P. 41 advisory committee's note to 2009 amendment.

engage in an overbroad seizure, such as seizing an entire computer, rather than only those files that contain evidence described in the warrant.[13] Then, investigators can subject the seized data to "a later review."[14] While this rule may ensure that law enforcement officers can perform a thorough seizure of evidence responsive to the warrant, it does not entirely solve the problem. Whenever the search ultimately takes place, investigators still must identify the evidence—tax returns, for example—and separate it from other non-responsive data, such as private letters. This raises the question of what limits, if any, should govern investigators' access to or use of the non-responsive information it encounters—a question that Rule 41 declines to answer.[15]

In an effort to fill this gap, a handful of magistrate judges took matters into their own hands in what has been described in some quarters as a "magistrates' revolt."[16] The "revolt" consisted of a series of opinions issued by federal magistrates around the country that sought to balance the interests of investigators against suspects' privacy rights by rejecting law enforcement's warrant requests for digital evidence unless those requests included (sometimes detailed) *ex ante* restrictions on how the government would carry out the search, such as limiting how long the government could keep the hardware it seized, specifying how the government would conduct the search, or explaining what the government would do with information it uncovered that fell outside the scope of the warrant.[17] The number of magistrates involved was not large, but the opinions had outsized effect, prompting a debate on the propriety of the practice.

The magistrates' approach has been championed by some commentators as an effective means of addressing the Fourth Amendment challenge posed by digital searches. Professor Paul Ohm argues, for example, that these types of

---

[13] FED. R. CRIM. P. 41(e)(2)(B).

[14] *Id.*

[15] *See infra* note 42 and accompanying text.

[16] *See, e.g.*, Reid Day, Comment, *Let the Magistrates Revolt: A Review of Search Warrant Applications for Electronic Information Possessed by Online Services*, 64 U. KAN. L. REV. 491, 510–11 (2015); 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), https://www.natlawreview.com/article/magistrates-revolt-unexpected-resistance-to-federal-government-efforts-to-get-genera; Scott H. Greenfield, *The Magistrates' Revolt Continues: Search Protocol*, SIMPLE JUST.: A CRIM. DEF. BLOG (Feb. 25, 2015), http://blog.simplejustice.us/2015/02/25/the-magistrates-revolt-continues-search-protocol/; Ann E. Marimow & Craig Timberg, *Low-Level Federal Judges Balking at Law Enforcement Requests for Electronic Evidence*, WASH. POST (Apr. 24, 2014), https://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.

[17] *See infra* Section II.B. and accompanying notes.

restrictions "have become necessary; they are the only way the courts can fulfill their constitutional duty to protect privacy from government overreaching."[18] The highly influential former Ninth Circuit Judge Alex Kozinski also contended that magistrates should include a series of *ex ante* instructions in the warrants for digital searches that they issue.[19] Indeed, several magistrates' orders considered part of the revolt used Judge Kozinski's suggested framework as a blueprint.[20]

Yet while it might seem like an elegant means to fill a gap in existing law, the practice has not been universally endorsed. Fourth Amendment expert Professor Orin Kerr has argued, for example, that memorializing *ex ante* rules for searches of electronic media is neither lawful nor normatively advisable.[21] Kerr and other opponents of the practice argue that it will result in excessive limitations on law enforcement officials, that necessary means of executing a digital search is unknowable *ex ante*, and that magistrates lack the expertise (and perhaps even the authority) to craft or oversee these types of restrictions.[22]

---

[18] Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. ONLINE 1, 11–12 (2011) (arguing that Professor Kerr is incorrect when he asserts that magistrates lack the authority to impose *ex ante* rules and stating, without elaboration, that magistrates *should* engage in this practice); *see also* Lily R. Robinton, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J.L. & TECH. 311, 343–44 (2010) (arguing that it would be unreasonable not to require investigators to employ "less intrusive, more effective search methods" where they exist); Derek Haynes, Comment, *Search Protocols: Establishing the Protections Mandated by the Fourth Amendment Against Unreasonable Searches and Seizures in the World of Electronic Evidence*, 40 MCGEORGE L. REV. 757, 771–74 (2009) (arguing that search protocols are not meant to impose unreasonable conditions on searches, but simply to determine how to exclude "irrelevant information from the scope of the search"); Marc Palumbo, Note, *How Safe Is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment*, 36 FORDHAM URB. L.J. 977, 999–1002 (2009) (arguing that technology exists that permits the government to engage in effective digital searches without "indiscriminately viewing everything on an individual's computer").

[19] *See infra* note 76.

[20] *E.g.*, *In re* the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1, 8 (D.D.C. 2014).

[21] *See, e.g.*, Orin S. Kerr, Ex Ante *Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1246 (2010) [hereinafter Kerr, Ex Ante *Regulation*] (arguing that *ex ante* restrictions are both unauthorized and unwise).

[22] *See id.*; *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 545–47, 575–76 (2005) [hereinafter Kerr, *Searches and Seizures in a Digital World*] (arguing that "it is more difficult to plan a computer search *ex ante*" because "the search procedures" are "more of an art than a science") (italics added); Andrew Vahid Moshirnia, Note, *Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain*, 23 HARV. J.L. & TECH. 609, 624–25 (2010) (arguing that limiting government search techniques "invites gaming" by bad actors); Bryan K. Weir, Note, *It's (Not So) Plain to See: The Circuit Split on the Plain View Doctrine in Digital Searches*, 21 GEO. MASON U. CIV. RTS. L.J. 83, 108–10 (2010) (arguing it is impossible to know in advance what methods will be necessary because the investigator, like the doctor "may not know how best to proceed until he opens up the patient and takes a look").

This Article contends that the true significance of this revolt has eluded both supporters and opponents. Neither appreciate that the magistrates' "revolt" was no revolt at all. Instead, these judges—whether consciously or unconsciously—have simply adapted to the digital search context a decades-old tool designed to resolve exactly the sort of privacy concerns that digital searches raise: "minimization."[23] Minimization procedures, whose specifics will vary from context to context, are procedural protections that judges may impose on searches and seizures when the investigative technique being authorized poses a significant privacy threat.[24] This Article contends that a brief look at the history of minimization procedures reveals that what some magistrates have been doing—the so-called revolt—is exactly the same thing that Congress has statutorily required in other contexts for decades.[25] It further argues that these judges should not only embrace the practice of imposing *ex ante* limits on digital searches but also recognize those limits for what they are—minimization procedures.

The most instructive, creative, and flexible use of minimization procedures—and thus the most useful model for magistrates—has come from the Foreign Intelligence Surveillance Court (FISA Court). The FISA Court is a federal court created by the Foreign Intelligence Surveillance Act of 1978 (FISA) to review government applications to engage in domestic surveillance for foreign intelligence purposes.[26] For the first three decades of its existence, the Court operated much like a magistrate judge evaluating requests for search warrants—determining (in secret and ex parte) whether government applications

---

[23] *See* 50 U.S.C. § 1801(h) (2012) (defining minimization procedures as procedures "reasonably designed in light of the purpose and technique" of the information collection "to minimize the acquisition and retention, and prohibit the dissemination," of private information). Minimization is statutorily required in multiple contexts. *See also* 18 U.S.C. § 2518(5) (2012) (criminal wiretaps); 50 U.S.C. § 1801(h) (electronic communications for foreign intelligence purposes); 50 U.S.C. § 1821(4) (2012) (physical searches for foreign intelligence purposes); The USA Freedom Act of 2015, Pub. L. No. 114-23, § 104(a)(3)(A), 129 Stat. 268, 272 (2015) (codified at 50 U.S.C. § 1861(g)(1) (2015)) (communications metadata).

[24] Anyone who watched the HBO series *The Wire* is already familiar with basic minimization procedures. When monitoring the communications of the Barksdale drug organization, members of the Major Crimes Unit listened to and recorded all conversations related to the illicit drug trade. But upon hearing a conversation with a clearly non-criminal purpose—someone making plans to attend church services with family members, for example—the police stopped recording. That is minimization. Since a wiretap warrant only authorizes law enforcement to collect communications that constitute evidence of a crime, refraining from recording non-crime-related communications minimizes (or prevents) collection of material beyond the scope of the warrant. *See The Wire: The Wire*, Season 1, Episode 6 (HBO television broadcast July 7, 2002). For a discussion of other forms of minimization, see Section II.B.

[25] *See infra* Section II.B.2. (discussing examples of the FISA Court's minimization procedures).

[26] 50 U.S.C. § 1803(a) (2012) (establishing an Article III court to review and approve government applications for authorization to conduct electronic surveillance for foreign intelligence purposes inside the United States).

for surveillance authority should be approved.[27] Since 9/11, however, the intelligence community's ever-expanding surveillance powers have driven a correspondingly expanded role for the FISA Court. As the scope of government authority grew, so too did the means by which the FISA Court sought to constrain that authority within constitutional and statutory limits.[28] The result was the development of a collection of minimization procedures now available for magistrates to tap.

Magistrates' characterization of *ex ante* warrant limitations as "minimization procedures" would be more than a simple semantic shift. As an initial matter, it would help to refute the contention that engaging in the practice is beyond the scope of magistrate judges' competence. Individual judges have always played a critical role in devising and overseeing the implementation of minimization procedures.[29] Recognizing that these magistrates are merely continuing to perform this function will therefore recast their actions as a new instantiation of a recognized, legitimate judicial role, rather than a new, potentially illegitimate practice. In addition, once magistrates envision *ex ante* rules for digital searches as minimization procedures, they can draw on the FISA Court's creative minimization jurisprudence. The FISA Court's opinions and orders include a rich variety of forms that minimization can take.[30] In addition, they demonstrate that minimization procedures can serve as effective, flexible tools with which to safeguard constitutional rights that are threatened by advances in the government's technological capabilities.[31] In short, they form part of the solution to the digital-search puzzle, and should be recognized as such.

This Article will proceed as follows: Part I will set out in more detail the particular Fourth Amendment difficulty arising from searches of electronically stored information. Part II will first explain minimization procedures' *raison d'être*: to safeguard individual rights when an information-collection technique risks mingling responsive and non-responsive information. It will then describe some of the innovative ways in which the FISA Court has used minimization procedures in pursuit of this goal. Finally, Part III will begin by offering insights

---

[27] *See infra* Section II.B.2.

[28] *Id.*

[29] *See infra* notes 106–109 and accompanying text. Usually, these judges are enforcing statutory requirements to minimize, but the FISA Court has also imposed minimization procedures in contexts where there was no such mandate. *See infra* notes 158–163 and accompanying text.

[30] *See infra* Section II.B.2.

[31] *See generally* Emily Berman, *Quasi-Constitutional Protections and Government Surveillance*, 2016 BYU L. REV. 771 (discussing in detail the array of minimization procedures employed by the FISA Court); Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577 (2017) (same).

into what the idea of minimization has to offer traditional courts facing the challenges inherent in authorizing electronic searches and then will go on to rebut existing critiques of the practice on both normative and doctrinal grounds.

I. DIGITAL SEARCHES AND THE FOURTH AMENDMENT

This Part will limn the contours of the Fourth Amendment dilemma that searches of digital storage presents. It will begin in section A by detailing the ways in which digital searches challenge existing Fourth Amendment doctrine. Section B will then explain how a few magistrate judges sought to address this challenge.

A. Digital Searches and the Fourth Amendment

This dilemma arises because the nature of digital evidence requires investigators to seize entire storage devices and search them for evidence later—a practice that poses significant threats to privacy—rather than seizing only evidence of criminality from the outset. Two differences between digital and analog evidence necessitate this "seize first, search later" approach. First, evidence of criminal activity will inevitably be mingled with irrelevant data. And due to the sheer size of digital devices' storage capacity, the volume of irrelevant data on any given device will be significant.[32] This means that any digital storage medium seized because it contains evidence of criminality will also include vast amounts of innocent, potentially intimate data, raising serious privacy concerns. A search of a cell phone's text messages might reveal not only communications between co-conspirators but also private text messages unrelated to the crime. The same is true of other forms of data as well, such as Internet search histories that reveal queries about health symptoms, addiction treatment, or family planning options.[33] Indeed, according to the Supreme Court, "a cell phone search would typically expose to the government far more than the most exhaustive search of a house."[34] And if the digital evidence at issue is a hard drive that stores information about multiple individuals—an accountant's records, a Gmail server, or a drug testing lab's files—then the privacy of "countless individuals

---

[32] *See* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 3 (2015) [Kerr, *Executing Warrants for Digital Evidence*] ("[A] law enforcement search for digital evidence requires searching for a needle in an enormous electronic haystack.").

[33] Riley v. California, 134 S. Ct. 2473, 2490 (2014).

[34] *Id.* at 2491 (italics omitted).

not implicated in any criminal activity, who might not even know that the information about them has been seized" is also at risk.[35]

Second, digital evidence differs from other forms of evidence because its nature as contraband is not always immediately evident. This complicates efforts to segregate digital evidence from non-responsive information. Data on digital storage devices "may be concealed, compressed, erased or booby-trapped" in ways that make it impossible to discover without accessing large numbers of non-responsive files.[36] And while criminals might seek to hide physical evidence as well—for example by stashing illicit drugs in containers with innocuous labels, such as "Sally's Legos"—there are only so many places such evidence can be hidden. Law enforcement may not, as the saying goes, look inside a matchbox if they are authorized to seize an elephant.[37] When it comes to digital evidence, contraband is more difficult to identify using only a cursory search.

