DIGITAL DUPLICATIONS AND THE FOURTH AMENDMENT

INTRODUCTION

The explosive growth of digital data in the twenty-first century has been both a boon and a curse for law enforcement. On one hand this growth has heralded a "golden age of surveillance" owing to the massive amount of information that is available about actual and potential lawbreakers,[1] but on the other hand the government now has that much more data to sort through. To search this ever-expanding "haystack," the government has adopted various techniques, including algorithmic queries. But in order to apply these queries — to search for the needle — the government must first collect the hay. One technique that law enforcement has adopted is to take "mirror images" of digital data for later off-site review.

A persistent question, though, is how the Fourth Amendment applies to both the initial act of duplicating digital data and the continued retention of that data. It goes without saying that the drafters of the Fourth Amendment did not contemplate its application to the digital era. And Fourth Amendment jurisprudence, accordingly, has long since departed from a strict originalist understanding. Beginning with *Katz v. United States*,[2] the Supreme Court adapted "[t]he right of the people to be secure . . . against unreasonable searches and seizures"[3] to cover modern technological developments by finding such a violation when the government surreptitiously recorded a phone conversation in a public phone booth.[4]

Since then, the Court has considered the Fourth Amendment's application to a variety of new technologies ranging from airplane surveillance to thermal imaging.[5] In *Riley v. California*,[6] for example, the Supreme Court analyzed the application of the Fourth Amendment to searches of a cell phone seized incident to arrest. Noting that modern cell phones contain vast troves of personal information, far beyond

---

[1] *E.g.*, Peter Swire, *The Golden Age of Surveillance*, SLATE (July 15, 2015, 4:12 PM), http://www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html [http://perma.cc/957N-QFL4].

[2] 389 U.S. 347 (1967).

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

[4] *See Katz*, 389 U.S. at 359.

[5] *See, e.g.*, United States v. Karo, 468 U.S. 705 (1984) (radio tracking); California v. Ciraolo, 476 U.S. 207 (1986) (airplane surveillance); Florida v. Riley, 488 U.S. 445 (1989) (helicopter surveillance); Kyllo v. United States, 533 U.S. 27 (2001) (thermal imaging); United States v. Jones, 132 S. Ct. 945 (2012) (GPS tracking); Maryland v. King, 133 S. Ct. 1958 (2013) (DNA swabs); Riley v. California, 134 S. Ct. 2473 (2014) (cell phones).

[6] 134 S. Ct. 2473.

what one historically could keep in one's pocket, the Court found that the rationale for the search-incident-to-arrest exception to the warrant requirement did not extend to a cell phone's digital contents.[7]

This Note attempts to address a narrow question in modern Fourth Amendment jurisprudence: should government duplication and retention of electronically stored information be characterized under the Fourth Amendment as a search, as a seizure, as both, or as neither?[8] Duplication and retention arise in many contexts.[9] But somewhat shockingly, it is not entirely settled that the government conducts either a search or a seizure when it makes a copy of locally stored data,[10] and then retains that data *without* further reviewing it.[11] As Justice Sotomayor worries, "[t]he Government can store such records and efficiently mine them for information years into the future."[12]

One technique the government has adopted to address the growth of relevant data, a technique which some courts have blessed, is to take a "mirror image" of a hard drive (or other data repository) on site, leave the original with the owner, and then perform the search off-site at a later time.[13] A mirror image is an exact duplicate of the original

---

[7] *Id.* at 2494–95.

[8] Although this Note does explore Fourth Amendment "reasonableness" balancing as applied to duplication and retention in Part IV, its primary focus is on the predicate question of whether a search or seizure has even occurred.

[9] For example, many warrants include temporary seizure provisions that require the government to return seized items after a certain period of time. The government could potentially make a copy of any hard drives seized and retain the copy beyond the warrant period. *See, e.g.*, United States v. Ganias, 755 F.3d 125 (2d Cir. 2014) (finding such conduct a seizure of the data and applying the exclusionary rule), *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015); *cf.* United States v. Cote, 72 M.J. 41 (C.A.A.F. 2013) (applying exclusionary rule to exclude evidence obtained from an original hard drive retained beyond the authorized period). Additionally, the technology certainly exists to enable the government to remotely access computers connected to the Internet, potentially allowing remote copying without requiring a physical trespass. *Cf.* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

[10] Under current law, information shared with third parties (such as with cloud storage) may lose the veneer of privacy and thus is no longer protected by the Fourth Amendment. *See* Smith v. Maryland, 442 U.S. 735, 743 (1979). This Note focuses on locally stored data for simplicity, but the Court in *Riley* suggested that the Fourth Amendment protections would apply equally to data stored "in the cloud," *see* 134 S. Ct. at 2491; *see also Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (noting that the third-party doctrine "is ill suited to the digital age"); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002) (warning against rigid application of this rule in the digital era).

[11] Later review by a government agent would most likely constitute a search. However, because the items being searched are duplicates in government possession, not originals, even this issue may not be fully settled. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 562–65 (2005).

[12] *Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring).

[13] *See, e.g.*, *Ganias*, 755 F.3d at 135 ("[T]he creation of mirror images for offsite review is constitutionally permissible in most instances . . . ."); United States v. Veloz, No. 12-10264, 2015 WL 3540808, at *5 (D. Mass. June 4, 2015); *cf.* United States v. Tamura, 694 F.2d 591, 595–96 (9th Cir.

data, which investigators can then access in a "read-only" state to avoid altering the data in even the smallest way.[14] This approach allows the search to proceed with minimal interference in the data owner's work or life, since the owner retains the originals. The investigators, for their part, are able to work in their own offices, under their own time constraints. And, because the data was copied exactly and remains unaltered, it is easily authenticated and used as evidence.[15]

At first blush, it is unclear how mirror-imaging fits into the constitutional landscape. The Fourth Amendment prohibits "unreasonable searches and seizures."[16] As the Court recently reiterated in *Riley*, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[17] However, the government can avoid even that standard if its actions constitute neither a search nor a seizure — a prerequisite to Fourth Amendment scrutiny.[18] The mirror-image approach thus raises the question of whether duplication and retention constitutes a search or seizure subject to Fourth Amendment reasonableness requirements.

Answering that question requires determining whether duplication either (a) violates the individual's reasonable expectation of privacy, or (b) interferes with the individual's possessory interest in the information.[19] The caselaw offers no conclusive answers. Indeed, until very recently, it tended to suggest that the Fourth Amendment had no application to duplication because it is neither a search nor a seizure. If the government just "copies" the data, without looking at it, then there is no invasion of privacy. If the data owner retains the original, then there is no intrusion on possessory interests. These answers, though, seem both unsatisfying and instinctively wrong.

Some courts and commentators have suggested that such duplication should be considered a seizure because it interferes with the individual's "right to delete" data[20] or right to exclude others from

---

1982) (noting that off-site review may be appropriate — subject to prior approval by a magistrate — when on-site review is infeasible).

