FOURTH AMENDMENT — SEARCH AND SEIZURE AND EVIDENCE RETENTION — SECOND CIRCUIT CREATES A POTENTIAL "RIGHT TO DELETION" OF IMAGED HARD DRIVES. — *United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014).

One of the most pressing challenges facing the legal world today is the application of constitutional law to rapidly evolving technology — particularly the application of the Fourth Amendment protection from unreasonable search and seizure to the digital frontier.[1] The Fourth Amendment was drafted primarily with physical property in mind,[2] to protect against general warrants "not limited in scope and application."[3] When executing warrants today, the standard approach in seizing electronic data is the creation of an identical read-only copy of the computer's contents called a forensic mirror image.[4] However, such evidence collection standards have generated a host of constitutional questions, centering on "how to limit the invasiveness of computer searches to avoid creating the digital equivalent of general searches."[5]

Recently, in *United States v. Ganias*,[6] the Second Circuit held that the government's retention of files outside the scope of a warrant from lawfully imaged hard drives for over two and a half years violated the Fourth Amendment.[7] While the reasoning behind this decision seems sound and intuitive when viewed against Fourth Amendment requirements regarding physical property, the opinion raises concerns about the evidentiary chain of custody;[8] as a result, the opinion risks creating a "right to deletion,"[9] which could unnecessarily complicate criminal prosecutions.

---

1 *See, e.g.*, Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

2 *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 313 (1972).

3 Maryland v. King, 133 S. Ct. 1958, 1980 (2013) (Scalia, J., dissenting); *accord* Kerr, *supra* note 1, at 536 ("General warrants permitted the King's officials to enter private homes and conduct dragnet searches for evidence of any crime.").

4 *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 (Aspatore 2013), 2013 WL 3759817, at *2 (offering a background on the standard procedures of digital forensics). Such sweeping data collection is constitutionally justified by the practical need to find files in the depths of a hard drive, akin to "intermingled documents" in a wholesale seizure. *Cf.* United States v. Tamura, 694 F.2d 591, 595–96 (9th Cir. 1982).

5 Kerr, *supra* note 1, at 535.

6 755 F.3d 125 (2d Cir. 2014).

7 *Id.* at 127–28.

8 This comment uses the terms "chain of custody" and "authentication" interchangeably to refer to the process of verifying the integrity of digital evidence.

9 Throughout this comment, the "right to deletion" refers to an individual's right to have the government delete electronic evidence that is nonresponsive to a search warrant and the government's responsibility to do so within a reasonable amount of time. This usage varies somewhat from some other legal scholarship. *See, e.g.*, Andrea M. Matwyshyn, *Privacy, the Hacker Way*, 87 S. CAL. L. REV. 1, 63–64 (2013) (proposing a statutory "right of deletion" for consumers' data after

In 2003, the Army launched an investigation into alleged "improper conduct" by an Army contractor, Industrial Property Management (IPM).[10] As part of the investigation, the Army obtained a warrant to seize materials from Stavros Ganias, IPM's accountant.[11] The warrant authorized the seizure of all "books, records, documents, materials, computer hardware and software and computer associated data relating to . . . [IPM]."[12] When the warrant was executed, the Army's computer specialists made forensic mirror images of all three of Ganias's computers.[13] "[T]he investigators were careful . . . to review only data" within the scope of the warrant.[14] However, they did not purge or delete the files that did not pertain to IPM and that were therefore "non-responsive" to the warrant.[15]

In late 2004, IRS investigators discovered accounting irregularities in the paper documents from Ganias's office.[16] The government then expanded its investigation of Ganias to include possible tax violations and discovered evidence that Ganias had improperly reported income for his clients, and perhaps for himself.[17] The IRS case agent sought to review Ganias's personal financial records, and although she knew they were stored on the government copies of Ganias's computers, did not believe she could properly review them as they were outside the scope of the 2003 warrant.[18] Ganias and his counsel did not respond to a request to access these files, and subsequently, the government obtained a warrant in April 2006 to search the preserved files of Ganias's personal financial records from 2003.[19]

In October 2008, Ganias was indicted by a grand jury for conspiracy and tax evasion.[20] In February 2010, Ganias sought to suppress the evi-

---

contract termination); Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. F. 10, 17–18 (2005) (using the term to refer to a right that a data owner could rely upon to compel the government to delete seized imaged hard drives); John Palfrey, *The Public and the Private at the United States Border with Cyberspace*, 78 MISS. L.J. 241, 291–92, 291 nn.138–39 (2008) (discussing the "right to demand deletion" suggested by Ohm and other scholars).

10 *Ganias*, 755 F.3d at 128.

11 *Id.*

12 *Id.*

13 *Id.*

14 *Id.* at 129.

15 *See id.*

16 *Id.*

17 *Id.*

18 *Id.*

19 *Id.* at 130. It was later discovered that Ganias had altered his computer files after the original seizure in 2003 and therefore the financial records "would not have existed but for the Government's retention." *Id.* However, the government conceded that it never considered retaking the files from Ganias himself. *Id.* at 139.