These differences mean that it is not feasible to require law enforcement to sift through all of that information for responsive data at the time of the initial search and seize only responsive information at the point of collection[38]—as Rule 41 acknowledges, "over-seizing is an inherent part" of digital evidence collection.[39] Moreover, large volumes of information on each digital device means that the over-collection will be significant, raising significant privacy concerns.[40] Yet to ensure effective searches, the government must be authorized to engage in this over-seizure at the outset and then examine the seized devices' contents later, usually at a law enforcement facility and often through advanced forensic methods performed by a computer specialist.[41]

---

[35] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010).

[36] *See, e.g.*, *id.* at 1170–71; United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) ("Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled 'flour' . . . .").

[37] *See* Wilkerson v. State, 594 A.2d 597, 605 n.3 (Md. Ct. Spec. App. 1991) ("The permitted scope of a search is, logically, whatever is necessary to serve the purpose of that particular search, but '[d]on't look for an elephant in a matchbox.'").

[38] *Hill*, 459 F.3d at 974–75 (endorsing the district court's reasoning that "the process of searching the files at the scene can take a long time. To be certain that the medium in question does *not* contain any seizable material, the officers would have to examine every one of what may be thousands of files on a disk—a process that could take many hours and perhaps days.").

[39] *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1177; *see also id*. at 1180 (Kozinski, J., concurring) ("Nothing any appellate court could say, however, would substitute for the sound judgment that magistrate judges must . . . exercise in striking this delicate balance.").

[40] *See, e.g.,* United States v. Schesso, 730 F.3d 1040, 1042 (9th Cir. 2013) ("Because electronic devices could contain vast quantities of intermingled information, raising the risks inherent in over-seizing data, law enforcement and judicial officers must be especially cognizant of privacy risks when drafting and executing search warrants for electronic evidence." (citation omitted)).

[41] *See* FED. R. CRIM. P. 41; Kerr, Ex Ante *Regulation*, *supra* note 21, at 1248.

While this two-step process resolves the problem regarding inability to segregate responsive information at the time of collection, it simply kicks the Fourth Amendment can down the road. Having seized an entire digital storage device, investigators will still need to decide how to segregate the needles of evidence buried in a haystack of information that is *not* responsive to the warrant—a question Rule 41 does not address. In fact, the Advisory Committee on the Rules of Criminal Procedure specifically noted that the amended Rule 41 "does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development."[42] As one magistrate judge put it, digital searches are one area where "an observable gap has arisen between the well-established rules lower courts *have* and the ones they *need*."[43]

The "plain view doctrine," which allows law enforcement to seize any evidence in plain view of any place they are lawfully permitted to be,[44] ensures that the privacy consequences of permitting a digital search without limitations are problematic. According to this doctrine, if the police have a warrant to search a home for firearms used in a robbery and see drugs sitting on a table upon entering the house, for example, those drugs may be seized as well. Imagine that officers seeking evidence of tax fraud come across email messages indicating that the suspect has enlisted a hitman to kill someone. Absent explicit restrictions, the suspect may now be charged not only with tax fraud, but also with attempted murder and solicitation. And while that example may not garner much sympathy for the suspect, who was, after all, soliciting murder, it represents a government intrusion into a private realm for which there was no probable cause and no warrant.

Moreover, the government's discovery of wholly legal conduct in the course of its search for contraband also can lead to real harm. Imagine that a high school principal is suspected of tax evasion and law enforcement obtains a warrant authorizing a search of his computer. On the computer, investigators discover emails that indicate the principal is having an extramarital affair, or that he has

---

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

43 *In re* the Search of Cellular Tels. Within Evidence Facility Drug Enf't Admin., Kan. City Dist. Office, No. 14-MJ-8017-DJW, 2014 WL 7793690, at *4 (D. Kan. Dec. 30, 2014) [hereinafter Cellular Tels.].

44 *See* Coolidge v. New Hampshire, 403 U.S. 443, 464–66 (1971) (establishing the plain view doctrine); *In re* Appeal of Application for Search Warrant, 71 A.3d 1158, 1173 (Vt. 2012) ("[W]hen law enforcement is conducting a search pursuant to a warrant, police are authorized to seize objects not listed in the warrant as long as the object is viewed from a lawful vantage point, the incriminating nature of the object is obvious, and it may be seized from a lawful right of access." (citing Horton v. California, 496 U.S. 128, 136–37 (1990))).

an enormous pornography collection. Though neither adultery nor possession of pornography is a crime, if such discoveries leak to the press or to his supervisors—or get posted on Twitter—there will likely be significant career-related ramifications for the principal. Finally, there is the simple fact that none of us wants government officials rummaging through our private photos, documents, and communications. Even if there is nothing illegal or embarrassing among them, the Fourth Amendment denies the state unfettered access to our "persons, houses, papers, and effects" to protect our privacy.[45] We should not be forced to relinquish that protection when it comes to digital material.

Federal courts of appeals have responded to the digital implications of the plain view doctrine in different ways. Some courts simply continue to apply the traditional plain view doctrine to digital searches, holding that investigators are free to collect and use any digital contraband they happen to come across while executing a valid warrant.[46] Others make a case-by-case assessment of whether a particular warrant authorized investigators to access particular files.[47] And in a concurrence, Ninth Circuit Judge Alex Kozinski advocated a more aggressive role for magistrate judges, encouraging them to "insist that the government forswear reliance on the plain view doctrine" to prevent turning "all warrants for digital data into" the reviled "general warrants," whose use by the British served as impetus for including the Fourth Amendment in the Bill of Rights.[48]

---

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

[46] *See, e.g.*, United States v. Stabile, 633 F.3d 219, 241–42 (3d Cir. 2011) (holding that the plain view doctrine applies to a computer search in which investigators accessed files not covered by the warrant after seeing incriminating file names); United States v. Williams, 592 F.3d 511, 522–23 (4th Cir. 2010) (determining that a warrant authorizing a digital search authorizes examination of every file on the target computer); United States v. Burgess, 576 F.3d 1078, 1092–94 (10th Cir. 2009) (same).

[47] *See, e.g.*, United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010) (opining that the scope of the plain view doctrine in digital searches should be allowed to develop incrementally on a case-by-case basis); United States v. Carey, 172 F.3d 1268, 1272–73 (10th Cir. 1999) (closed computer files were not in plain view even though their file names were visible). Professor Kerr also prefers to allow the law of digital searches to develop through *ex post* case-by-case review, though his views on the role of the plain view doctrine have evolved over time. He first argued that the plain view doctrine should not apply to computer searches at all, and then subsequently disavowed that approach to argue instead that courts should interpret the Fourth Amendment to impose a use restriction on non-responsive electronic data. *Compare* Kerr, *Searches and Seizures in a Digital World*, *supra* note 22, at 566–82 (arguing that the plain view doctrine simply should not apply to computer searches), *with* Kerr, *Executing Warrants for Digital Evidence*, *supra* note 32, at 17 (arguing that courts should interpret the Fourth Amendment to impose a use restriction on non-responsive data).

[48] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178 (9th Cir. 2010 (Kozinski, J., concurring); *see also* Riley v. California, 134 S. Ct. 2473, 2494 (2014); Ashcroft v. al-Kidd, 563 U.S. 731, 742 (2011) ("The Fourth Amendment was a response to the English Crown's use of general warrants, which often allowed royal officials to search and seize whatever and whomever they pleased . . . ."); *Payton v. New York,* 445 U.S. 573, 583 (1980) (describing British use of general warrants to authorize searches and seizures as "the immediate evils that prompted the framing and adoption of the Fourth Amendment").

B. The Magistrates' Revolt

The magistrates' "revolt" was motivated by several magistrates' perception that courts' responses to the privacy threat posed by digital searches was inadequate. The revolt was to prevent government officials from accessing large amounts of non-responsive data in the second step of Rule 41's two-step procedure that prompted some magistrate judges to take matters into their own hands.[49] Some began to include constraints on how the government could execute digital searches in the warrants that they issued. These limits took a variety of forms. First are limits on the seizure of the hardware itself, with some judges insisting that the government justify why it needed, for example, to seize multiple computers in a home rather than only the suspect's office computer.[50] The magistrate would then authorize the seizure of only those devices whose collection the government could justify. A second set of limits applied to the actual search of the hardware once it had been seized. These include time limits, giving investigators a deadline by which the search must be completed;[51] requiring the government to return or destroy records that fell outside the scope of the warrant;[52] and—perhaps most controversially—including within the warrant details of how the data might be searched, such as what type of search

---

[49] The revolt began in response to requests for warrants for the contents of email accounts, but the rationale was extended to warrants of electronic devices and web-based services as well. *In re* the Search of Premises Known as: Three Hotmail Email Accounts: [redacted]@hotmail.com, [redacted]@hotmail.com, [redacted]@hotmail.com Belonging to and Seized from [redacted], No. 16-MJ-8036-DJW, 2016 WL 1239916, at *5 (D. Kan. Mar. 28, 2016) [hereinafter Three Hotmail Email Accounts].

[50] *See, e.g.*, United States v. Hill, 459 F.3d 966, 975 (9th Cir. 2006) (holding that officials must get pre-approval from a magistrate to seize computers and search them at a later date).

[51] *See, e.g.*, United States v. Mutschelknaus, 592 F.3d 826, 828 (8th Cir. 2010) (describing a warrant issued by a magistrate judge that provided a sixty-day window to search a seized computer); United States v. Brunette, 76 F. Supp. 2d 30, 42 (D. Me. 1999) (search of computer must be finished within thirty days of the seizure).

[52] *See In re the Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc.*, 21 F. Supp. 3d 1, 9–10 (D.D.C. 2013) (requiring the return or destruction of data to "prevent the government from collecting and keeping indefinitely information to which it has no right"); *see also, e.g., In re the Search of Black iPhone 4*, 27 F. Supp. 3d 74, 80 (D.D.C. 2014) (insisting the "government must specify what will occur" with "data that is seized by the government and is outside the scope of the warrant"); *In re* the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 145, 155–56 (D.D.C.) [hereinafter *In re* the Search of Info. Associated with [redacted]@mac.com], *vacated by* 13 F. Supp. 3d 157, 160–64 (D.D.C. 2014) [hereinafter Stored at Premises].

protocols,[53] investigators may use.[54] Examples might include specific key word searches, file types (e.g., text files, picture files, video files), metadata, or the protocol might include more sophisticated, computer science-based methodologies.[55] Even when search protocols were not included in the warrant itself, some judges required the government to return to the magistrate for permission to move forward once it determined what type of search it needed to perform.[56] Whichever method was employed, the magistrate specified the limits in the warrant itself, thereby placing ex ante limits on how investigators carried out their search.

The magistrates were not accused of "revolting,"[57] however, until a handful of them began actually denying warrant applications in which the government failed to propose sufficient (in the magistrates' view) ex ante limits on the search.[58] Their overarching concern, laid out in a series of thoughtful opinions,

---

[53] *See Three Hotmail Email Accounts*, 2016 WL 1239916, at *2 (defining a search protocol as "a document submitted by the government explaining to the Court how it will conduct its search of an individual's [electronically stored information]"); *In re* the Search of Apple iPhone, IMEI 013888003738427, 31 F. Supp. 3d 159, 166 (D.D.C. 2014) [hereinafter Apple iPhone] (defining a search protocol as *"an explanation of the scientific methodology the government will use to separate what is permitted to be seized from what is not"*); *id.* (treating different types of searches as accessing different "regions" of an electronic device, necessitating search protocols to satisfy the Fourth Amendment's particularity requirement) .

[54] *See, e.g.*, *In re* the Search of: 3817 W. West End, First Floor, Chi., Ill., 60621, 321 F. Supp. 2d 953, 963 (N.D. Ill. 2004) (insisting that the government submit search protocols prior to executing the search). *But see In re* a Warrant for All Content and Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 399 (S.D.N.Y. 2014) [hereinafter Gmail Account] (declining to impose search protocols but acknowledging magistrates' power to do so).

[55] *See, e.g.*, *Three Hotmail Email Accounts*, 2016 WL 1239916, at *19–24 (suggesting categorical or keyword limits, specifying a search protocol, using special masters or filter teams to segregate non-responsive evidence, and imposing rules for returning or destroying non-responsive data); *In re* the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1, 7 (D.D.C. 2014).

[56] *See, e.g.*, *In re* the Search of the Premises Known as 1406 N. 2nd Ave., Iron River, Mich. 49935, No. 2:05-MJ-28, 2006 WL 709036, at *1 (W.D. Mich. Mar. 17, 2006) (requiring government to return to the magistrate for express permission to search computers after they had been seized).

[57] The term "magistrates' revolt" was first coined in the media and later embraced by at least one of the magistrate judges who participated. *See supra* note 16.