14 *See* Scott Carlson, *New Challenges for Digital Forensics Experts and the Attorneys Who Work with Them*, *in* UNDERSTANDING THE LEGAL ISSUES OF COMPUTER FORENSICS 17, 19–20 (2013), 2013 WL 3759817, at *2 (discussing digital forensics procedures).

15 *See* Recent Case, 128 HARV. L. REV. 743, 748–49 (2014) (describing authentication process).

16 U.S. CONST. amend. IV.

17 Riley v. California, 134 S. Ct. 2473, 2482 (2014) (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)).

18 For example, using a trained canine to sniff the exterior of a bag for drugs is not subject to any "reasonableness" analysis because the Supreme Court has held that such an action is neither a search nor a seizure. *See* United States v. Place, 462 U.S. 696, 707 (1983); *see also* Illinois v. Caballes, 543 U.S. 405, 409 (2005) (finding that a canine sniff of car stopped for a traffic violation was not a search). *But see* Florida v. Jardines, 133 S. Ct. 1409, 1417–18 (2013) (finding a canine sniff on the front porch of home was a search).

19 *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984). This Note assumes that the individual has an actual (subjective) expectation of privacy — without which no search occurs.

20 *See* Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. F. 10 (2005).

data.[21] Others have argued that it is a seizure if it "freezes" evidence for later review rather than as a memory aid.[22] While such conceptions subject duplication of electronic data to Fourth Amendment scrutiny, they do so by shoehorning the process into existing precedent on "seizures." But the problem with government duplication is not easily conceived of as interference with "possessory interests," since the data owner not only retains unfettered rights to the original, but also may not have exclusive rights over much of the data in the first instance. Accordingly, it makes little sense to label such conduct as a "seizure."

Instead, this Note proposes, courts should focus on the privacy interests at stake in duplication of that information, and whether government duplication and retention of an individual's private data violates that expectation, and is therefore a search. Privacy, often defined as "control over personal information,"[23] is clearly infringed when the government duplicates that information, thus depriving the data owner of control. Viewing duplication as a search would avoid some of the complications that arise from characterizing it as a seizure, such as whether the data owner does in fact have a right to exclusive possession of the particular data.

Part I explores the doctrine surrounding searches and seizures in general terms and examines some background cases analogous to the digital duplication context. Part II considers the arguments advanced by some courts and commentators that digital duplication is properly conceived as a seizure. In Part III, the Note shows why the doctrine supports viewing duplication as a search. Part IV examines some of the consequences that arise from the proposed recharacterization.

I. BACKGROUND SEARCH AND SEIZURE DOCTRINE

Fourth Amendment jurisprudence has been adapted to new technology many times throughout its history.[24] As the government has acquired new methods for collecting evidence, courts have adjusted the test for what constitutes a violation.[25] Most significantly, in *Katz*, the Court moved beyond its prior trespass inquiry to bring a listening de-

---

[21] *See* United States v. Ganias, 755 F.3d 125, 137 (2d Cir. 2014), *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015); Mark Taticchi, Note, *Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures*, 78 GEO. WASH. L. REV. 476 (2010).

[22] *See* Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 714–15 (2010).

[23] *See infra* section III.A, pp. 1059–63.

[24] *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) (discussing the shifts in the jurisprudence in response to new technologies).

[25] Professor Orin Kerr calls this the "equilibrium" approach to the Fourth Amendment, wherein the Court tries to maintain the status quo between "cops and robbers." *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 486 (2011).

vice on a public phone booth within the Fourth Amendment's ambit.[26] In *Kyllo v. United States*,[27] the Court ruled that the government "searched" a home when, from a car on a public way, it used thermal imaging to measure the heat given off from the roof of a home.[28] In *Riley*, the Court imposed strict limitations on the circumstances under which a police officer could search a cell phone incident to arrest.[29] But there is little Supreme Court guidance on applying the Fourth Amendment to duplications, and lower courts have had to analogize from old caselaw of questionable relevance in the modern context. Consequently, earlier cases tended to find that duplication constituted neither a search nor a seizure. More recently, however, that trend has reversed itself, and courts have begun to apply Fourth Amendment scrutiny to duplications of digital data.

A. Search or Seizure

The Fourth Amendment regulates both searches and seizures. These are two discrete government actions, each of which is independently subjected to the Constitution's "reasonableness" requirement. In *United States v. Jacobsen*,[30] the Court defined a seizure as "some meaningful interference with an individual's possessory interests" in the property.[31] A seizure threatens the individual's "interest in retaining possession of property"[32] and "contemplates a forcible dispossession of the owner."[33]

Jacobsen also defined a search: a search "occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[34] This definition builds on Justice Harlan's concurrence in *Katz*.[35] *Katz* unquestionably elevated the importance of privacy to the Fourth Amendment inquiry, and indeed, until *United States v. Jones*,[36] privacy seemed to have attained status as not only the primary but

---

[26] Katz v. United States, 389 U.S. 347, 353 (1967). In several recent cases, the Court, led by Justice Scalia, has revived the trespass inquiry as an additional test for Fourth Amendment violations. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 953 (2012). Kerr has suggested that, contra *Jones*, there was no "trespass test" before *Katz*. *See* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 68.

[27] 533 U.S. 27 (2001).

[28] *Id.* at 30, 40.

[29] Riley v. California, 134 S. Ct. 2473, 2495 (2014).

[30] 466 U.S. 109 (1984).

[31] *Id.* at 113.

[32] Texas v. Brown, 460 U.S. 730, 747 (1983) (Stevens, J., concurring in the judgment); *see also* United States v. Place, 462 U.S. 696, 716 (1983) (Brennan, J., concurring in the result).

[33] Hale v. Henkel, 201 U.S. 43, 76 (1906), *overruled in part by* Murphy v. Waterfront Comm'n, 378 U.S. 52 (1964).

[34] 466 U.S. at 113.

[35] *See* 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[36] 132 S. Ct. 945 (2012).

perhaps the exclusive focus of Fourth Amendment search analysis.[37] Although this primacy has been criticized by commentators, there are strong reasons for maintaining a focus on privacy.[38] In any event, even after *Jones*, privacy is plainly a part of the search inquiry. If the government has "infringed" a reasonable expectation of privacy, then it has conducted a search.