20 *Id.* at 130. James McCarthy, Ganias's client and the owner of IPM, was also indicted. *Id.* In December 2009, the grand jury returned a superseding indictment with counts against McCar-

dence obtained as a result of the 2006 warrant,[21] arguing that the data outside the scope of the 2003 warrant were held for an unreasonable amount of time and should have been returned.[22] In April 2010, the U.S. District Court for the District of Connecticut denied the motion on the grounds that the data were seized pursuant to a valid warrant by "means less intrusive to the individual . . . than other means . . . authorized."[23] On April 1, 2011, the jury convicted Ganias on both counts of tax evasion.[24] Ganias moved for a new trial on the basis of alleged jury misconduct, but the district court denied the motion[25] and later sentenced Ganias to twenty-four months' imprisonment.[26]

The Second Circuit reversed the denial of the motion to suppress, vacated Ganias's conviction, and remanded for further proceedings.[27] Writing for the panel, Judge Chin[28] framed the question before the court as "whether the Fourth Amendment permits officials executing a warrant for the seizure of particular data on a computer to seize and indefinitely retain every file on that computer for use in future criminal investigations."[29] He answered that it did not.[30] The decision rejected each of the government's five arguments that there was legal authority for its indefinite retention of the computer files nonresponsive to the 2003 warrant. First, the claimed practical necessity of creating hard drive mirror images did "not justify the indefinite *retention* of non-responsive documents," and without a warrant for Ganias's personal records, copies of such records could not be regarded as government property without violating the Fourth Amendment.[31] Second, obtaining the 2006 warrant did not cure any defect in searching the

---

thy and Ganias related to McCarthy's taxes, as well as two counts solely against Ganias relating to his personal taxes. *Id.*

[21] *Id.*

[22] United States v. Ganias, No. 3:08CR00224, 2011 WL 2532396, at *6 (D. Conn. June 24, 2011). In this case, "return" would essentially mean deletion given the nature of the seized evidence — copies of Ganias's files stored on government-owned hard drives.

[23] *Id.* at *8. Ganias also challenged the 2003 warrant on the basis that seizing the entirety of his hard drives via mirror images effected a general warrant. *Id.* at *9. The district court rejected this argument, noting the particularity of the warrant and practical realities of searching electronic storage devices. *Id.* at *9–10.

[24] *Ganias*, 755 F.3d at 130. The district court had previously severed the tax evasion counts relating to Ganias's personal taxes from the other charges. *Id.*

[25] United States v. Ganias, No. 3:08CR00224, 2011 WL 4738684, at *1 (D. Conn. Oct. 5, 2011).

[26] *Ganias*, 755 F.3d at 131.

[27] *Id.* at 141.

[28] Judge Chin was joined by Judge Restani of the United States Court of International Trade, sitting by designation.

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

[30] *Id.* Judge Chin also rejected the argument that Ganias's right to a fair trial was violated by one juror's use of social media, relying primarily upon the district court's finding that the juror in question "deliberated impartially and in good faith." *Id.* at 132.

[31] *Id.* at 138 (emphasis added).

wrongfully retained files.[32] The opinion analogized the breadth of data obtained from an imaged hard drive to a sweeping seizure of paper documents and determined that allowing retention until probable cause was found would essentially transform every warrant into a general warrant.[33] Third, the fact that Ganias had since altered the original files did not justify the government's actions; Fourth Amendment considerations "embod[y] a judgment that some evidence of criminal activity may be lost for the sake of protecting property and privacy rights."[34] Fourth, in response to the government's argument that returning or deleting the nonresponsive files would leave the remaining data impossible to authenticate, the court wrote that it was "not convinced that there is no other way to preserve the evidentiary chain of custody."[35] Finally, Ganias's failure to bring a motion for the return of property did not preclude suppression.[36] Thus, finding that the police had violated the Fourth Amendment by searching the retained files and further finding that the exclusionary rule applied, the court held that the lower court erred in denying Ganias's motion to suppress and vacated his conviction accordingly.[37]

Judge Hall concurred in part and dissented in part. Judge Hall agreed that the government's retention of nonresponsive files without some independent basis for an extended period of time was an unreasonable seizure.[38] However, he dissented from the portion of the opinion holding that the evidence should be suppressed.[39] He found that the government had complied with what little case law existed at the time of the search, and therefore did not act in bad faith.[40]

While copying computer files is generally viewed as a seizure, courts and scholars have debated the proper procedures that the government should use and the extent of the protections that defendants

---

[32] *Id.* at 138–39.

[33] *Id.*

[34] *Id.* at 139.

[35] *Id.*

[36] *Id.* Federal Rule of Criminal Procedure 41(g) allows for a motion to return property, but such a motion is not required as a "prerequisite" for a motion to suppress generally, as the court noted. *Id.*; *see also* FED. R. CRIM. P. 41. The opinion also emphasized that Ganias did not need the files returned, but merely deleted, as they were copies. *Ganias*, 755 F.3d at 139.