[58] In re *the Search of Info. Associated with [redacted]@mac.com*, 25 F. Supp. 3d at 8; *In re* Applications for Search Warrants for Info. Associated with Target Email Address, Nos. 12-MJ-8119-DJW, 12-MJ-8191-DJW, 2012 WL 4383917, at *6 (D. Kan. Sept. 21, 2012) [hereinafter Email Search Warrants I]. Before actually denying any warrants, at least one magistrate repeatedly asked the government to submit more limited warrant applications and modified several of those applications. *See Apple iPhone,* 31 F. Supp. 3d at 169; *In re* [redacted]@gmail.com, 62 F. Supp. 3d 1100, 1101, 1104–5 (N.D. Cal. 2014); *In re the Search of Info. Associated with [redacted]@mac.com*, 25 F. Supp. 3d at 9 ("By the Court's count, it modified approximately twenty search and seizure warrants for electronic information in September and December 2013. It will no longer do so. Instead, any warrants that do not comport with the requirement of the Fourth Amendment will—like the present Application—be denied . . . ."). *But see Gmail Account,* 33 F. Supp. 3d at 401 (rejecting requirement that warrants for electronic searches require detailed *ex ante* limitations).

was the Fourth Amendment's requirement that "searches deemed necessary should be as limited as possible."[59] The requirements that warrants be based on probable cause and identify the places to be searched and the things to be seized with particularity, they pointed out, are meant to eliminate "the specific evil" of the "'general warrant' abhorred by the colonists"[60] and to limit investigators' discretion.[61] In addition, they advocated "greater vigilance" when it came to searches of electronically stored information because digital devices and their "ability to store and intermingle a huge array of one's personal papers in a single place" leads to increased "risk that, given an unrestricted warrant, the government will be able to access a plethora of information which it has no constitutional foundation to view."[62] The job of a magistrate, as they saw it, was

---

[59] *Email Search Warrants I*, 2012 WL 4383917, at *5 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)); *see also, e.g.*, Maryland v. Garrison, 480 U.S. 79, 84 (1987) (holding that the particularity "requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit"); *Coolidge*, 403 U.S. at 467 (judicial oversight of search warrants is meant "to eliminate altogether searches not based on probable cause").

[60] *Email Search Warrants I*, 2012 WL 4383917, at *5 (quoting *Coolidge*, 403 U.S. at 467); *see* Riley v. California, 134 S. Ct. 2473, 2494 (2014) (pointing out that "the Fourth Amendment was the founding generation's response to the reviled 'general warrants' . . . of the colonial era," which permitted indiscriminate searches); Payton v. New York, 445 U.S. 573, 583 (1980) ("It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment.").

[61] Three Hotmail Email Accounts, No. 16-MJ-8036-DJW, 2016 WL 1239916, at *4 (D. Kan. Mar. 28, 2016); *see also, e.g.*, Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 621–22 (1989) ("An essential purpose of a warrant requirement is to protect privacy interests by assuring citizens subject to a search or seizure that such intrusions are not the random or arbitrary acts of government agents."); Delaware v. Prouse, 440 U.S. 648, 653–54 (1979) ("The essential purpose of the proscriptions in the Fourth Amendment is to impose a standard of 'reasonableness' upon the exercise of discretion by government officials . . . 'to safeguard the privacy and security of individuals against arbitrary invasions.'" (citation omitted)); *Email Search Warrants I*, 2012 WL 4383917, at *6 ("[N]othing is to be left to the discretion of the officer executing the warrant." (quoting Marron v. United States, 275 U.S. 192, 196 (1927))); Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 316–17 (2016) ("It has long been a common consensus that the Fourth Amendment guards against the evil of arbitrary government rummaging in people's lives."); M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief that Gave It Birth*, 85 N.Y.U. L. REV. 905, 921 (2010) ("[T]he mischief that gave birth to the Fourth Amendment was the oppressive general search . . . . The lesson from this mischief is that granting unlimited discretion to [government officials] inevitably leads to incursions on privacy and liberty . . . .").

[62] *Email Search Warrants I*, 2012 WL 4383917, at *7 (quoting United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (citation omitted)*;* Cellular Tels., No. 14-MJ-8017-DJW, 2014 WL 7793690, at *5 (D. Kan. Dec. 30, 2014); *see also In re the Search of Info. Associated with [redacted]@mac.com*, 25 F. Supp. 3d at 6 ("Any search of an electronic source has the potential to unearth tens or hundreds of thousands of individual documents, pictures, movies, or other constitutionally protected content." (citing United States v. Leary, 846 F.2d 592, 600 (10th Cir. 1988))).

to ensure that "the search will be carefully tailored to its justifications"[63] rather than becoming "a general, exploratory rummaging in a person's belongings."[64]

The magistrates thus began rejecting government applications for warrants when those warrants "fail[ed] to set out any limits on the government's review" of the data, "on the universe of information to be disclosed to and searched by the government," or on "the government's review of the content"[65] as well as when they viewed the limits the government did propose as inadequate.[66] The most frequent ground for denying applications was a lack of sufficiently detailed search protocols.[67] Because while the ability to copy and store "thousands or millions of documents with relative ease" means that "the potential for abuse has never been greater,"[68] search tools provide "the potential for narrowing searches so that they are more likely to find only the material within the scope of the warrant."[69] Thus, judges saw search protocols as the best available means of circumscribing digital searches and expected the government to take advantage of them. Opinions denying warrant applications often included affirmative suggestions for methods that the government could employ to address these concerns[70] as well as evidence of "exasperation" with the government for not affirmatively suggesting limits itself.[71] And while "not every

---

63 *Email Search Warrants I*, 2012 WL 4383917, at *6.

64 *Id.* at *5 (citing *Coolidge*, 403 U.S. at 467).

65 *In re* Search Warrants for Info. Associated with Target Email Address, Nos. 12-MJ-8119-DJW, 12-MJ-8191-DJW, 2012 WL 4383917, at *25 (D. Kan. Aug. 27, 2013); *id.* at *28, *30.

66 *In re* the Search of ODYS LOOX Plus Tablet, Serial No. 4707213703415, in Custody of U.S. Postal Inspection Serv., 1400 N.Y. Ave. NW, Wash., D.C., 28 F. Supp. 3d 40, 46 (D.D.C. 2014) (requiring the government to submit a search protocol "with sufficient information such that it will not be authorizing the general, exploratory rummaging in a person's belongings that the Fourth Amendment prohibits") (citation omitted); Apple iPhone, 31 F. Supp. 3d 159, 161 (D.D.C. 2014) (denying application because "the government fails to articulate how it will limit the possibility that data outside the scope of the warrant will be searched"); *In re* the Search of Premises Known as Nextel Cellular Tel. with Search Warrant [redacted] (Unknown Assigned Tel. No.) Belonging to and Seized from [redacted], No. 14-MJ-8005-DJW, 2014 WL 2898262, at *14 (D. Kan. June 26, 2014) [hereinafter Nextel Cellular] ("[T]he government must provide the court with a search methodology substantially more detailed than the one provided here.").

67 *See, e.g.*, *In re* the Search of: 3817 W. W. End, First Floor, Chi., Ill., 60621, 321 F. Supp. 2d 953, 963 (N.D. Ill. 2004) (requiring government to submit to magistrate judge for review a proposed search protocol before issuing a warrant to search the contents of a computer).

68 *Apple iPhone*, 31 F. Supp. 3d at 167.

69 *Id*.

70 *In re* the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1, 7–8 (D.D.C. 2014); Cellular Tels., No. 14-MJ-8017-DJW, 2014 WL 7793690, at *19–23 (D. Kan. Dec. 30, 2014) (discussing various possibilities in some detail); Email Search Warrants I, Nos. 12-MJ-8119-DJW, 12-MJ-8191-DJW, 2012 WL 4383917, at *10 (D. Kan. Sept. 21, 2012).

71 *In re* the Search of Info. Associated with [redacted]@mac.com, 13 F. Supp. 3d 145, 154 (D.D.C. 2014) (noting "exasperation that the government has, despite repeated warnings," failed to offer alternatives to its overbroad warrant applications); Three Hotmail Email Accounts, No. 16-MJ-8036-DJW, 2016 WL 1239916, at *24 (D. Kan. Mar. 28, 2016).

search is created equal and not every warrant must include search protocols to comply with the Fourth Amendment," the inclusion of a search protocol helps the court determine if the "search and seizure requested will be governed by sufficient boundaries."[72]

Despite their good-faith effort to solve an acknowledged tension in Fourth Amendment doctrine, magistrate judges' so-called revolt has not been universally embraced. Indeed, their demands for detailed search protocols were often overruled,[73] and no court has held that such protocols are required.[74] At the same time, some courts have expressed support for the idea of including ex ante search limits in warrants.[75] Judge Kozinski, meanwhile, was the lone voice going beyond endorsement to enumerate a set of proposed rules for judges to include in warrants to search electronic data.[76] Commentators, like courts, have split on the issue.[77]

---

[72] *Cellular Tels.*, 2014 WL 7793690, at *7.

[73] *See, e.g.*, Stored at Premises, 13 F. Supp. 3d 157, 159–60 (D.D.C. 2014) (vacating a magistrate judge's opinion requiring the government to submit to *ex ante* limits).

[74] *E.g.*, United States v. Russian, 848 F.3d 1239, 1245 (10th Cir. 2017) (requiring only that warrants for computer searches include some limiting principle (quoting United States v. Christie, 717 F.3d 1156, 1165 (10th Cir. 2013)); United States v. Galpin, 720 F.3d 436, 451 (2d Cir. 2013) ("[W]e do not impose any rigid requirements [that warrants include specific search protocols] at this juncture."); *Stored at Premises*, 13 F. Supp. 3d at 157; *see also* Kerr, Ex Ante *Regulation*, *supra* note 21, at 1277–81.

[75] *E.g.*, United States v. Cartier, 543 F.3d 442, 447–48 (8th Cir. 2008) ("[T]here may be times that a search methodology or strategy may be useful or necessary."); United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) (noting that the absence of search protocols is not "fatal" to a warrant, but that the court "look[s] favorably upon" their inclusion); *United States v. Garcia-Alvarez*, No. 14-cr-0621 JM, 2015 WL 777411, at *5 (S.D. Cal. Feb. 24, 2015) (observing that "it may have been better if the warrant had included a search protocol that minimized unnecessary intrusion"); *In re* Appeal of Application for Search Warrant, 71 A.3d 1158, 1170 (Vt. 2012) (holding that *ex ante* limits on warrant executions are not required, but are "sometimes acceptable mechanisms for ensuring the particularity of a search").

[76] United States. v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178–80 (9th Cir. 2010) (Kozinski, J., concurring) (stating that judges issuing such warrants should "insist that the government forswear reliance on the plain view doctrine," so that just because investigators come across data on a computer while executing a valid warrant, that data cannot itself be seized; "the magistrate judge should order that the seizable and non-seizable data be separated by an independent third party under the supervision of the court," such as a computer specialist; the methods the government uses to search for responsive information "must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents," and to the extent there remains a risk that agents involved in the investigation might examine or retain "any data other than that for which probable cause is shown," the warrant should include "a protocol for preventing" that from happening; absent judicial authorization to the contrary, the government must destroy or return non-responsive data).

[77] *Compare, e.g.*, Kerr, Ex Ante *Regulation*, *supra* note 21, at 1246 (arguing that *ex ante* warrant restrictions are "unauthorized and unwise"), *with, e.g.*, Ohm, *supra* note 18, at 11–12 (arguing that *ex ante* warrant restrictions are necessary to prevent government overreaching), *and* Kerr, Ex Ante *Regulation*, *supra* note 21, at 1245 n.14 (listing articles that, contrary to his view, favor restrictions).

The contention of this Article is that what has been labeled a "magistrates' revolt" was actually no such thing. Instead, magistrate judges simply turned to a time-honored means of addressing privacy threats posed by broad collection authority: minimization.[78] The history of minimization procedures—and particularly the FISA Court's implementation of them—reveals not only that they provide an excellent means of constraining digital searches but also that what some magistrates have been doing—and have been criticized or overruled for—is simply borrowing the tool that Congress has statutorily demanded the FISA Court use for decades. This Article therefore turns now to a discussion of minimization itself.

II. MINIMIZATION PROCEDURES: CONGRESS'S RESPONSE TO INEVITABLE OVER-COLLECTION

While not a product of the digital age, the idea of minimization was nonetheless invented to address the very same concern raised by digital searches: how to prevent privacy intrusions when the government executes a warrant that will inevitably collect information beyond the scope of the authorized seizure.[79] This Part first traces, in section A, minimization's development from a judicially required element of Congress's criminal wiretapping statute to its prominent role in the implementation of FISA.[80] Section B then documents how minimization has been employed in practice.[81] As this discussion will demonstrate, minimization procedures have played a relatively minor role in the regulation of criminal investigations, but the FISA Court's use of them has been both innovative and effective.

---

[78] At least two magistrate judges explicitly recognized that what they were doing was minimization. *See In re* the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1, 5 (D.D.C. 2014); Gmail Account, 33 F. Supp. 3d 386, 396 (S.D.N.Y. 2014) (describing as "minimization procedures" privacy protections required in *In re the Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc.*, 21 F. Supp. 3d 1, 9–10 (D.D.C. 2013)).

[79] *See* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1647 (2010) (explaining that in each context that it applies, the role of minimization is "to protect against the acquisition[, retention, and dissemination] of private information unrelated to the purpose of the criminal investigation").

[80] 50 U.S.C. §§ 1801–1813 (2012).

[81] For a more detailed discussion of the origin and evolution of minimization procedures, particularly in the foreign intelligence context, see generally Berman, *Quasi-Constitutional Protections*, *supra* note 31, from which much of the discussion in this part is drawn.

A. The Origins of Minimization Procedures

By the mid-twentieth century, a technological advancement in fighting crime—wiretaps—had become "indispensable" to effective law enforcement, particularly against organized crime.[82] The technique's novelty, however, meant that legal principles governing its use were initially unclear.[83] The Supreme Court stepped in to lay down some rules of the road in two 1967 cases. First, in *Berger v. New York*, the Court struck down New York State's wiretapping law as unconstitutional because it permitted collection that was too indiscriminate.[84] The problem, according to the Court, was that New York's law permitted wiretaps that could capture not only a suspect's communications, but also "the conversations of any and all persons coming into the area covered by the device . . . without regard to their connection with the crime under investigation."[85] *Berger* then "laid out guidelines for the Congress and State legislatures to follow in enacting wiretapping and electronic eavesdropping statutes which would meet constitutional requirements."[86] *Katz v. United States* clarified that even wiretaps of public phone booths were searches subject to these same Fourth Amendment limitations.[87]

Guided by the *Berger* and *Katz* opinions, Congress drafted what would ultimately become Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), which governs the use of wiretaps in federal criminal investigations.[88] Title III, "tailored to meet the constitutional requirements imposed by" the Supreme Court,[89] contained a variety of procedural safeguards.