But privacy defies easy definition.[39] In general, though, courts and commentators have come to view privacy as "determining for oneself when, how and to whom personal information will be disclosed."[40] Privacy is an "individual's control of information concerning his or her person."[41] This definition dates back at least to Professor Alan Westin's seminal work, published the same year *Katz* was decided.[42] Westin's definition has gained traction in Fourth Amendment scholarship.[43] Left to debate, of course, is what information is "personal" and thus private. But so defined, it seems natural to say that an individual has an expectation that she will retain control over the information contained in her data storage device. Whether the expectation is reasonable is illuminated by reference to real and personal property law and societal understandings.[44]

A few examples serve to illustrate the dichotomy between searches and seizures. As noted, a seizure occurs when the government meaningfully interferes with an individual's possessory interests.[45] If a police officer takes your phone away from you, then that officer has "seized" your phone. A court reviewing that action would then ask whether that seizure was "reasonable" within the meaning of the

---

[37] *Jones* renewed the focus on property rights, but as that case illustrates, the property-driven analysis had never been entirely displaced. *See, e.g.*, Soldal v. Cook County, 506 U.S. 56, 62 (1992) ("[O]ur cases unmistakably hold that the [Fourth] Amendment protects property as well as privacy.").

[38] *See generally* Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches*, 48 TEX. TECH L. REV. (forthcoming 2016) (rebutting criticisms of the significance of privacy in Fourth Amendment analysis).

[39] *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 10–11 (2008) (proposing sixteen categories of privacy); *see also* David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1113 (2014) (defining privacy as a type of refuge from the government).

[40] Nat'l Cable & Telecomms. Ass'n v. FCC, 555 F.3d 996, 1001 (D.C. Cir. 2009).

[41] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

[42] *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (defining privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others").

[43] *See* Sklansky, *supra* note 39, at 1083–84 (describing the dominance of Westin's definition in modern academic discourse); *see also* Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 51 (1995).

[44] *See* Rakas v. Illinois, 439 U.S. 128, 144 n.12 (1978).

[45] *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

Fourth Amendment.[46] A search, on the other hand, occurs when the government violates an individual's actual and reasonable expectation of privacy.[47] Thus, if a police officer looks at your phone's contents, such as your contacts list or stored videos, that officer has "searched" your phone because he has interfered with your control over the personal information contained within. The reviewing court would ask whether that search was reasonable — which, as *Riley* emphasized, generally means pursuant to a warrant.[48] If an officer takes your phone from you and then looks at the photos on it, that officer has seized and then searched your phone. By contrast, when the police officer watches you talking on your phone as you walk down Main Street, he has conducted neither a search nor a seizure.[49] No reasonable expectation of privacy has been invaded by the officer's observations of you in public, and the officer's action in no way interferes with your possession of your phone. That action, then, is never subjected to Fourth Amendment reasonableness analysis.[50]

B. Early Duplication Cases

Arizona v. Hicks[51] concerned duplication but is far removed from the digital context: While searching an apartment for the source of an errant gunshot, a police officer noticed some high-end stereo equipment that he suspected might be stolen and recorded the serial number to check against a police database of stolen equipment.[52] The Court quickly discarded the argument that recording the serial number constituted a seizure. The recording did not "meaningfully interfere" with the defendant's possessory interest in the information; because the officer did not confiscate the stereo, he had not interfered with the defendant's possession of either the stereo or the serial number.[53]

Some lower courts have also considered duplication in other nondigital contexts, such as photocopies and photographs. Several cases, for example, suggest that photocopying is not a seizure.[54] But in

---

[46] *See, e.g.*, United States v. Place, 462 U.S. 696, 709–10 (1983).

[47] *See Jacobsen*, 466 U.S. at 113; Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* Smith v. Maryland, 442 U.S. 735, 740 (1979) (adopting Justice Harlan's approach from *Katz*).

[48] Riley v. California, 134 S. Ct. 2473, 2495 (2014).

[49] *See* United States v. Knotts, 460 U.S. 276, 281–82 (1983).

[50] *See, e.g.*, Illinois v. Caballes, 543 U.S. 405, 408–10 (2005) (declining to consider the reasonableness of a dog sniff after concluding that the dog sniff was not itself a search).

[51] 480 U.S. 321 (1987).

[52] *Id.* at 323.

[53] *Id.* at 324. The Court nonetheless affirmed the exclusion of the evidence, holding that moving the stereo to reveal the serial number constituted a search, which was unreasonable given the lack of probable cause. *Id.* at 328.

[54] *See, e.g.*, United States v. Thomas, 613 F.2d 787, 793 (10th Cir. 1980) ("The agent's act of photocopying . . . was not a 'seizure.' A 'seizure' is a taking of property.").

2001, in *United States v. Gorshkov*,[55] the U.S. District Court for the Western District of Washington addressed head-on the issue of copying digital information. The FBI had obtained the defendant's password through a sting operation, and then used the password to remotely access the defendant's server.[56] Because they feared that the defendant's accomplices might delete the information on the server, the FBI remotely copied the information — without reviewing it — before applying for or obtaining a warrant.[57] The court ruled that this did not constitute a seizure, noting that the remote copying had "absolutely no impact" on possessory interests because it did not prevent others from accessing the data.[58] In the context of copying the contents of a cell phone temporarily seized incident to arrest, or of imaging a hard drive pursuant to a warrant authorizing seizure of the original, the question may be even clearer[59] because the original has already been legitimately seized and the owner's possession is already precluded.

Gorshkov was not without its detractors, as commentators recognized the potential scope of the *Hicks* rule if applied to digital duplications. If the government can make duplicates without implicating the Fourth Amendment, it could copy all of our files, which might contain "a cache of sensitive personal information,"[60] and then "efficiently mine them for information years into the future."[61]

II. POSSESSORY INTERESTS IN INFORMATION

To fit digital duplications into the Fourth Amendment, some have suggested characterizing duplication and retention as a seizure, relying on property notions of exclusive ownership. Several courts that considered the matter subsequently were similarly unpersuaded by *Gorshkov*'s reasoning, and have considered duplication to be a seizure.

A. The Possessory Rights Argument

Given that there are seemingly greater privacy implications than possessory implications to duplication, it seems strange that the prevailing view is to consider duplications as seizures. But several aca-

---

55 No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

56 *Id.* at *1.

57 *Id.*

58 *Id.* at *3. The *Gorshkov* court further noted that the Fourth Amendment did not apply because the defendant was a foreign national whose server was located overseas, *id.*, and that, even if the copying did constitute a search or seizure, it was a reasonable one, *id.* at *4.

59 The *Gorshkov* court held an evidentiary hearing to determine whether the copying had prevented access by other users. *See id.* at *3 n.1; *see also In re* United States, 665 F. Supp. 2d 1210, 1222 (D. Or. 2009) ("[T]here was no . . . meaningful interference due to the nature of electronic information, which can be accessed from multiple locations, by multiple people, simultaneously.").

60 Riley v. California, 134 S. Ct. 2473, 2490 (2014).

61 United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

demic commentators have convincingly focused the arguments on possessory interests by emphasizing application of traditional property concepts to information. Some have looked at how the act of copying interferes with use of the information, and others at how the government might use the information.