---

[82] S. REP. NO. 90-1097, at 11 (1968) (Title III findings); *see also* THE PRESIDENT'S COMM'N ON LAW ENF'T & THE ADMIN. OF JUST., THE CHALLENGE OF CRIME IN A FREE SOCIETY 201 (1967) (New York County's District Attorney "testified that electronic surveillance is[] 'the single most valuable weapon in law enforcement's fight against organized crime'").

[83] THE PRESIDENT'S COMM'N ON L. ENF'T & THE ADMIN. OF JUST., THE CHALLENGE OF CRIME IN A FREE SOCIETY 94 ("The state of the law in this field is so thoroughly confused that no policeman, except in States that forbid both practices totally, can be sure about what he is allowed to do."); *see also id*. at 202 (suggesting that Congress enact legislation regulating wiretapping).

[84] Berger v. New York, 388 U.S. 41, 44, 58–59 (1967).

[85] *Id.* at 59.

[86] S. REP. NO. 90-1097, at 68 (1968).

[87] 389 U.S. 347, 352 (1967).

[88] Pub. L. No. 90–351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2525 (2012)); S. REP. NO. 90-1097, at 75 ("[T]he subcommittee has used the *Berger* and *Katz* decisions as a guide in drafting title III."); *see also id*. at 28 ("This proposed legislation conforms to the constitutional standards set out in *Berger v. New York* . . . and *Katz v. United States* . . . .").

[89] S. REP. NO. 90-1097, at 224 (views of Sens. Dirksen, Hruska, Scott, Thurmond, and others); *see also*, *e.g.*, United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994) (recognizing that minimization is a necessary part of ensuring the constitutionality of surveillance); *In re* Sealed Case, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (noting that some circuit courts have held that minimization is a "constitutionally significant" element of Title III).

These of course included the traditional Fourth Amendment warrant requirements: a neutral magistrate must determine that there is probable cause to wiretap the target, and the type of evidence officials expect to collect must be identified with particularity.[90] Congress also inferred from the Supreme Court's jurisprudence, however, the need for an additional procedural protection: minimization.[91] Specifically, Title III requires that every wiretap order "shall contain a provision that the authorization to intercept shall be . . . conducted in such a way as to *minimize* the interception of communications not otherwise subject to interception."[92]

In practice, this requires government investigators to take steps to screen out conversations that are not pertinent to the investigation. The most straightforward way to do so is to monitor the wiretap constantly and record only those conversations whose collection is authorized.[93] So when the target of the investigation is on the phone with his co-conspirators, that conversation should be recorded, but when the same facility is used for unrelated conversations, authorities should decline to collect those communications. There are other methods as well, such as recording only during the hours of the day when the target is likely to be discussing criminal activity, or recording all conversations and then deleting those that turn out to be non-pertinent.[94]

Ten years after Title III was enacted, when Congress again considered the regulation of electronic surveillance—this time in the context of foreign

---

[90] *See* Dalia v. United States, 441 U.S. 238, 255 (1979).

[91] *See* Bynum v. United States, 423 U.S. 952, 952 (1975) (Brennan, J., dissenting from the denial of certiorari) (citing S. REP. NO. 90-1097, at 68); *see also id.* ("Together [the provisions of Title III] are intended to meet the test of the Constitution that electronic surveillance techniques be used only under the most precise and discriminate circumstances."); Scott v. United States, 425 U.S. 917, 917 (1976) (Brennan, J., dissenting from the denial of certiorari) (quoting *Bynum*, 423 U.S. at 952).

[92] 18 U.S.C. § 2518(5) (2012) (emphasis added). *Berger* requires "[l]imitations on the officer executing the eavesdrop order which would (a) prevent his searching unauthorized areas, and (b) prevent further searching once the property sought is found." S. REP. NO. 90-1097, at 74; *see also id.* at 74–75 (noting *Katz*'s observation that the surveillance at issue in that case would have been constitutionally valid had the government gotten a judicial order, at least in part because "the agents confined their surveillance to the brief periods during which petitioner used the telephone booth and took great care to overhear only the conversations of the petitioner himself").

[93] *See* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 15.4 (3d ed. 2007 & Supp. 2017) (explaining that "intrinsic minimization consists of attempting to screen out non-pertinent conversations as each conversation is taking place").

[94] *See id.* § 15.5 ("Extrinsic minimization involves limiting the time period during which monitoring is conducted."); *id.* § 15.6 (explaining that dual recorder minimization records on two devices at once—on one machine, investigators endeavor to listen only to pertinent conversations while on the other they record every conversation in full to be used only for the purpose of rebutting charges they have deleted exculpatory remarks); *id.* § 15.7 (explaining that after-the-fact minimization takes place when every conversation is recorded, but only pertinent conversations are transcribed or re-recorded and the original tapes are sealed away).

intelligence collection—legislators once again turned to minimization procedures to safeguard privacy. Like Title III, FISA[95]—which sets out the rules for the conduct of electronic surveillance inside the United States for foreign intelligence purposes—includes procedural safeguards, such as minimization procedures,[96] that reflect Congress's understanding of what protections were necessary to render FISA constitutional.[97]

FISA minimization procedures were more expansive, however, than those included in Title III.[98] Like searches of electronically stored information, foreign intelligence collection is also difficult to limit meaningfully at the collection stage. As Congress and the courts pointed out, "it may not be possible to avoid acquiring all conversations" from a targeted phone line, rather than only those relevant to the court order.[99] The intercepted communications will sometimes be in code or in a foreign language for which there is no translator present,[100] and sometimes the complexity of the investigation will make it difficult at the moment of collection to discern the foreign intelligence value of any given piece

---

[95] 50 U.S.C. §§ 1801–1813 (2012).

[96] S. REP. NO. 95-701, at 39 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 4008; *see also* H.R. REP. NO. 95-1283, at 54 (1978). Then-Attorney General Griffin Bell agreed that, "the American people need the imposition of minimization standards" because there had been "too much dissemination . . . due to carelessness or without thinking." *Foreign Intelligence Surveillance Act of 1978: Hearings on S. 1566 Before the S. Subcomm. on Intelligence & the Rights of Ams. of the Select Comm. on Intelligence*, 95th Cong. 24 (1977).

[97] S. REP. NO. 95-701, at 13, *as reprinted in* 1978 U.S.C.C.A.N. at 3982 (The legislation "embodies a legislative judgment that court orders and other procedural safeguards are necessary to insure that electronic surveillance by the U.S. Government within this country conforms to the fundamental principles of the [F]ourth [A]mendment."); *see, e.g.*, United States v. Duggan, 743 F.2d 59, 73 (2d Cir. 1984) ("FISA reflects both Congress's 'legislative judgment' that the court orders and other procedural safeguards laid out in [FISA] 'are necessary to insure that electronic surveillance . . . conforms to the fundamental principles of the [F]ourth [A]mendment.'"), *superseded by* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 271 (2001), *as recognized in* United States v. Abu-Jihaad, 630 F.3d 102, 119–20 (2d Cir. 2010); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 220 (2015) ("FISA was Congress's express decision to curb executive power as a constitutional matter."). This understanding came, at least in part, from a 1972 Supreme Court decision rejecting the executive branch's long-term practice of warrantless wiretapping, which held that the Constitution did not permit electronic surveillance of domestic security threats absent *ex ante* judicial approval. *See also* United States v. U.S. D. for E.D. Mich., 407 U.S. 297, 320–23 (1972) (citing Camara v. Mun. Ct., 387 U.S. 523, 534–35 (1967)) [hereinafter Keith].

[98] *Keith* recognized that the procedural safeguards necessary for the conduct of foreign intelligence need not be identical to those used for criminal investigations. *Keith*, 407 U.S. at 322 ("We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.' . . . Given these potential distinctions[,] . . . Congress may wish to consider protective standards for [intelligence surveillance] which differ from those" in Title III).

[99] S. REP. NO. 95-604, at 38 (1977).

[100] *In re* Sealed Case, 310 F.3d 717, 740–41 (FISA Ct. Rev. 2002).

of information.[101] As a result, FISA's minimization requirements applied not only to the *collection* of electronic communications, but also to the *retention* and *dissemination* of that information.[102] In other words, recognizing the inevitability of collecting communications entirely unrelated to the FISA-approved investigation, Congress determined that minimization must also limit how the government may use the information it collects.[103] Thus FISA minimization procedures are defined as "specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination" of private information about Americans.[104] When subsequent statutes further expanded foreign intelligence collection, those statutes also required all three forms of minimization.[105]

In both Title III and FISA, Congress entrusted the judge issuing a warrant or surveillance order with determining what minimization requires in any given instance. Congress envisioned a strong and continuing role for judges in overseeing both the procedures themselves and the government's compliance with them. Under Title III, judges may insist that the government provide periodic reports updating the judge on "what progress has been made toward achievement of the authorized objective."[106] FISA is even clearer on this point, authorizing the judge, at any time, to "assess compliance with the minimization procedures by reviewing the circumstances under which information . . . was

---

[101] *Id.*

[102] 50 U.S.C. § 1801(h) (2012) (providing that minimization procedures must be "reasonably designed in light of the purpose and technique of the particular surveillance [or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons"); *see also* DAVID S. KRIS & DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 9:1.50 (2016) (explaining that minimization procedures "require the government to 'minimize' the amount of irrelevant information that it acquires, retains, and disseminates"). The definition of minimization requirements for electronic surveillance are codified at 50 U.S.C. § 1801(h) (2012); for physical searches at 50 U.S.C. § 1821(4) (2012); and for access to tangible things at 50 U.S.C. § 1861(g)(1) (2012). All of these provisions direct the Attorney General to promulgate detailed minimization procedures. 50 U.S.C. §§ 1801(h), 1821(4), 1861(g)(1).

[103] S. REP. NO. 95-701, at 17 (1978) (arguing that FISA would "provide adequate protection for Americans" by "strengthen[ing] the 'minimization' requirements to limit strictly the dissemination of information about U.S. persons"); *see also Foreign Intelligence Surveillance Act of 1978: Hearings on S. 1566 Before the S. Subcomm. on Intelligence & the Rights of Ams. of the Select Comm. on Intelligence*, 95th Cong. 220 (1977) ("[M]inimization procedures are a vital part of the bill because they regulate the acquisition, retention, and most importantly, the dissemination of information about U.S. persons" "inadvertently swept up" by FISA.).

[104] 50 U.S.C. § 1801(h)(1).

[105] *See infra* Section II.B.2.

[106] 18 U.S.C. § 2518(6) (2012).

acquired, retained, or disseminated."[107] Moreover, a FISA judge "has the discretionary power to modify the order sought, such as with regard to . . . the minimization procedures," must "monitor compliance with the minimization procedures" it imposes, and may treat non-compliance with the minimization procedures as contempt of court.[108] Congress clearly determined that courts are the institutions best suited to assess minimization needs and to oversee their implementation.[109]

B. The Implementation of Minimization Procedures

This section will explore the various ways in which judges have employed minimization procedures to address privacy concerns, first in the traditional criminal context and then in various forms of foreign intelligence surveillance. In practice they have played a much larger role in shaping FISA surveillance than they have in shaping criminal investigations.[110]

1. Minimization in Criminal Investigations

There are several methods that investigators may use to observe Title III's requirement that wiretaps be "conducted in such a way as to minimize the interception"[111] of non-pertinent conversations.[112] In practice, however, if Supreme Court cases are any indication, the directive to minimize criminal wiretaps is often more honored in the breach. In *Scott v. United States*, the Supreme Court held that wiretapping does not necessarily violate Title III or the Fourth Amendment even if law enforcement officers "fail to make a good-faith effort" to comply with the minimization requirement.[113] Then in *United States*

---

[107] 50 U.S.C. § 1805(d)(3) (2012).

[108] S. REP. NO. 95-604, at 47, 49 (1977).

[109] *Id*. at 48; *see also* S. REP. NO. 95-701, at 57 (1978); H.R. REP. NO. 95-1720, at 29 (1978) ("[A]t the end of the period of time for which an electronic surveillance was approved . . . the judge may assess compliance with the minimization procedures."); *see also* 125 Cong. Rec. 10900 (Apr. 20, 1978) (statement of Sen. Evan Bayh II, in support of an amendment, later adopted, clarifying the judiciary's power to oversee the implementation of minimization procedures); Helene E. Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs are Doing Their Jobs*, 12 RUTGERS L.J. 405, 439 (1981) (emphasizing the FISA Court's independent role in assessing the sufficiency of minimization procedures).

[110] Note that Congress has expanded minimization in the foreign intelligence context to apply to other forms of collection as well. 50 U.S.C. § 1822 (2012) (physical searches); 50 U.S.C. § 1842 (2012) (pen registers and trap-and-trace devices); 50 U.S.C. § 1861 (2012) (business records and other tangible things); 50 U.S.C. § 1881a (2012) (communications of non-U.S. persons outside the United States).

[111] 18 U.S.C. § 2518(5) (2012).

[112] *See supra* notes 93–94.

[113] 436 U.S. 128, 130 (1978) (instructing courts to assess whether failure to minimize was reasonable "in light of the facts and circumstances" investigators faced).

v. Kahn, the Supreme Court held that law enforcement officials need not minimize crime-related conversations even if the conversation's participants were not the individual(s) identified in the warrant as a person "whose communications are to be intercepted."[114]

In light of *Scott* and *Kahn*, the role of minimization procedures has been relatively minimal in the Title III context. Rather than imposing meaningful checks on the government's exercise of power as Congress intended, "the minimization provision plays at best a diminished role in protecting privacy of those being investigated."[115] As an example, in *Bynum v. United States*, Justice Brennan dissented from the Supreme Court's denial of certiorari to review the Second Circuit's determination that investigators met minimization requirements when they intercepted seventy-one calls by the defendant's teenage babysitter, "who was totally innocent of any knowledge of her employer's criminal enterprise."[116]

2. Minimization in Foreign Intelligence Surveillance

Edward Snowden's massive leak of intelligence information in the summer of 2013, along with documents the government declassified in response, ended the decades-long obscurity that FISA minimization procedures had enjoyed. A close look at the orders issued by the FISA Court over the past fifteen years reveals resourceful use of minimization procedures as bulwarks against threats to individual privacy rights.[117] Through creativity and assertive exercise of the oversight power both inherent in the judiciary and statutorily conferred on the FISA Court, FISA judges were able to cabin some of the broadest government information-collection authority ever exercised.

FISA minimization procedures are much more conspicuous than their Title III counterparts because they apply to retention and dissemination as well as collection.[118] Variables such as which type of intelligence collection is at issue, which agencies are involved, and the nature of the target all will impact what minimization requires. Each agency that handles foreign intelligence develops its own standard minimization procedures tailored to that agency's mission and authority.[119] In many cases, the standard procedures are sufficient, but FISA

---

114 415 U.S. 143, 152 (1974).

115 FISHMAN & MCKENNA, *supra* note 93, at § 15:8.

116 423 U.S. 952, 954 (1975) (Brennan, J., dissenting from denial of certiorari).

117 *See* Berman, *Quasi-Constitutional Protections*, *supra* note 31, at 790–817.

118 *In re* Sealed Case, 310 F.3d 717, 740 (FISA Ct. Rev. 2002).

119 *See* KRIS & WILSON, *supra note* 102, at § 9:3 ("Shortly after FISA's enactment, 'standard minimization procedures' were created for various kinds of electronic surveillances . . . ."); FBI, STANDARD MINIMIZATION

judges can—and do—sometimes tailor the procedures to address issues arising in a particular circumstance.[120]

What follows is a discussion of how minimization procedures manifest in various forms of foreign intelligence surveillance. It begins with so-called traditional FISA, the common label for the surveillance mechanism set up in the original FISA statute in 1978. It then turns to two surveillance programs authorized by the FISA Amendments Act of 2008. And finally, it examines the minimization procedures imposed on two metadata collection programs based on a provision of the USA PATRIOT Act.

a. "Traditional" FISA

Under traditional FISA surveillance of electronic communications—i.e., FISA as it was enacted in 1978—minimization tends to take place at the retention and dissemination stage, as Congress anticipated.[121] Retention minimization happens after the information is reduced to an "intelligible form" by decoding, translating, or otherwise rendering collected information readable.[122] If "the information seized is or might be foreign intelligence information," the reviewing agent will log that information "into the FBI's records and [file it] in a variety of storage systems from which it can be retrieved for analysis."[123] If, on the other hand, she finds that the information "*could not be* foreign intelligence information or are not evidence of a crime," she will minimize by discarding, erasing, destroying, or (more often) not including the information in the indexing log.[124] As for dissemination, the agency in

PROCEDURES FOR FBI ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH CONDUCTED UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 4 (2008) (setting out the FBI's standard minimization procedures). FISA requires the Attorney General to promulgate "specific procedures" for minimization that will be filed with the FISA Court for every individual target. 50 U.S.C. § 1801(h)(1).

120 Schwartz, *supra* note 109, at 416 (citing interviews with executive branch officials); Banks, *supra* note 79, at 1659–60 ("[T]he court may modify the procedures and order that the modified procedures be followed if it finds that the [government's] proposed procedures do not satisfy the FISA definition."); KRIS & WILSON, *supra* note 102, at § 9:3.

121 Note that FISA authorizes electronic surveillance, physical searches, the collection of tangible things, and the collection of data from pen registers and trap-and-trace devices. With minimal exceptions, minimization is defined in the same way for each of these forms of collection. 50 U.S.C. §§ 1801(h), 1805, 1881a (2012). Unlike the provisions governing electronic surveillance and physical searches, the definition of the minimization of tangible things does not include collection minimization at all. 50 U.S.C. § 1861(g)(2) (2012).

122 *In re* All Matters Submitted to the Foreign Intelligence Surv. Ct, 218 F. Supp. 2d 611, 617–18 (FISA Ct. 2002).

123 *Id*. at 618.

124 *Id*.; Schwartz, *supra* note 109, at 411 (quoting H.R. REP. NO. 95-1283, at 56 (1978)) (Transcripts of a suspected spy's wife's "conversations might be retained for a reasonable period until it could be determined

possession of the information may disseminate it only after all U.S. persons' names and personal identifiers are redacted.[125]

b. The FISA Amendments Act: PRISM

The FISA Court has also overseen electronic surveillance under statutory provisions enacted more recently—especially sections of the USA PATRIOT Act[126] and the FISA Amendments Act (FAA).[127] FAA collection is sometimes referred to as "Section 702" collection, for the section of the FAA that codified the power. When using Section 702 authority, the National Security Agency (NSA) used the code word "PRISM" when it collected a target's electronic communications from their communications service provider.[128] By contrast, when the government acquired a target's communications by capturing the information directly from the Internet "backbone" as it transits the web, it is known as "upstream" collection.[129] It is in the context of these new programs that the FISA Court began to get creative with the use of minimization as a constitutional stop-gap.

The new type of minimization procedures that the FISA Court imposed on the PRISM program was a response to the ways in which the FAA collection authority differed from traditional FISA authority. As an initial matter, the definition of who may be targeted is much more capacious under the FAA. While traditional FISA requires probable cause that the target is an agent of a foreign power, the FAA requires only that the target is a non-U.S. person "reasonably believed to be outside the United States" and that the collection is undertaken for foreign intelligence purposes.[130] This means the bar the government must clear to engage in FAA surveillance is far lower than it had been before—it represented a significant expansion of the government's collection authority.

---

whether she too was culpable," after which, if she were uninvolved, the information would be "destroyed or reduced to an essentially non-usable form.").

125 KRIS & WILSON, *supra* note 102, at § 9:7. The statute creates an exception for this restriction when "such person's identity is necessary to understand foreign intelligence information or assess its importance" or is evidence of a crime. 50 U.S.C. §§ 1801(h)(2), 1821(4)(B); In re *All Matters*, 218 F. Supp. 2d at 618.

126 USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272–73 (2001).

127 Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, 2438 (codified at 50 U.S.C. § 1881a (2012)).

128 *E.g.*, James Bamford, *They Know Much More than You Think*, N.Y. REV. BOOKS, Aug. 15, 2013 (describing PRISM as giving the NSA access to data from individual companies).

129 *Id.* (quoting NSA slide describing upstream collection as a "collection of communications on fiber cables and infrastructure as data flows past").

130 50 U.S.C. § 1881a(g)(2).

At the same time, the FISA judge's role in choosing those overseas targets was far more circumscribed under the FAA. Traditional FISA surveillance requires a FISA judge to assess *ex ante* the validity of each surveillance target.[131] This requires the judge to determine, among other things, that there is probable cause that the target is an agent of a foreign power and that the proposed minimization procedures are sufficient.[132] In other words, as with Title III warrants, each target must be individually approved by an Article III judge. Section 702 surveillance, by contrast, allows the executive branch itself to select targets. The government must establish rules governing how targets will be selected,[133] and the FISA Court must agree that those targeting rules are sufficiently likely to identify only non-U.S. persons outside the United States.[134] Once the rules are approved, however, the FISA Court has no role in assessing the propriety of individual surveillance targets.[135] The same process applies to minimization procedures—the government must submit to the FISA Court proposed minimization procedures for its approval,[136] but the court has no role in calibrating them on a target-by-target basis.[137] Once the FISA Court approves the government's general minimization procedures, the government follows a one-size-fits-all approach that simply applies these pre-approved procedures to all Section 702 surveillance.

The FISA Court responded to this simultaneous expansion of surveillance authority and constriction of the scope of judicial review by adding new safeguards to the minimization procedures it approved. They go beyond traditional FISA practices of simply indexing only the information that might qualify as foreign intelligence and determining which communications may be disseminated under what circumstances. Section 702's PRISM minimization rules include, for example, guidelines governing what to do when an agency discovers that, contrary to statutory requirements, a target turns out to be either

---

131 50 U.S.C. § 1805(a)–(b) (2012).

132 *Id.* § 1805(a)(3)–(4).

133 *See* ERIC H. HOLDER, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2011).

134 50 U.S.C. § 1881a(i)(2). Some argue that this difference renders the regime unconstitutional. *See generally* Donohue, *supra* note 97, at 134 ("The incidental collection of large quantities of U.S. persons' international communications, the scanning of content for information 'about' non-U.S. person targets, and the interception of non-relevant and entirely domestic communications in multi-communication transactions . . . fall outside the reasonableness component of the Fourth Amendment."). A challenge to the constitutionality of the FAA was dismissed for lack of standing. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).

135 50 U.S.C. § 1881a(a) (granting the Attorney General and the Director of National Intelligence, rather than a FISA court, the authority to jointly authorize surveillance of individuals).

136 *See* ERIC H. HOLDER, *supra* note 133.

137 50 U.S.C. § 1881a(g)(2).

a U.S. person or inside the United States.[138] They include limits on who may access Section 702-acquired information and what records of that access the government must maintain.[139] They impose requirements for tagging stored information as FAA-acquired and removing identifying information for U.S. persons from that information.[140] They place limits on the use of "sensitive information"—defined as information consisting of religious academic, political, or highly personal activities as well as medical information and information about minors[141]—and instruct the government how to handle information that falls within the attorney-client privilege or provides evidence of a crime.[142] This non-exhaustive list gives a sense of the nature of the minimization required. Thus recognizing that the more permissive collection rules that governed PRISM collection risked more over-collection than traditional FISA, and lacking the ability to oversee each decision regarding who to target, the FISA Court enlisted a more fulsome regulatory regime regarding the use and dissemination of PRISM information to account for Americans' privacy interests.

c. The FISA Amendments Act: "Upstream" Collection

The FISA Court's oversight of Section 702 upstream collection provides an even more vivid example of minimization's potential. Due to technological constraints related to how information transits the Internet, Section 702 upstream collection of electronic communications directly from the Internet backbone was necessarily overbroad.[143] It was inescapable that upstream collection was capturing some unpredictable—though not negligible—number of entirely

---

[138] *E.g.*, LORETTA E. LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 4 (2016).

[139] *E.g.*, *id.* at 6–8.

[140] *E.g.*, *id.* at 9.

[141] *E.g.*, *id.* at 10.

[142] *Id.* at 12–13.

[143] PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., EXEC. OFFICE OF THE PRESIDENT, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FISA 6 (2014) [hereinafter PCLOB SECTION 702 REPORT] (noting that collection could not be limited to communications to and/or from a specific target but would also capture any communications "concerning" the target); *id.* at 39 (explaining that information moves across the Internet in the form of "transactions," which are bundles of data, and some—known as multiple-communications transactions (MCTs)—contain within them multiple discrete communications); [REDACTED], No. PR/TT [REDACTED], at 31 (FISA Ct. Oct. 3, 2011) (explaining that the NSA's upstream Internet collection devices cannot distinguish MCTs from transactions containing only a single discrete communication). Nor can the NSA "identify the parties to any particular communication within a transaction" prior to collection. *Id*. at 43. The NSA discontinued "about" collection in April 2017. Charlie Savage, *N.S.A Halts Collection of Americans' Emails About Foreign Targets*, N.Y. TIMES (Apr. 28, 2017), https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html.

domestic communications unrelated to any surveillance target.[144] Personal communications of U.S. persons who were not valid targets were inevitably being acquired in the process.

To satisfy itself that upstream's inevitable over-collection was constitutional, the FISA Court once again relied upon an expanded menu of minimization procedures, specifically at the retention stage. In a 2011 opinion, the FISA Court determined that—despite its overbroad nature—upstream *collection* did not require additional minimization rules because it was already as narrowly targeted as technology permitted.[145] But because that targeting could only be so narrow, it was all the more important for the NSA's *retention* minimization to adequately minimize information "not relevant to the authorized purpose of the acquisition"—i.e., wholly domestic communications.[146] In this, the FISA Court found, the upstream retention procedures were insufficient.

The FISA judge's means of addressing this concern demonstrates one method by which the government and a judge with ongoing oversight authority can craft case-specific ways to limit privacy intrusions in even in the most technologically complex collection contexts. The FISA judge suggested and the government adopted a series of additional retention minimization procedures that were tailored specifically to challenges posed by upstream collection. These additional procedures restricted access to databases most likely to contain wholly domestic communications; required domestic communications to be purged from the system when identified as such; provided that information collected through the upstream program would be permanently tagged with that status in government databases, alerting users to the fact that the data is particularly sensitive; and limited retention of upstream-acquired information to two years, rather than the PRISM standard of five years.[147] In light of these additional safeguards, the Court subsequently determined that the program was statutorily and constitutionally sound.[148]

---

144 [REDACTED], No. PR/TT [REDACTED], at 32–36 (FISA Ct. Oct. 3, 2011); PCLOB SECTION 702 REPORT, *supra* note 143, at 121 ("[N]o one knows how many wholly domestic communications the NSA may be acquiring each year.").