Professor Orin Kerr — who initially argued that the faithful application of the *Hicks* rule precluded classifying data duplication generally as a seizure[62] — has distinguished between "copying-as-freezing" (a seizure) and "copying-as-an-aid-to-memory" (not a seizure).[63] Kerr focuses on the purpose of a seizure — to secure evidence for later use — to distinguish between copies made for different purposes.[64] If data had already been exposed to an agent, then a duplicate of it was just made to aid that agent's memory, and was therefore not a seizure.[65] This understanding preserves the rule of *Hicks* because the officer there had already seen the serial number when he wrote it down.[66]

Professors Susan Brenner and Barbara Frederiksen have made two arguments in favor of characterizing duplication as a seizure.[67] First, as Kerr later argued, they note that copying data on a computer, unlike duplications of other mediums, interferes with the access and functioning of the computer, however briefly, during that process.[68] Second, they argue that the majority opinion in *Katz* recognized that *information* can be seized when it characterized the recording of the conversation as a seizure.[69] Copying data, even though it leaves the original intact, deprives the owner of something of value and interferes with exclusive use and possession, just as the theft of data does.[70]

Brenner and Frederiksen's first point hasn't gained much traction,[71] but several commentators have elaborated on the second. Professor Paul Ohm offers a narrower possessory interest that is infringed by duplication: the "right to delete."[72] Ohm argues that this right at-

---

[62] *See* Kerr, *supra* note 11, at 560–61.

[63] *See* Kerr, *supra* note 22, at 714–18.

[64] *Id.* at 710.

[65] *See id.* at 714–15.

[66] *Id.* at 716.

[67] *See* Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 111–13 (2002).

[68] *Id.* at 112.

[69] *Id.* at 111 (citing Katz v. United States, 389 U.S. 347 (1967)). Note, however, that the majority opinion is not so clear: although the Court referred to the recording as a "search and seizure," it was using the conjunctive term, explicitly quoting the Fourth Amendment itself, to express generally that it fell within the ambit of the Fourth Amendment. *See Katz*, 389 U.S. at 353.

[70] Brenner & Frederiksen, *supra* note 67, at 112 n.236.

[71] Ohm has criticized such a limited understanding because, as technology advances, this interference will become less and less. *See* Ohm, *supra* note 20, at 17.

[72] *See id.* As Ohm later elaborated, this right to delete derives from the traditional property right to destroy. *See* Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2, ¶¶ 62–63, https://journals.law

taches to digital data, but that it did not apply in *Hicks* because that right evaporated once the serial number was in plain view.[73] Mark Taticchi argues that the concept of exclusive possession renders exact duplicates a seizure.[74] Taticchi notes that the right to exclude others from data should be limited to exact duplicates, and not extend to summaries or memories, because the degree of interference with exclusive possession is smaller, and a rule applying to notes and memories would be "too socially costly and difficult to administer."[75]

Although several courts have concluded that duplication is a seizure, few have relied on any explicit possessory-interest analysis. In *United States v. Jefferson*,[76] the court found that taking high-resolution photographs of the defendant's documents outside the scope of the initial warrant constituted a "seizure" of the information in those documents.[77] The court emphasized that the defendant's interests extended to the data contained within the documents, not just the physical documents themselves, and that the photographs interfered with sole possession of that information.[78] In *United States v. Metter*,[79] the court noted that government possession of an imaged hard drive "presents the same privacy concerns as would the government's retention of the original communications,"[80] and found that the fifteen-month retention of the duplicate was "an unreasonable seizure."[81] In *United States v. Comprehensive Drug Testing, Inc.*,[82] the Ninth Circuit affirmed three lower-court orders requiring the United States to "return" duplicates of information that were made during the execution of a search warrant but that were outside the scope of the original warrant.[83] The court referred to the information as "seized data"[84] and "seized materials."[85] Although it did not offer any real analysis for *why* the duplication amounted to a seizure, the court plainly thought it did.[86]

.stanford.edu/sites/default/files/stanford-technology-law-review/online/ohm-olmsteadian-seizure-clause.pdf [http://perma.cc/Q3VN-ZWM6].

[73] Ohm, *supra* note 20, at 16.

[74] *See* Taticchi, *supra* note 21, at 496.

[75] *Id.* at 497.

[76] 571 F. Supp. 2d 696 (E.D. Va. 2008).

[77] *Id.* at 704.

[78] *Id.* at 702–03.

[79] 860 F. Supp. 2d 205 (E.D.N.Y. 2012).

[80] *Id.* at 212.

[81] *Id.*

[82] 621 F.3d 1162 (9th Cir. 2010) (en banc).

[83] *See id.* at 1166–67, 1178 (per curiam).

[84] *E.g.*, *id.* at 1168.

[85] *E.g.*, *id.* at 1169.

[86] Federal Rule of Criminal Procedure 41, the provision at issue, treats "seizing" and "copying" as separate concepts. *See* FED. R. CRIM. P. 41(e)(2)(B) ("A warrant . . . may authorize . . . seizure *or* copying of electronically stored information." (emphasis added)).

Recently, in *United States v. Ganias*,[87] a panel of the Second Circuit adopted the "right to exclusive possession" argument. In executing a warrant to search an accountant's computer for evidence of his clients' potential fraud, investigators imaged three hard drives, which also contained the accountant's private files.[88] Two-and-a-half years later, the investigators obtained a second warrant to search those same files for evidence of the accountant's *own* wrongdoing in a wholly separate crime.[89] The accountant, now a defendant, argued that the lengthy retention of his files that were not responsive to the initial warrant constituted an unreasonable seizure — even though he retained (and had since destroyed) the originals.[90] The Second Circuit agreed, finding that the defendant's possessory interests included the "exclusive control over [his] files" and that the government's retention of the duplicate meaningfully interfered with that interest and was thus a seizure.[91] Because the government retained that data for so long without adequate justification, the seizure was unreasonable.[92] The court did not specify at what point it became unreasonable and noted (with skepticism) that the government might have had legitimate interests in retaining the data, such as for authentication of the hard drive.[93] And although the court seemed to emphasize the "prolonged period" for which the government retained the data, its holding narrowed the importance of that factor by focusing on the use of the retained data for evidence "in a future criminal investigation."[94]

B. Why This Might Be Wrong

While this possessory-interest analysis does subject duplication and retention to Fourth Amendment scrutiny, it is a curious way to do it. After all, a seizure does not occur based on every interference with possessory interests, but only upon a *meaningful* interference.[95] If the individual retains the original copy, unaltered, and is free to use (or destroy) that copy as he sees fit, is the impingement on possessory interests (assuming there is one) meaningful? Given the multitude of cases

---

[87] 755 F.3d 125 (2d Cir. 2014), *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015). In its brief for the en banc hearing, the government conceded, "[f]or purposes of this appeal," that the mirror-imaging constituted a seizure. Brief on Rehearing En Banc for the United States at 17 n.7, *Ganias*, No. 12-240 (2d Cir. Aug. 28, 2015), 2015 WL 5112418, at *17 n.7.

[88] *Ganias*, 755 F.3d at 128.

[89] *Id.* at 130.

[90] *Id.* at 130–31.

[91] *Id.* at 137.

[92] *Id.* at 137–38.

[93] *Id.* at 139.

[94] *Id.* at 138. One might expect the "legitimate governmental interest" in accessing evidence to prosecute a crime to be categorically greater than the interest in authenticating a hard drive in another case. *See infra* section IV.A, pp. 1064–66.

[95] United States v. Jacobsen, 466 U.S. 109, 113 (1984).

where courts have found either no seizure or else a de minimis seizure when interference with possessory interests was marginal,[96] it seems tenuous to argue that *this* infringement — which has no impact on the user's own experience with his data — is a sufficient interference either to implicate the Fourth Amendment in the first place or ever to be found unreasonable.

Perhaps one reason duplication nonetheless seems to be a "seizure" is that, after duplication, the government itself now possesses something that it did not possess before. That is, if the government exerts "dominion and control"[97] over something, it must have seized it. But this focus on the *government* is divorced from the doctrine as laid out in *Jacobsen*, which teaches to assess the infringement on the individual's possession, not the government's gain. Therefore, in order to classify duplication as a seizure, the focus must be on the individual's right to *exclusive* possession of that which has been duplicated.

With tangible property, duplication would rarely amount to a seizure. If the government makes a duplicate of a coffee mug, one would be hard pressed to say that it infringed on anyone's possession of the coffee mug. After all, you're still able to look at it, drink from it, or even destroy it as you see fit.[98] Perhaps this characteristic would be different in the context of intangible property. But except for certain trade secrets or other intangible commercial property, digital data is a nonrivalrous good.[99] In most instances, the possession of data by another will not undermine the original owner's use or enjoyment. Of still more concern is that a data owner might not even have a right to exclusive possession of all the information on her hard drive, such as digital copies of movies, books, and music. If you have a copy of Ayn Rand's *Atlas Shrugged* on your hard drive, you have no right to exclusive possession of that book's contents. If the government buys its own copy, its ownership in no way infringes on your possession. And if instead it just duplicates your copy, your possession is similarly uninfringed.

---

[96] *See, e.g.*, *id.* at 125 (holding that permanent destruction of small portion of property for drug testing a de minimis intrusion on possessory interest and thus a reasonable seizure); *cf.* United States v. Mendenhall, 446 U.S. 544, 554 (1980) (suggesting that some limited physical contact might not constitute a seizure); Pennsylvania v. Mimms, 434 U.S. 106, 111 (1977) (per curiam) (concluding that intrusion on liberty in asking lawfully stopped driver to get out of car is de minimis).

[97] *Jacobsen*, 466 U.S. at 120.

[98] Paul Ohm believes otherwise. He suggests that if the government used a "Star Trek replicator on steroids" to duplicate an entire house and all of its contents, but locked the resulting duplicate in a warehouse without examining it, a court would hold that it was a seizure but not a search. Ohm, *supra* note 20, at 17; *see also id.* at 17–18.

[99] *See* Adam D. Moore, *A Lockean Theory of Intellectual Property Revisited*, 49 SAN DIEGO L. REV. 1069, 1091 (2012). A nonrivalrous good is one whose use by others does not reduce the value of the good. *See, e.g.*, Brett M. Frischmann, *An Economic Theory of Infrastructure and Commons Management*, 89 MINN. L. REV. 917, 942 (2005).

If there is no right to exclusive possession, then there is no infringement, and accordingly no seizure, at least as to that information. The right to delete or exclude would not extend to this type of data because it doesn't really "belong" to the individual. The government should not be able to duplicate an individual's home library to see what books she is reading just because she has no right to exclusive possession of the contents of those books. But the seizure analysis that courts are starting to adopt seems to suggest just such a result.

Focusing on the right to exclude also suggests that individuals might retain that right even after sharing their data publicly. The right to destroy and the right to exclude do not evaporate just because an owner grants temporary access to his property.[100] Conceptualizing data retention as a seizure, then, might mean that the government could not retain copies of publicly released information, such as blog posts. Thus, because a blogger often retains ownership over his posts, he presumably could choose to delete the post, and could similarly request that the government delete its copies as well. The owner of the data would assert his right to exclusive possession, and the government intrusion on that right would accordingly render the duplication a seizure.[101] Such an understanding might well mean that the government could not collect and retain data posted publicly unless it first obtained a warrant. But such a rule, however sensible, is inconsistent with the understanding that the police can observe — and record — what takes place in public without implicating the Fourth Amendment.[102] This rule would apply similarly to a conversation in a public place: if recording that conversation counts as "seizing" it because the speaker has a right to exclude others from the information relayed, then the government presumptively needs a warrant to record it, even though the speaker has no reasonable expectation of privacy.

This analysis is not conclusive: a court might say that an individual gives up the right to exclude once he shares the data publicly, just as a court would say that the individual has given up any reasonable expectation of privacy by sharing his information.[103] But property law questions of these types might arise over and over again,[104] and a

---

[100] Recall Ohm's argument that *Hicks* was rightly decided because the defendant's right to delete evaporated upon exposure to the officer. *See supra* p. 1054–55.

[101] Though, the seizure might be reasonable: a court might consider the possessory interest weakened by the fact that the data had previously been widely shared.

[102] United States v. Knotts, 460 U.S. 276, 281–82 (1983).

[103] *See infra* section IV.C, p. 1067.

[104] One district court found that an individual had no "possessory interest" in metadata held by a third party, and accordingly found the data was not "seized" when the government copied it. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 30 n.41 (D.D.C. 2013), *vacated and remanded*, 880 F.3d 559 (D.C. Cir. 2015). As another example, the government argued in *Kyllo v. United States* that the defendant had "abandoned" the heat emanating from the home. *See* Transcript

court would have to consider whether, as to the particular information at issue, the individual actually has a right to exclusive possession.

III. DUPLICATION AS AN INFRINGEMENT OF PRIVACY

It may well be that duplications of certain data are seizures, but because the greater concern with duplications is the privacy violation, and because the seizure analysis might not cover all data, it makes more sense to identify duplication as a search. But duplication without actual review is not obviously a search — after all, if no person reviews the documents then perhaps there has been no invasion.[105] As Ohm argues, "the government has a reasonable argument that when it seals the collected data [after duplication], it stops short of invading or intruding on the data owner's privacy."[106] True enough, but the government also has a reasonable argument that when it leaves the original intact and in the owner's possession, it stops short of interfering with the owner's possessory interests. This is not to discard the critique entirely, but merely to emphasize that courts are in uncharted waters here and can draw the lines where they make the most sense.