145 [REDACTED], No. PR/TT [REDACTED], at 47–48 (FISA Ct. Oct. 3, 2011).

146 *Id.* at 59–61, 78 (NSA's minimization procedures enhanced "the risk of error, overretention, and dissemination of non-target information, including information protected by the Fourth Amendment").

147 [REDACTED], No. PR/TT [REDACTED], at 7–11 (FISA Ct. Nov. 30, 2011).

148 *Id.* at 14.

d. Metadata Collection

Two communications metadata collection programs—one that collected Internet metadata and another that collected telephony metadata—provide the most dramatic example of minimization's ability to compensate for overbroad collection.[149] The first program used an expansive interpretation of FISA's provision authorizing the use of a pen register or trap-and-trace device (pen/trap) to acquire Internet metadata about Americans' electronic communications, such as email routing and addressing information.[150] The second program used a similarly aggressive interpretation of Section 215 of the USA PATRIOT Act,[151] to collect all domestic and international telephony metadata—information such as telephone numbers dialed and the date, time, and duration of the call.[152] These programs had no targeting rules at all. Instead, the NSA collected *everyone's* data and then queried the resulting databases using phone numbers or email addresses associated with known terrorists in an effort to determine who might be in contact with them.[153]

The FISA Court acknowledged that its approval of these programs permitted the government to engage in an "exceptionally broad form of collection" in which "only a very small percentage" of the information collected would be "directly relevant" to an investigation.[154] Such over-collection was necessary because, according to the FISA Court, "the subset of terrorist communications is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried . . . [so] the whole production is relevant to the ongoing investigation out of necessity."[155]

---

[149] Both programs have been discontinued. Brian Bennett, *The NSA Will Stop Collecting U.S. Phone Data. Now What?*, L.A. TIMES (June 3, 2015), http://www.latimes.com/nation/nationnow/la-na-nsa-phone-data-20150603-story.html; PCLOB SECTION 702 REPORT, *supra* note 143, at 38; OFFS. OF INSPECTORS GEN'L OF THE DEP'T OF DEF., DEP'T OF JUSTICE, CIA, NAT'L SECURITY AGENCY & OFFICE OF THE DIR. OF NAT'L INTEL., UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 29 (July 10, 2009). *But see* Charlie Savage, N.Y. TIMES, *File Says N.S.A. Found Way to Replace Email Program* (Nov. 19, 2015), https://www.nytimes.com/2015/11/20/us/politics/records-show-email-analysis-continued-after-nsa-program-ended.html (reporting that the NSA found a "functional equivalent" for the program overseas).

[150] Pen registers record outgoing communication information, such as the numbers called from a particular phone; trap-and-trace devices record information about incoming communications. *See* 50 U.S.C. § 1842 (2012) (foreign intelligence investigations); 18 U.S.C. § 3127 (2012) (criminal investigations).

[151] *See In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-109, at 9 (FISA Ct. Aug. 29, 2013).

[152] *Id.* at 2 n.2.

[153] PCLOB SECTION 702 REPORT, *supra* note 143, at 41, 48.

[154] [REDACTED], No. PR/TT [REDACTED], at 23, 48 (FISA Ct. July 14, 2004) [hereinafter FISC's Pen/Trap Opinion].

[155] *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-109, at 22 (FISA Ct. Aug. 29, 2013).

Recognizing that the "raw volume of the proposed collection is enormous" and that the programs authorized the government to acquire "[metadata] pertaining to communications of U.S. persons located within the United States who are not the subject of any FBI investigation,"[156] the Court concluded that the program "carries with it a heightened risk that collected information could be subject to various forms of misuse."[157] Due to the enormity of the inevitable over-collection, the FISA Court in this context relied again on program-specific minimization procedures to limit the impact on Americans' privacy.

For our purposes, it is important to note that the FISA Court determined that the Fourth Amendment did not apply to the collection in either of these programs, and only the telephony metadata collection had statutory minimization requirements.[158] Nevertheless, because the programs represented "an extraordinarily broad implementation of a type of surveillance that Congress has regulated by statute, even in its conventional, more narrowly targeted form,"[159] the Court deemed strict procedural protections necessary even where no statutory or constitutional mandate existed.[160] When Congress enacted the USA FREEDOM Act of 2015, the culmination of the public debate sparked by Edward Snowden's 2013 leak, it endorsed the FISA Court's actions in this regard.[161] The primary purpose of the legislation was to strengthen privacy rights in the context of metadata collection. To accomplish this goal, Congress codified both the majority of the minimization procedures, described below, that the

---

156 *Id.* at 39 (quoting government application).

157 *Id.* at 68.

158 Because both programs collected only metadata, the government and the FISA Court deemed the Fourth Amendment inapplicable based on the third party doctrine, which states that the Fourth Amendment does not regulate government collection of information you have voluntarily provided to a third party, such as your phone records. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (no Fourth Amendment protection for phone call metadata); United States v. Miller, 425 U.S. 435, 443 (1976) (no Fourth Amendment protection for bank records). Section 215 did include a statutory mandate to minimize. But since minimization procedures need only be "reasonably designed in light of the purpose and technique" of collection under 50 U.S.C. § 1861(g), it is likely that minimization procedures for non-content, non-Fourth Amendment-protected information like telephony metadata need not be particularly stringent.

159 *FISC's Pen/Trap Opinion*, at 69, 80–87 (FISA Ct. July 14, 2004).

160 Unlike upstream collection of communications content under Section 702 of the FAA and some business records orders issued under Section 215, pen/trap devices will never collect anything other than communications metadata—i.e., non-content information that is unprotected by the Fourth Amendment. *See supra* text accompanying note 158 (explaining third party doctrine). This likely explains the lack of minimization requirement in this provision at the time.

161 USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 104(a)(3), 129 Stat. 268, 272 (2015) (to be codified at 50 U.S.C. 1861(c)(1)).

FISA judges had insisted upon[162] and the FISA Court's conclusion that all communications metadata collection must be subject to minimization.[163]

The restrictions the FISA Court imposed on the metadata collection programs were both procedural and substantive.[164] Many of the procedural protections resembled those previously imposed on Section 702-acquired data: access to the metadata databases was limited to authorized analysts by requiring a user name and password, records of which would be maintained for auditing purposes;[165] all queries of the databases containing the information collected under these programs had to be approved by one of a limited number of senior officials;[166] and that information would only be available for a limited time.[167] The order also included a ninety-day limit on the length of the authorized surveillance.[168] When applying for reauthorization at the end of each ninety-day period, the FISA Court required the government to include a report discussing the queries that had been made since the previous application and describing any proposed changes.[169]

Other minimization rules were substantive and entirely novel: First, the Court imposed a Reasonable Articulable Suspicion (RAS) standard on database queries, which required the government to conclude prior to running a query regarding any specific search term that, "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known [redacted—probably email or IP address] is associated with [redacted—probably international terrorist organization or Al Qaeda]."[170] This requirement served to limit government access to Internet or communications metadata to individuals about whom the government had individualized reasons to suspect involvement in international terrorism. Much in the way a warrant requires the government to demonstrate probable cause before engaging in a search, the RAS

---

162 *Id.* § 101(b)(3), 129 Stat. at 270 (to be codified at 50 U.S.C. § 1861(c)(2)).

163 *See id.* § 202(a), 129 Stat. at 277–78 (requiring "privacy procedures" when employing pen/trap devices) (to be codified at 50 U.S.C. § 1842(h)).

164 *E.g.*, Memorandum of Law and Fact in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes at 3, [REDACTED], No. PR/TT [REDACTED] (FISA Ct. 2004); *FISC's Pen/Trap Opinion*, at 69–70.

165 *FISC's Pen/Trap Opinion*, at 83.

166 *Id.* at 84.

167 *Id.* at 85–86.

168 *Id.* at 80.

169 *Id.* at 86–87.

170 *Id.* at 57.

standard limited the government's access to this vast trove of information to instances in which there was objective evidence that justified doing so.[171]

The FISA Court also imposed limits on the type of analysis to which the information could be subjected, and modified the minimization procedures imposed on these bulk collection programs over time to address concerns that arose in the course of their implementation.[172] Finally, unable to monitor the government's implementation of these rules on a daily basis, the FISA Court assigned that role to the NSA Office of General Counsel.[173] That office had to ensure that analysts with access to the metadata received adequate training, monitor compliance with the RAS standard, and review the legal adequacy of the basis of any query about a U.S. person's account.[174] As with the Section 702 upstream program, the court's authority to impose, modify, and oversee compliance with minimization procedures empowered it to confine the privacy risks presented by these programs whose very design included over-broad collection.

Minimization procedures can therefore serve to constrain government power in contexts where technological change has resulted in inevitable over-collection. Indeed, they can supply necessary protections even in the absence of statutory requirements. The next Part considers the implications of this lesson beyond the FISA context.

---

171 *See* Berman, *Quasi-Constitutional Protections*, *supra* note 31, at Section III.A. (arguing that the FISA Court's minimization procedures for the bulk metadata collection programs were stand-ins for the traditional warrant requirements of an *ex ante* showing of probable case and particularity).

172 After the government informed the FISA Court in 2009 of a number of instances of government non-compliance, the FISA Court imposed additional minimization requirements: the Justice Department had to review a sample of the NSA's justifications for querying data once every ninety days, twice every ninety days the NSA's Office of General Counsel (subsequently substituted with the Justice Department's National Security Division) conducted random spot checks, *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 06-05, at 8, 10 (FISA Ct. Aug. 18, 2006), and the NSA had to submit periodic reports to the FISA Court regarding the queries it had conducted and the information it had disseminated. Order Regarding Further Compliance Incidents, *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 09-13, at 3 (FISA Ct. Sept. 25, 2009); *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 09-06, at 7 (FISA Ct. June 26, 2009).

173 FISC's Pen/Trap Opinion, at 84–85 (FISA Ct. July 14, 2004); Order Regarding Further Compliance Incidents, *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 09-13, at 3 (FISA Ct. Sept. 25, 2009).

174 *FISC's Pen/Trap Opinion*, at 84.

III. MINIMIZATION PROCEDURES: MITIGATING PRIVACY CONCERNS IN DIGITAL SEARCHES

This Part makes the case that magistrate judges should employ minimization procedures to mitigate Fourth Amendment concerns in digital searches. As noted above, some magistrate judges have, in fact, been including in their warrants *ex ante* limits on the parameters of digital searches, though almost never actually referring to them as "minimization procedures."[175] Section A will explain the benefits of both adopting the minimization label and embracing the use of the tool. Section B will then address the policy-based objections to this practice and argue that *ex ante* minimization requirements are, in fact, a superior means of addressing the concerns raised by digital searches than reliance on *ex post* judicial review. Finally, section C will make the case that, despite the absence of a statutory mandate, magistrate judges do in fact have the authority to impose these requirements.

A. Minimization's Untapped Potential

Adopting the "minimization" label for magistrate judges' *ex ante* search instructions would yield several benefits. First, it would recognize that digital searches present a problem for which the law already has generated a solution. As the FISA Court's experience demonstrates, minimization procedures can address Fourth Amendment concerns that arise when a particular investigative technique risks significant over-collection.[176] Recall that the original purpose of FISA minimization was to force the government to segregate evidence that it was authorized to collect from other, Fourth Amendment-protected information.[177] The mechanism Congress and the Supreme Court settled on for this task was to expand the concept of minimization from its origins as a means of *preventing* over-collection—through wiretap-collection minimization—to address circumstances when over-collection is *unavoidable*—through retention, use, and dissemination minimization.[178]

---

[175] There are a few exceptions. *See, e.g.*, United States v. Galpin, 720 F.3d 436, 451 (2d Cir. 2013); Gmail Account, 33 F. Supp. 3d 386, 396 (S.D.N.Y. 2014); *In re* the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1, 5 (D.D.C. 2014).

[176] Note that not everyone considers FISA minimization an unparalleled success. Some argue that some of the government's surveillance programs, like Section 702 for example, are simply unconstitutional on their face. To those holding this view, minimization procedures might be seen as an effort to put a Band-Aid on a gaping wound, providing the appearance, but not the substance, of constitutional constraints. *See, e.g.*, Donohue, *supra* note 97, at 124.

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

[178] *See* Katz v. United States, 389 U.S. 347, 352 (1967); Berger v. New York, 388 U.S. 41, 44 (1967); Pub. L. No. 90–351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2522 (2012)).

Digital searches present a conceptually analogous problem to the one posed by FISA surveillance in that, as Rule 41's two-step process recognizes, it is often not possible at the point of collection to limit the seizure of digital evidence to material covered by the warrant. The challenge therefore, as with FISA surveillance, is to devise a way to limit post-collection privacy intrusions. In imposing *ex ante* limits, magistrate judges recognized how technological innovation had given rise to this same problem in a new context and simply applied to that new context a proven, accepted technique of safeguarding constitutional rights.[179] The fact that most magistrates did not consciously invoke the idea of minimization to justify *ex ante* limitations on searches does nothing to undermine the force of this argument. Whether consciously or unconsciously, these judges saw the need to impose post-collection privacy safeguards and implemented them.[180] Embracing the term "minimization" thus recasts what some have characterized as a "revolt" into merely the implementation of a long-standing, battle-tested privacy-protection tool.