A. Privacy and Duplications

Courts clearly recognize that it is privacy that is at stake in duplication,[107] which probably follows most people's intuition: we don't want the government to have copies of our files because we don't trust it not to read them. It therefore seems more natural to conceptualize

---

of Oral Argument at 47, Kyllo v. United States, 533 U.S. 27 (2001) (No. 99-8508), http://www.supremecourt.gov/oral_arguments/argument_transcripts/99-8508.pdf [http://perma.cc/52MA-NKP5]; Sarilyn E. Hardee, Note, *Why the United States Supreme Court's Ruling in* Kyllo v. United States *Is Not the Final Word on the Constitutionality of Thermal Imaging*, 24 CAMPBELL L. REV. 53, 61 (2001).

[105] *See, e.g.*, Susan Brenner, *Copying as a Seizure (Again)*, CYB3RCRIM3 (July 15, 2009, 6:31 AM), http://cyb3rcrim3.blogspot.com/2009/07/copying-as-seizure-again.html [http://perma.cc/8YJS-PPGD] (arguing that while defensible arguments support conceptualizing duplication as a search, they stretch the word "search" too far). The Second Circuit, in the metadata context, adopted a similar view without elaboration. *See* ACLU v. Clapper, 785 F.3d 787, 801 (2d Cir. 2015) (suggesting that metadata collection should be characterized as a seizure of data, rather than a search).

[106] Ohm, *supra* note 72, ¶ 53.

[107] Even the courts that conclude that duplication is a seizure emphasize the privacy interests at stake. For example, in *Ganias*, the Second Circuit panel characterized its challenge as "adapt[ing] traditional Fourth Amendment concepts" to the modern era "[b]ecause the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology." United States v. Ganias, 755 F.3d 125, 134 (2d Cir. 2014), *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015). In *Metter*, the court emphasized that a data owner has "identical privacy concerns with the government's retention of the imaged document." United States v. Metter, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012). And in *Jefferson*, the court noted that "the Fourth Amendment privacy interest extends . . . to the information" itself, United States v. Jefferson, 571 F. Supp. 2d 696, 702 (E.D. Va. 2008), and that "taking notes or photographs necessarily diminishes the privacy value of information once privately-held," *id.* at 703.

duplication as an invasion of privacy — and therefore a search — than as an invasion of possessory interests. And, despite some lower courts' characterization of duplication as a seizure, the Court's doctrine strongly suggests that duplication is indeed a search. Recall that, under *Katz* (as filtered through the years), a search is an action that violates an individual's "reasonable expectation of privacy."[108] Accepting Westin's definition of privacy as control over information,[109] it is an easy step to say that duplication interferes with an individual's reasonable expectation of control over personal information.

Given the focus in *Jefferson*, *Metter*, and *Ganias* on privacy, the conclusion in those cases that duplication was a seizure is somewhat surprising. Indeed, the *Ganias* panel, for example, parroted Westin's definition of privacy when it proclaimed that the retention was an interference with the owner's "control over [his] files."[110] These cases nonetheless found an infringement on property rights, and then concluded that a seizure had occurred. But searches are often defined in relation to property law. And as the Court elaborated in *Rakas v. Illinois*,[111] the fact that an individual can exclude others strongly suggests that the individual has a reasonable expectation of privacy.[112] This conception is consistent with Justice Harlan's discussion in *Katz*, which recognized that although the decision departed from the original trespass inquiry, it ultimately concluded by reference to places.[113] Thus, a court having recognized the *privacy* interests at stake then might, and indeed should, consider whether tenets of property law suggest that an individual would have a reasonable expectation of privacy in that context.[114] The Court's second test for whether or not a search has occurred, advanced in *United States v. Jones*[115] and *Florida v. Jardines*,[116] asks whether "'the Government obtain[ed] information by physically intruding' on persons, houses, papers, or effects."[117] In *Jones*, Justice Scalia applied founding-era trespass principles to the government's placement of a GPS device on a defendant's car to classify it as a search.[118] This reasoning promotes the underlying purpose

---

[108] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); *see also* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

[109] WESTIN, *supra* note 42, at 7.

[110] *Ganias*, 755 F.3d at 137.

[111] 439 U.S. 128 (1978).

[112] *See id.* at 149; *see also id.* at 143 n.12.

[113] *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *see also* Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 8 (2009).

[114] *See, e.g.*, Oliver v. United States, 466 U.S. 170, 183 (1984) ("The existence of a property right is but one element in determining whether expectations of privacy are legitimate.").

[115] 132 S. Ct. 945 (2012).

[116] 133 S. Ct. 1409 (2013).

[117] *Id.* at 1414 (quoting *Jones*, 132 S. Ct. at 950 n.3).

[118] *Jones*, 132 S. Ct. at 949–50, 953.

of the Fourth Amendment search restrictions, to protect the "right of the people to be secure," to protect, that is, individual privacy. Property law principles, then, can operate as a shortcut for determining whether an invasion of privacy — a search — has occurred.

In *Ganias*, for example, the panel focused on the infringement of the individual's right to exclude others from his property. But this infringement does not necessarily result in the action being a seizure. In *Jones*, the Court did *not* find that the government had "seized" the defendant's car by placing a GPS tracker on it — even though this interfered with the defendant's right to exclude others from his property.[119] Instead, the Court viewed violation of the right to exclude as evidence to support its conclusion that a search had occurred.[120] In the digital context, then, the property law analogues are useful in determining whether a *search* occurred, either under the trespass test[121] or because they illuminate the reasonableness of expectation of privacy.[122]

There are two complications to this conception, however. First, in *United States v. Karo*,[123] the Supreme Court explicitly rejected the notion that "potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment."[124] Second, if duplication of data is an invasion of privacy because of the *potential* that the government will read it, then many actions currently classified as seizures also become searches. If the government seizes a filing cabinet without opening it, for example, then risks to the privacy of the cabinet's contents still attach. These hurdles should be cleared, though, by recognition that duplication does not just *risk* violation, but is in fact *itself* a violation of privacy, because duplication inherently reduces one's ability to control her information.

In *Karo*, the police had given to the defendant a can of ether containing a hidden tracking device.[125] The Court ruled that this delivery did not constitute a search because the beeper was "unmonitored" at that time.[126] Kerr argues that this holding indicates that a search has not occurred until the data is observed by an actual person.[127] But additional language in *Karo* calls this conclusion into question: "It is the exploitation of technological advances that implicates the Fourth

---

119 *See id.* at 949; *id.* at 958 (Alito, J., concurring in the judgment) ("The Court does not contend that there was a seizure.").

120 *Id.* at 949 (majority opinion).

121 *See Jardines*, 133 S. Ct. at 1414 (noting that a "search" occurs when government "obtains information" by invading a constitutionally protected place (quoting *Jones*, 132 S. Ct. at 950 n.3)).