Second, characterizing magistrates' practice of imposing *ex ante* limits as minimization procedures highlights the effectiveness of the practice. As discussed in Part II, FISA judges were able to develop minimization strategies that accounted for privacy concerns while still permitting the government to pursue its desired counterterrorism and counterintelligence policies, even as those policies expanded in scope. For technological reasons stemming from the nature of Internet traffic, the requirements of sophisticated data analysis, and the difficulty in pinpointing the location of particular individuals and electronic devices, several FISA surveillance programs implemented in the decade after 9/11 presented Fourth Amendment challenges.[181] The FISA Court, charged with ensuring that these programs comported with constitutional requirements, had two options. It could simply have denied the government authority to engage in the type of collection it sought despite that collection's national security value. Or it could find a way to curtail the privacy threat those programs posed. Minimization thus served to protect individual privacy rights while acknowledging the government's investigative needs. Moreover, these strategies were able to adapt as technology—and the government's surveillance programs themselves—grew and changed.

---

[179] *See, e.g.*, *supra* cases cited in notes 51–56.

[180] *See, e.g.*, United States v. Ganias, 755 F.3d 125, 140 (2d Cir. 2014), *rev'd en banc on other grounds*, 824 F.3d 199 (2d Cir. 2016).

[181] *See, e.g.*, [REDACTED], No. PR/TT [REDACTED], at 31 (FISA Ct. Oct. 3, 2011); U.S. DEP'T OF JUSTICE, THE FISA AMENDMENTS ACT: Q&A 2 (2017) (describing the impact of technological change on government surveillance authorities), https://fas.org/irp/agency/doj/fisa/faa-fact.pdf.

To be sure, minimization did not eliminate all privacy threats, and it increased the administrative burden on the government. But the Fourth Amendment does not deal in absolutes. As the Supreme Court repeatedly reminds us, the touchstone of the Fourth Amendment is reasonableness, and whether a search or seizure is reasonable ultimately rests on whether it successfully balances the government's interest against those of individuals.[182] The FISA Court's jurisprudence provides an example of how minimization empowers courts with tools they can use to calibrate this balance.

Third, pointing to the parallel between minimization and magistrates' *ex ante* requirements illustrates the critical role judges play in addressing case-specific privacy concerns. There are no particular procedures that are inherently part of "minimization" as a concept. Rather, minimization is any set of procedures "reasonably designed in light of the purpose and technique" of information collection "to minimize the acquisition and retention, and prohibit the dissemination," of information whose collection is not authorized.[183] Consider the modification of minimization rules undertaken to shore up the privacy protections of Section 702 upstream collection.[184] Those procedures were tailored very specifically to that form of collection and its unique challenges. Recognizing that it was impossible for the NSA to avoid the acquisition of some domestic U.S. person communications, the FISA judge in that case focused on how modifications to retention rules might ameliorate privacy concerns.[185] And in developing those enhanced retention rules, the judge took into account the structure of the databases containing Section 702-acquired information as well as the NSA's internal procedures for handling the raw intelligence.[186] Magistrate judges can exhibit similar flexibility in their efforts to tailor *ex ante* rules in ways that enable the government to successfully locate digital contraband without exceeding constitutional limits.

Indeed, the FISA Court's experience demonstrates how judges and the government can form an effective team for designing ways to meet the needs of both privacy and effective investigation. Recognizing the legitimacy of the judges' ongoing oversight authority encourages a partnership, rather than an

---

182 *E.g.*, Riley v. California, 134 S. Ct. 2473, 2482 (2014) ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'"); United States v. Ramirez, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis . . . governs the method of execution of the warrant.").

183 50 U.S.C. § 1801(h)(1) (2012).

184 *See supra* Section II.B.2.

185 [REDACTED], No. PR/TT [REDACTED], at 59–61, 78 (FISA Ct. Oct. 3, 2011).

186 *Id.*

adversarial relationship, between the government and the court. There were multiple FISA-related instances where the government only discovered technical limitations or systemic (though inadvertent) non-compliance due to its obligations to report back to the FISA Court periodically, which provided the court with the opportunity to adjust the applicable minimization procedures.[187] Viewing *ex ante* restrictions on digital searches as minimization procedures allows judges to assume this role and empowers them to craft, along with the government, a set of rules for each search that both protects Fourth Amendment interests and recognizes the government's investigative needs.

Fourth and finally, explicitly adopting minimization procedures as the means of regulating digital searches will draw both the government and magistrates' attention to the wealth of specific, innovative examples that the FISA Court's jurisprudence provides. Recall the broad range of requirements that the FISA Court developed to facilitate judicial oversight of surveillance programs. FISA Court orders dictated what information could be retained and under what circumstances.[188] They restricted who could access certain information and what sort of internal executive branch oversight was necessary. They required periodic reports on how orders were implemented.[189] They limited what type of analysis the government could employ on data garnered through bulk collection programs—i.e., search protocols. They imposed substantive standards that the government had to meet before accessing information it had collected. Magistrate judges imposing minimization procedures could employ some of these methods, or they might feel empowered to follow in the FISA Court's footsteps and devise their own additional context-specific measures where appropriate. They could require supervisory oversight of search procedures. They could insist that the government provide audit logs indicating exactly what kinds of analysis it performed. They could adopt traditional FISA's common means of acquisition minimization by barring investigators from documenting non-responsive material, thus making it more difficult to access in the future. The list is endless and infinitely malleable, allowing courts to adapt not only to each investigation but also as technology changes. This is a powerful tool to have available when the pace of technological change means that minimization needs will evolve over time, as both criminals and government agencies continue to exploit the latest digital tools.

---

187 *See supra* note 172 and accompanying text.

188 *See supra* Section II.B.2.

189 *See supra* Section II.B.2.d.

B. The Advantages of Ex Ante *Minimization Over* Ex Post *Judicial Review*

Despite the benefits of embracing minimization procedures in both name and substance, the government and some commentators have expressed resistance to the idea that magistrate judges should be taking on this role as a policy matter. Professor Orin Kerr argues, for example, that rather than imposing *ex ante* limits, magistrates should allow the rules regarding digital searches to develop through *ex post* judicial review.[190] This would mean that magistrates would simply issue warrants, law enforcement would execute those warrants, and judges would assess the constitutionality of that execution if and when a criminal defendant moved for the court to suppress the fruits of the search. *Ex post* review is preferable, opponents of *ex ante* minimization rules argue, for three reasons: first, permitting magistrates to impose *ex ante* limits will impose unnecessary restrictions on government searches;[191] second, magistrates and prosecutors lack the ability to predict search needs;[192] and finally, the use of *ex ante* instructions will impede higher courts' development of Fourth Amendment requirements when it comes to computer searches.[193]

With respect to the concern that *ex ante* limits place constraints on government investigators that are too strict and thereby impede effective investigations, there are at least two responses. First, if the government begins to execute a warrant and determines that it needs broader searching capabilities or an extension of time limits, there is nothing that prevents returning to the magistrate for a modification of the existing warrant or applying for a new warrant. Indeed, when investigators executing a warrant authorizing a search for evidence of drug trafficking found evidence of child pornography as well, the Tenth Circuit held that upon first discovering child pornography, they should have applied for a second warrant before seeking out additional evidence of child pornography.[194] Second, courts imposing *ex ante* limits do not do so to dictate how searches will be executed. Instead, they seek "a sophisticated technical

---

[190] *See* Kerr, Ex Ante *Regulation*, *supra* note 21, at 1278–80.

[191] *See* Three Hotmail Email Accounts, No. 16-MJ-8036-DJW, 2016 WL 1239916, at *16 (D. Kan. Mar. 28, 2016) (describing objections) (citing *In re* Appeal of Application for Search Warrant, 71 A.3d 1158, 1171 (Vt. 2012)).

[192] *See* Gmail Account, 33 F. Supp. 3d 386, 400 (S.D.N.Y. 2014) ("Our inability to predict the best mechanism for conducting a search strongly counsels against including any search protocol in a warrant."); Kerr, Ex Ante *Regulation*, *supra* note 21, at 1281–84.

[193] *See* Kerr, Ex Ante *Regulation*, *supra* note 21, at 1278–90. These drawbacks, in his view, outweigh the benefits of addressing the current legal uncertainty. *Id.*

[194] United States v. Carey, 172 F.3d 1268, 1274–76 (10th Cir. 1999); *see also* United States v. Turner, 169 F.3d 84, 88 (1st Cir. 1999) (suppressing evidence of child pornography that officers found by opening JPEG files on a computer in a home they were searching for physical evidence of assault).

explanation of how the government intends to conduct the search so that the Court may conclude that the government is making a genuine effort to limit itself to a particularized search."[195] In other words, the issuing court is not imposing its own limits so much as ensuring that the government has a plan to impose constraints on itself.

Objections based on magistrates' ability to determine in advance what type of search is necessary are similarly misplaced. One version of this objection is simply based on magistrates' (and prosecutors', for that matter) lack of a crystal ball; it is impossible to predict in advance what steps investigators will need to take to perform an effective search. But again, *ex ante* limits are neither finite nor set in stone. Magistrates' demands have simply been that the government, as part of its warrant application, explain its search plans—how it intends to find responsive information, and what it intends to do with information it comes across that falls outside the scope of the warrant.[196] The content of *ex ante* limits thus comes not from prognostication but rather from a description of the government's plans.

Opponents also question the magistrates' ability to assess the government's search needs as a matter of institutional competence. They question, that is, whether magistrates have sufficient expertise or knowledge to set out effective rules to govern digital searches. Here again, this objection seems to misconstrue the magistrates' actual role. The government does not simply submit an application to the magistrate and rely upon him or her to construct from scratch a set of rules. Rather—as with the FISA Court—the government's application itself contains proposed limits.[197] It is up to the government to determine how it will go about its search, so long as it can articulate some constraints on its authority.[198] And as several magistrates have stressed, the government need not

---

[195] Apple iPhone, 31 F. Supp. 3d 159, 167–68 (D.D.C. 2014) ("[T]his Court is not requiring a search protocol so that it may specify how the warrant is to be executed. Instead, the protocol will explain to the Court how the government intends to determine where it will search."); *see also* Cellular Tels., No. 14-MJ-8017-DJW, 2014 WL 7793690, at *10 (D. Kan. Dec. 30, 2014); *In re* the Search of ODYS LOOX Plus Tablet, Serial No. 4707213703415, in Custody of U.S. Postal Inspection Serv., 1400 N.Y. Ave. NW, Wash., D.C., 28 F. Supp. 3d 40, 45 (D.D.C. 2014).

[196] *Three Hotmail Email Accounts*, 2016 WL 1239916, at *2; *id.* at *20 ("The government is free to determine the best procedure and techniques to use, so long as the government provides notice as to what those procedures are."); *see also* In re *the Search of ODYS LOOX Plus Tablet*, 28 F. Supp. 3d at 46 (noting that the search protocol "need not be overly detailed—the Court is not asking for a list of search terms—but the overview must provide" enough information to assure that court that it would not be authoring a general search).

[197] *See, e.g.*, *Apple iPhone*, 31 F. Supp. 3d at 168.

[198] *See In re* the Search of Info. Associated with [redacted]@mac.com, 13 F. Supp. 3d 145, 153–54 (D.D.C. 2014) (describing magistrates' frustration at government's persistent failure to respond to repeated requests that it include search limits in its application).

be concerned that its applications will prove too technologically sophisticated for magistrates to digest. Instead, "[t]he government should not be afraid to use terms like 'MD5 hash values,' 'metadata,' 'registry,' 'write blocking' and 'status marker,' nor should it shy away from explaining what kinds of third party software are used and how that software is used to search for particular types of data."[199] In other words, magistrates are not holding themselves out as technical experts. They are merely asserting the need to be sure that the government's own experts have devised a sufficiently circumscribed protocol.

Finally, this Part turns to concerns that permitting magistrates to impose *ex ante* rules on searches will prevent case law regarding what qualifies as reasonable when it comes to digital searches from developing. Fourth Amendment law frequently evolves as a result of *ex post* review of law enforcement activities. That is to say, after government officials execute a search or a seizure, that action is subject to judicial review when a criminal defendant seeks to suppress the fruits of that search or seizure. Advocates for *ex post* review are concerned that, if magistrate judges regularly impose *ex ante* rules for searches, then higher courts' review of the lawfulness of a search will be focused on whether the government complied with the magistrate's instructions, rather than whether the search itself was reasonable.[200] There will therefore be no vehicle driving the development of the law regarding what constitutes a reasonable search or seizure.

There are both legal and policy-based responses to this argument. As a legal matter, it is important to note that magistrates who have articulated their justification for imposing *ex ante* limits have not identified them as a way to ensure that searches are reasonable. Rather, they have imposed those limits to satisfy the requirements of probable cause and particularity, without which they cannot issue warrants.[201] When magistrate judges, for example, have insisted that warrants include a particular search protocol, they have done so "not *in addition to* the requirements of the Fourth Amendment, but *in satisfaction of*

---

199 *Apple iPhone,* 31 F. Supp. 3d at 168.

200 *See* Kerr, Ex Ante *Regulation*, *supra* note 21, at 1287–90.

201 *E.g.*, Nextel Cellular, No. 14-MJ-8005-DJW, 2014 WL 2898262, at *10 (D. Kan. June 26, 2014) (rejecting application for warrant allowing unlimited search of cell phone contents as authorizing seizure of data for which government lacks probable cause and failing to satisfy the Fourth Amendment's particularity requirement); *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 *3, *8 (D. Kan. Aug. 27, 2013) (rejecting warrant application for not describing the data to be seized in a sufficiently particularized fashion); Ohm, *supra* note 18, at 10 (recognizing that "magistrate judge-imposed restrictions on search warrants protect against not only the failure of particularity but also the manifest failure of probable cause").

them."[202] If magistrates are correct that warrants for digital searches that lack limitations do not satisfy the probable cause or particularity requirements, then evidence uncovered by such searches risks being suppressed at trial for that reason. A search executed on the basis of a warrant issued without probable cause or sufficient particularity is almost always, by definition, unreasonable.

As a policy matter, Professor Kerr's insistence on *ex post* review is curious given his usual recognition of the need for flexibility. In other contexts, he argues, for example, that because "the privacy implications of particular rules can fluctuate as technology advances," we need mechanisms that can "adapt to technological change."[203] For Kerr, that usually means a preference for legislative action over judicial decision-making, because Congress is free to experiment and make amendments,[204] while Fourth Amendment-based judicial decisions enshrine in constitutional law approaches that may become dated.[205]

But if flexibility is important, *ex ante* minimization rules outperform legislatures as well as *ex post* judicial review. Indeed, the NSA has explicitly objected to codifying minimization procedures on the grounds that "it can be difficult to change a statute if the procedures need to be changed in order to meet operational needs."[206] Even if some investigative techniques pose threats to privacy and therefore require minimization, there is no rule dictating what the minimization procedures must look like. Therefore if a judge determines, for example, that the current state of technology demands that investigators employ a taint team to limit access to non-responsive information contained in a suspect's cell phone, that limit can be included in a judicial order authorizing the search without necessarily imposing that same rule on all cell phone searches going forward. If six months later, technology has evolved to mitigate the

---

[202] Cellular Tels., No. 14-MJ-8017-DJW, 2014 WL 7793690, at *6 (D. Kan. Dec. 30, 2014); *see also* In re *the Search of Info. Associated with [redacted]@mac.com*, 13 F. Supp. 3d at 152 (denying government's warrant application to seize all emails from an account because it has shown probable cause only for *some* of the emails in that account).

[203] *See* Kerr, *The Fourth Amendment and New Technologies*, *supra* note 3, at 871–75.

[204] *E.g.*, *id.* at 805–806. As Justice Alito pointed out, even if the best solution to privacy concerns arising from dramatic technical change are legislative, neither Congress nor most states have enacted statutes regulating, for example, the use of GPS tracking technology for law enforcement purposes. United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring). The same can be said for computer and cell phone searches and the use of information contained in law enforcement databases. Others advocate for a more robust judicial role. *See, e.g.*, Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1752–53 (1995) (arguing that when technological changes disrupt the law, the lower courts should wrestle with the difficult questions "to create a body of legal material from which others may draw in considering these questions").

[205] Kerr, *The Fourth Amendment and New Technologies*, *supra* note 3, at 805–07, 858 ("[I]t is difficult for judges to fashion lasting guidance when technologies are new and rapidly changing.").

[206] Banks, *supra* note 79, at 1664 (quoting NSA's minimization procedures).

privacy threat posed by cell phone searches, judges would be free to impose minimization demands that take account of this development.[207]

Establishing rules *ex ante* also benefits the investigators themselves. Normally, uncertainty in Fourth Amendment jurisprudence is disfavored by law enforcement because the absence of clear rules means government officials have insufficient guidance regarding how they may lawfully carry out their duties.[208] Often this aversion to uncertainty produces a preference for bright-line constitutional rules that make plain what conduct is acceptable.[209] Placing *ex ante* rules within the warrant itself means that even in the face of uncertainty regarding the constitutional requirements for digital searches, law enforcement will know at the outset what is permissible in the execution of any given warrant. Of course, a court might subsequently disagree that the minimization procedures laid down in a warrant actually were adequate to meet Fourth Amendment requirements. However, this is likely to be a rare occurrence.[210] Investigators following *ex ante* rules can therefore execute their search confident in their future ability to use its fruits as evidence at trial, whereas investigators without such guidelines must speculate whether the trial judge will allow the evidence to be introduced. Minimization therefore mitigates the usual concern about the absence of bright-line rules to guide law enforcement action when the applicable law is uncertain.

There are two additional advantages to encouraging magistrates to use *ex ante* minimization rather than relying on *ex post* judicial review. The first flows from that fact that so many defendants challenging digital searches are charged with possession of child pornography. Individuals whose digital devices contain such images do not create a sympathetic context in which to consider the propriety of a search. Judges are likely—consciously or unconsciously—to seek to validate arguably problematic searches because of what they uncover, potentially skewing the resulting doctrine in the government's favor.[211] While

---

[207] *See* United States v. Hill, 459 F.3d 966, 979 (9th Cir. 2006).

[208] Kerr, *The Fourth Amendment and New Technologies*, *supra* note 3, at 884 ("[I]n the criminal context rule-uncertainty is a liability.").

[209] *E.g.*, O'Connor v. Ortega, 480 U.S. 709, 730 (Scalia, J., concurring) (noting that the Supreme Court "repeatedly has acknowledged the difficulties created for courts, police, and citizens by an ad hoc, case-by-case definition of Fourth Amendment standards to be applied in differing factual circumstances."); White v. United States, 454 U.S. 924, 927 (1981) (White, J., dissenting) (dissenting from denial of certiorari because of "uncertainty involv[ing] a fundamental aspect of law enforcement operations" and because "clarification of the boundaries of legitimate police activity under the Constitution is ultimately this Court's responsibility").

[210] *See* Kerr, Ex Ante *Regulation*, *supra* note 21, at 1285–86 (recognizing that evidence within the scope of a warrant is hard to suppress unless the warrant is flagrantly disregarded).

[211] *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 802 (1994).

inadvertently rooting out someone with child pornography is not necessarily a bad thing, the next time that same search technique is used, it might be on the digital storage of someone completely innocent.

Second, *ex ante* minimization requirements will prevent the government from benefiting from clear constitutional violations due to the good-faith exception to the exclusionary rule.[212] The good-faith exception says that the exclusionary rule should not bar the use of evidence obtained pursuant to searches executed in reasonable reliance on a warrant that is ultimately found to be invalid.[213] It may be the case that post hoc review determines that some warrants issued without *ex ante* instructions in them are invalid—because they lack sufficient probable cause or particularity, or because the search they authorized was otherwise unreasonable. Unless the warrant's deficiencies were relatively clear to the executing officers at the time the search was conducted, however, the government will face no penalty for having invaded a defendant's Fourth Amendment rights. *Ex ante* limits have the benefit of preventing constitutional violations before they ever take place.[214]

Minimization provides the best of all worlds: it ensures privacy protections in each search, preserves flexibility while simultaneously offering sufficient guidance for law enforcement, and provides judges the freedom to experiment and evolve as both technology and investigative techniques develop.[215] Ultimately, if the Supreme Court or Congress determines that rules for these searches should be codified more permanently, judges' use of varying forms of minimization and their relative effectiveness also will provide appellate judges and policymakers valuable information regarding which tools are most effective.[216]

C. Magistrate Judges' Authority to Require Minimization Procedures

The potential advantages of *ex ante* regulation can only be exploited if judges and magistrates actually have the authority to include minimization rules

---

[212] In United States v. Ganias, the full Second Circuit applied the good faith exception to the warrant clause for a search, 824 F.3d 199, 225–26 (2d Cir. 2016) (en banc), reversing the panel's opinion, which held that the search was "a widespread seizure of files beyond the scope of the warrant—conduct that resembled an impermissible general search." United States v. Ganias, 755 F.3d 125, 140 (2d Cir. 2014), *rev'd en banc on other grounds*, 824 F.3d 199 (2d Cir. 2016).

[213] United States v. Leon, 468 U.S. 897, 920–21 (1984).

[214] *See* Cellular Tels., No. 14-MJ-8017-DJW, 2014 WL 7793690, at *10 (D. Kan. Dec. 30, 2014) ("While *ex post* remedies are aimed at mitigating harm resulting from an unconstitutional search and seizure, *ex ante* restrictions help ensure that no violation of an individual's Fourth Amendment rights takes place at all.").

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

[216] *See* Lessig, *supra* note 204, at 1752–53.

in search warrants. Again, Professor Kerr is skeptical, arguing that the magistrate's role in crafting warrants is "surprisingly narrow" and does not include the kind of *ex ante* rulemaking authority contemplated here.[217] This contention rests on the language of the federal search warrant statute, which is mirrored by many states, as well as the doctrine emerging from several judicial opinions.[218] As Professor Ohm effectively refutes Kerr's doctrinal argument, this Article need not repeat his analysis in detail here.[219] Having examined the sources on which Kerr relies, however, he concludes that while it is true that the Supreme Court has never *required ex ante* limits, neither has it *forbidden* them.[220]

As for the textual argument, Kerr opines that Rule 41's requirement "that judges *must* issue warrants when investigators" establish probable cause means that judges have no "authority to condition issuance of a warrant on its execution."[221] To be sure, Rule 41 does include that compulsory language. As an initial matter, this argument only has force if law enforcement's showing of probable cause is valid in the absence of *ex ante* instructions.[222] Even if there is no question as to the sufficiency of the probable cause showing, however, nothing in the rule imposes any restrictions on including content in the warrant above and beyond the mandatory elements.[223] At the same time, Rule 41 does specify that warrants for electronically stored information are assumed to authorize "a later review of the media or information *consistent with the warrant*."[224] Rule 41's requirement that a later review of electronic media be "consistent with the warrant" arguably contemplates a warrant that not only

---

[217] *See* Kerr, Ex Ante *Regulation*, *supra* note 21, at 1261.

[218] United States v. Grubbs, 547 U.S. 90, 97–98 (2006) (anticipatory warrants need not include a particular description of the triggering condition to be valid); Lo-Ji Sales v. New York, 442 U.S. 319, 328 (1979) (holding that the magistrate's participation in the execution of the warrant violated the Fourth Amendment, and arguably construing magistrates' roles narrowly); Dalia v. United States, 441 U.S. 238, 257 (1979) (holding that warrants need not include a specification of the precise manner in which they are going to be executed).

[219] *See* Ohm, *supra* note 18, at 2–11 (arguing that Kerr's analysis errs, *inter alia*, in evaluating the use of *ex ante* search limits under the Fourth Amendment's reasonableness requirement rather than viewing such limits as a means of satisfying the requirements of probable cause and particularity).

[220] *Id.*; *see also* Ferguson, *supra* note 6.

[221] Kerr, Ex Ante *Regulation*, *supra* note 21, at 1271 (emphasis added); FED. R. CRIM. P. 41(d)(1) ("After receiving an affidavit or other information, a [judge] . . . must issue the warrant if there is probable cause to search for and seize a person or property . . . .").

[222] *See supra* notes 201–202 (pointing out that some magistrates have included *ex ante* rules as a means of satisfying probable cause requirements, because only by following those rules will law enforcement's access be limited to material for which they have probable cause).

[223] FED. R. CRIM. P. 41(e)(2)(A) (listing as mandatory requirements that all warrants command law enforcement to execute the warrant within two weeks, during the daytime, and return the warrant once it has been executed).

[224] FED. R. CRIM. P. 41(e)(2)(B) (emphasis added).

authorizes the search but also includes terms with which the government must act consistently. There is nothing to say that these terms may not include specific limitations on how the government executes the search.

Indeed, magistrates regularly include such limitations outside the digital context,[225] and magistrate judges already are explicitly authorized in Rule 41 to specify a deadline by which the warrant must be executed, to dictate whether the warrant may be executed at night, and to require any unlawful property deprivation be remedied.[226] Additional minimization procedures are not a significant departure from such measures.

Finally, recall the FISA Court's treatment of the Internet metadata collection program. The orders approving that program included exceedingly detailed, rigorous minimization procedures.[227] Yet neither the Constitution nor the relevant statute required minimization of that information at the time. This implies that the judicial power includes some discretion regarding whether and when the government should be subject to privacy-related constraints. In any event, if judges currently do lack this power, Rule 41 could easily be amended to include a provision mirroring FISA's language specifically delegating to issuing judges the power to devise, require, and oversee minimization procedures.

CONCLUSION

Minimization procedures have always straddled the divide between statutory and constitutional territory. They almost always derive from statutory demands, but Congress uses them in legislation to allay concerns about the constitutionality of over-broad collection. In other words, where they are statutorily required, they are there because they are constitutionally necessary. This tool, however, can also address the constitutional concerns raised by inevitable over-broad collection in circumstances where they are *not* statutorily required. Indeed, minimization presents an elegant solution to a challenge the courts currently face. The FISA Court devised a remarkable variety of minimization procedures to meet privacy concerns. In so doing, it showed how helpful a safeguard minimization can be in situations where narrowly targeted collection is technologically challenging. FISA judges also demonstrated the benefit of having reviewing judges help to design the limits as part of their *ex*

---

225 *See* Ohm, *supra* note 18, at 4 ("Outside the computer context, magistrate judges regularly impose *ex ante* restrictions on search warrants in order to ensure probable cause and particularity." (italics added)).

226 FED. R. CRIM. P. 41(e), (g).

227 *See supra* Section II.B.2.d.

ante oversight of searches and seizures. Judges facing the analogous challenge of crafting warrants to search digital storage devices cleverly recognized that the tool could address their concerns as well. Rather than accusing magistrates of revolting, we should be praising their foresight in importing an existing legal mechanism to protect individual privacy while also enabling effective criminal investigations.