122 *See* Rakas v. Illinois, 439 U.S. 128, 149 (1978).

123 468 U.S. 705 (1984).

124 *Id.* at 712.

125 *Id.* at 708.

126 *Id.* at 712.

127 *See* Kerr, *supra* note 11, at 554.

Amendment, not their mere existence."[128] Indeed, what the Court meant by "unmonitored" was not that no one was actually reviewing the data at that time, but rather that the device was not passing any information to the police.[129] The Court did not address, for example, the government's recording location data and then viewing it later. In that situation, the government would have been "exploiting" the technology immediately, even if an actual person did not immediately review it. As soon as the data — personal information about movements — is recorded, the individual has lost control over that information.

Similarly, in *Kyllo*, the Court ruled that a police officer who had used a thermal imager to measure heat radiating from a house had performed a search.[130] But if the technology had not immediately relayed that information to the officer — if the officer had needed to return to the station to analyze the data collected — the search would still have occurred upon collection rather than review. Once the data is recorded, the information is beyond the control of the data owner.

These situations are analogous to digital duplication in that the invasion of privacy happens at the time of collection or duplication, not only upon later review. Duplication of private information is an active — though often automated — process, done at the direction of the government agent. A duplication is itself an "exploitation of [a] technological advance[]."[131]

By contrast, when the government seizes a filing cabinet,[132] it has not yet directed anything at the information within. This may mean that seizing a filing cabinet is not also a search of its contents. Only when the government directs its technology at an individual's private information does it invade that individual's reasonable expectation of privacy and accordingly perform a search. On the other hand, perhaps we *should* consider the seizure of a filing cabinet as also a search of its contents — this action plainly should be subject to Fourth Amendment review, and there is no pressing reason to reject a "belt and suspenders" approach when both privacy and possessory interests are infringed. Thus, neither the Court's seemingly limiting language in *Karo* — that "potential" invasions do not implicate the Fourth

---

128 *Karo*, 468 U.S. at 712.

129 *Id.* (noting that the beeper "conveyed no information that Karo wished to keep private, for it conveyed no information at all").

130 Kyllo v. United States, 533 U.S. 27, 40 (2001).

131 *Karo*, 468 U.S. at 712. Relying on the analogy of the government digitally "rooting around" illustrates some of the problems with extending nondigital concepts to the digital world. *See* Brenner, *supra* note 105. Although the idea is appealing, the results are less so. *Cf.* TRON (Walt Disney Productions 1982).

132 *Cf.* United States v. Chadwick, 433 U.S. 1 (1977) (finding that police needed a warrant to open — search — a lawfully seized footlocker).

Amendment — nor the implication that certain seizures may also be searches undermines the classification of duplications as searches.

B. Retention

One might, then, view the act of duplication as a search, and duplication and subsequent retention as a "search and seizure."[133] This approach seems natural because, if the government "possesses" something, it must have seized it. But, as mentioned above, such logic reverses the Fourth Amendment seizure inquiry, which focuses not on whether the government possesses something, but rather on whether the government's action was a "meaningful interference with an individual's possessory interests."[134] Thus, it is at least ambiguous whether retention constitutes a seizure.[135]

But retention likely is a search. In *Klayman v. Obama*,[136] for example, the district court held that bulk metadata collection efforts constituted a search.[137] While several factors contributed to the court's conclusion, the retention of data was itself considered a part of the Fourth Amendment search.[138] The court ordered the government not to stop its analysis of the data, but rather to "destroy any such metadata in its possession."[139] The retention is itself an ongoing violation of privacy — in fact, copying without retention is not much of a violation of privacy at all.[140]

One feature of Fourth Amendment search jurisprudence is the inability, once a search is completed, to revoke consent.[141] Thus, if an individual consents to duplication of his data, he may not be able to revoke that consent once the copying is complete.[142] This anomaly makes viewing data retention as a seizure appealing to civil libertarians because such a conception would allow the data owner to rescind

---

133 *Cf.* Katz v. United States, 389 U.S. 347, 354 (1967) (characterizing the recording and listening to of private conversations as a "search *and* seizure" (emphasis added)); Berger v. New York, 388 U.S. 41, 54 (1967) (same).

134 United States v. Jacobsen, 466 U.S. 109, 113 (1984).

135 *See supra* section II.B, pp. 1056–59.

136 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

137 *Id.* at 32.

138 The court found that the plaintiffs had no "possessory interest" in metadata held by a third party, and accordingly found no seizure. *See id.* at 30 n.41. This result illustrates the limits of the possessory interest framework discussed above in section II.B.

139 *Id.* at 43.

140 Though it may still be a search, duplication without retention is probably de minimis or otherwise reasonable. *See infra*, section IV.B, pp. 1066–67.

141 *See, e.g.*, United States v. Lattimore, 87 F.3d 647, 651–52 (4th Cir. 1996).

142 The same would result if the initial copying were authorized by warrant or a warrant exception: if the search ends when the copying is complete, the government would need no further justification for retaining the data.

consent and recover sole possession of her data at any time.[143] But because copying and continued retention of the data each interfere with control over personal information, each is a search. When consent is revoked, therefore, the ongoing retention must end.

On the other hand, if duplication is a seizure because it interferes with the right to delete[144] or exclusive possession,[145] then the protection would not extend to information the individual doesn't own. Movies, for example, to which the hard drive owner has no right to exclusive possession, might be excluded from any seizure analysis.[146] Yet even if an individual has no claim to exclusive ownership, she does have a privacy interest in her files — including keeping private the information that reveals *what* movies, music, or books she owns. By viewing data retention as a search instead of a seizure, the individual can demand deletion because she retains a reasonable expectation of privacy in that information, whether or not she "owns" it.

Because privacy refers to an individual's control over information, and retention interferes with that control, retention is an invasion of privacy, and thus a search. The consequence of the government possessing a copy is exactly the same: a loss of control over the data.

IV. Consequences of the Search Designation

Several consequences flow from identifying duplication and retention as a search, rather than a seizure. For example, as discussed above, consent, and more particularly the right to revoke consent, plays a different role in searches than in seizures. In addition, the different nature of government intrusion affects both the reasonableness analysis and the de minimis analysis. Finally, classifying duplication as a search has different implications for data that has been shared publicly. This Part examines these additional consequences in turn.

A. Duplications and Reasonableness

The Fourth Amendment prohibits only *unreasonable* searches and seizures. Duplicating information might be a search, but that conclusion does not necessarily render the action a violation of the Fourth Amendment. Rather, it merely subjects the action to Fourth Amendment reasonableness analysis. The reasonableness of a search is determined by weighing "the degree to which it intrudes upon an indi-

---

143 *See* Taticchi, *supra* note 21, at 483–84.

144 *See* Ohm, *supra* note 20, at 11–12; Ohm, *supra* note 72, ¶¶ 61–67.

145 *See* United States v. Ganias, 755 F.3d 125, 137 (2d Cir. 2014), *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015); *see also* Taticchi, *supra* note 21, at 496.

146 *See supra* pp. 1057–58.

vidual's privacy" against "the degree to which it is needed for the promotion of legitimate governmental interests."[147]

Because the privacy interest violated can vary with the government's use of the data, courts can more easily conduct reasonableness balancing when the government asserts a need for the data for some purpose other than as evidence. Recall that in *Ganias* the government argued it might need to retain nonresponsive data for authentication purposes.[148] If retention of data is a seizure, then the individual's interest is binary: her right to delete or exclude is fully infringed regardless of the purpose for which the government retains her data. The individual-interest side of the balance varies only with the length of time of the infringement.[149] Thus, in *Ganias*, for example, the individual's side of the balance contained only the right to exclusive possession infringed by ongoing retention, regardless of what the government did with the data: whether the government used the data for authentication, as evidence in the initial contract fraud prosecution, or as evidence in the subsequent tax fraud prosecution, the infringement on Ganias's possessory interests was the same.

If the retention is a search, however, then the individual's interest more naturally varies with the government's use of the data. Thus, a court could recognize the data retention as a search, but find that it is reasonable so long as it is for the limited purpose of authentication. Retention for any other purpose might be unreasonable because of the correspondingly greater infringement on privacy interests, and thus any evidence obtained from an unreasonable use of the duplicated data could be subject to the exclusionary rule.[150]

In *Riley*, the government argued that it might need to search a cell phone immediately out of concern that the data could be remotely deleted.[151] The Court was unconvinced, citing the availability of technology that could stop remote deletion.[152] Another approach to the deletion concern might be digital duplication of the phone's contents. Under the analysis laid out in this Note, this duplication would plainly be a search. But the flexibility of the search "reasonableness" analysis applies with equal force here. *Merely* copying a phone to preserve it from remote wiping, pursuant to the exigent circumstance of imminent

---

147 Wyoming v. Houghton, 526 U.S. 295, 300 (1999).

148 *See Ganias*, 755 F.3d at 139.

149 *See* United States v. LaFrance, 879 F.2d 1, 6 (1st Cir. 1989). As that court noted, the "nature and extent" of the intrusion matter as well. *Id.* (quoting United States v. Place, 462 U.S. 696, 705 (1983)). But in the duplication-as-seizure context, that "nature" is already defined as the infringement on the right to exclude or delete, and thus the "intrusiveness" of the duplication, conceived as a seizure, varies only with the length of time of the infringement.

150 *Cf. Ganias*, 755 F.3d at 140–41 (applying exclusionary rule to unreasonable seizure of data).

151 Riley v. California, 134 S. Ct. 2473, 2486 (2014).

152 *Id.* at 2487.

deletion, might be a reasonable search. Because the invasion of privacy is less than when the officer actually examines the phone's contents, the government's countervailing interest in preserving the data might render the action reasonable. But the extent of the interference with privacy also varies, like a seizure, with the length of time of the interference. The longer the information is out of the individual's control, the greater the interference. Thus, at a certain point, the warrantless retention of the copy would become unreasonable.

Of course, classifying duplication as a search, rather than as a seizure, may not affect the ultimate outcome of the reasonableness analysis in this context. If duplication is a seizure because it interferes with the right to exclusive possession, it may still be reasonable to make a seizure to prevent remote wiping. The key difference, though, is that the infringement on exclusive possession varies only with the length of the infringement. In a close case, what the government does with the duplicated data that it has reasonably seized does not affect the reasonableness of the seizure. Once the government interests overcome the invasion of the right to exclusive possession, any subsequent action doesn't alter this fundamental balancing.[153]

B. De Minimis Searches

As Kerr explains, a computer, in the course of its normal function, must make copies for internal use. If this internal duplication is a search, it would presumptively require a warrant.[154] But preexisting concepts in search jurisprudence mitigate this concern. The copying that is intrinsic to computer use could be conceived of as a de minimis violation that is either no intrusion at all, or such a minor violation that it is presumptively reasonable.[155] Because such internal copying is temporary, never subject to the computer user's control, and never even at risk of exposure, it can easily be considered de minimis. If it interferes with the data owner's control over his information, this interference is small and temporary. This type of copying, even if it should be considered a "search" insofar as it is directed at private information, is a reasonable search given the low level of violation and

---

[153] Orin Kerr presents a slightly different take, at least in the context of subsequent searches of nonresponsive data, as occurred in both *Ganias* and *CDT*. *See* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 29–32 (forthcoming 2016). Kerr argues that the subsequent use of nonresponsive data obtained in the execution of an initial warrant converts that first warrant into a general warrant. *Id.* at 31. He does not apply the traditional reasonableness balancing test, but instead relies on the Warrant Clause. *See* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but . . . particularly describing the . . . things to be seized.").

[154] *See* Kerr, *supra* note 11, at 551.

[155] *Cf.* Jeffrey Brown, *How Much Is Too Much? The Application of the* De Minimis *Doctrine to the Fourth Amendment*, 82 MISS. L.J. 1097, 1109 (2012).

its necessity to the operation of a computer. The same analysis might also apply, of course, in the seizure context: the impingement on the right to exclude is so temporary that it may be a de minimis seizure.

C. Publicized Information

As discussed above in section II.B, classifying duplication and retention as a seizure might mean that the government could not retain copies of publicly released information, such as blog posts. By viewing data duplication and retention as searches, though, the government *could* retain publicly posted information without a warrant. This is so because, by posting them in a public forum, the blogger loses any reasonable expectation of privacy.[156] That is, by sharing the information with the world, the individual gave up control. To obtain this information from the Internet, the government need not commit any violations of property law, such as trespass, which might otherwise suggest that the data owner retained a reasonable expectation of privacy. Thus, collection of such data would not constitute a search at all and would not be subject to the requirements of the Fourth Amendment. While there might be reasons to limit broad electronic trawling of the public Internet, they cannot be located in the Fourth Amendment.

CONCLUSION

The Fourth Amendment protects people from two things: unreasonable seizures and unreasonable searches. It is important to recognize these as distinct protections lest the value of the protections deteriorate. A seizure is best viewed as a dispossession of property, and a search as an invasion of privacy. There may well be times when these two overlap, and often a seizure will include risks to privacy. Viewing collection of data only as a seizure would dramatically reduce the Fourth Amendment's protections over vast amounts of personal, private information in which the individual may have no cognizable property interests. The government could conceivably collect private information that does not have a property component — such as the heat signatures in *Kyllo* or the titles of the books in private libraries — with impunity as long as it doesn't review the data. Instead, we should recognize these invasions of privacy, reviewed by a government agent or not, for what they are: Fourth Amendment searches.

---

[156] *Cf.* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").