[37] *See Ganias*, 755 F.3d at 139–41. The court held that the exclusionary rule applied here because the government's widespread seizure was not covered by the warrant, the agents did not act in good faith, the benefits of deterring such police conduct were great, and the costs of suppression were minimal. *Id.* at 140–41.

[38] *Id.* at 141 (Hall, J., concurring in part and dissenting in part).

[39] *Id.*

[40] *Id.* at 142. Further, Judge Hall wrote, the balance between deterrence and the cost of suppression was miscalculated by the majority opinion as the evidence here was irreplaceable and, because of the serious effects of white-collar crime, the defendant could be considered dangerous. *Id.*

should be afforded.[41] The decision in *Ganias* highlights some of the difficulties in determining these details. Although the court properly found that Ganias's Fourth Amendment rights had been violated, the decision failed to appreciate the importance of authentication requirements for electronic evidence. As a result, *Ganias* may unnecessarily complicate prosecutions by potentially creating a perceived "right to deletion" — a prescription that federal prosecutors must delete files nonresponsive to a warrant sooner rather than later.[42] The court could have avoided any potentially burdensome effects of this prescription on the evidentiary authentication process had it issued a more narrow ruling merely suppressing the evidence.

The *Ganias* court's opinion properly held that Ganias's Fourth Amendment rights were violated, and it rightly recognized the importance of the particularity requirement[43] in the context of electronic evidence. A hard drive contains detailed personal information including correspondence, lists of associates, web history, and financial information. Forensic investigators can also often recover deleted files as well as use "metadata," a host of associated data detailing when and how a computer was used, to discover a wealth of additional information and reconstruct the development of a file.[44] The opinion reflects the fear that the government could retain a defendant's files indefinitely, and then much later, when probable cause is finally developed, obtain a search warrant, causing every warrant for specific electronic data to "become, in essence, a general warrant."[45] The court expressed very real concerns that allowing the actions of the government in a case like this would essentially "reduce[] the Fourth Amendment to a form of words."[46]

But the court may have gone further than necessary in safeguarding this constitutional interest. The decision in *Ganias* stated that the gov-

---

[41] *See id.* at 135 (majority opinion) ("These Fourth Amendment protections apply to modern computer files. . . . If anything, even greater protection is warranted.") (citing United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013); United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009)); *see also* Kerr, *supra* note 1, at 548–57 (discussing at what stage of examining or copying files on a computer a search should be held to occur).

[42] *See* Orin Kerr, *Commentary on the* Ganias *Case*, WASH. POST: VOLOKH CONSPIRACY (June 24, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/24/commentary-on-the-ganias-case [http://perma.cc/9LK2-KL97]; Orin Kerr, *Court Adopts a Fourth Amendment Right to the Deletion of Non-Responsive Computer Files*, WASH. POST: VOLOKH CONSPIRACY (June 18, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/18/court-adopts-a-fourth-amendment-right-to-the-deletion-of-non-responsive-computer-files [http://perma.cc/W72H-PC65].

[43] The "particularity requirement" of the Fourth Amendment limits the scope of searches by obligating warrants to specify exactly what is being searched and where it is being searched. *See* U.S. CONST. amend. IV.

[44] *See, e.g.*, Kerr, *supra* note 1, at 542–43.

[45] *Ganias*, 755 F.3d at 139.

[46] *Id.* at 138 (quoting Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920)) (internal quotation marks omitted).

ernment is not authorized to "retain all non-responsive documents indefinitely."[47] This has led some commentators to note that the court created an implied "right to deletion" that has potentially broad implications, particularly in relation to the evidentiary chain of custody.[48] Such a reading is supported by sweeping language that appears at times throughout the majority opinion indicating that the retention itself, rather than the specific use of the retained data by the government, may have been an issue for the court.[49] Although it is unclear from the opinion *exactly* when such data must be deleted, the court's opinion could be read to suggest that nonresponsive data must be deleted sooner rather than later.

However, such a prescription threatens the authentication process. Upon execution of a warrant for electronic data, the government copies the entire hard drive before segregating the responsive files.[50] The *Ganias* court acknowledged this practical reality of electronic forensic analysis, stating that it would be both "impractical" and "unnecessary" for the government not to use off-site analysis via mirror imaging.[51] After collecting a hard drive image, the data must be authenticated for it to be admissible under current procedural rules.[52] "Hash values," strings of characters described as "digital fingerprints," are the best method of verifying that the copied files are identical and unaltered.[53] Forensic examiners calculate the hash value of the entire original drive and then compare it to the hash value of the entire image, or copy, they have created.[54] Hashing also permits vast quantities of data to be

---

[47] *Id.* at 140.

[48] *See* sources cited *supra* note 42.

[49] *See, e.g.*, *Ganias*, 755 F.3d at 128 ("We . . . hold that the Government's retention of the computer records was unreasonable."). The opinion also directly dismisses the government's argument regarding the impracticalities of returning or destroying nonresponsive data due to evidence authentication concerns. *Id.* at 139. Judge Hall's opinion also indicates that the majority is calling for a "right to deletion," writing: "I agree that the Government violated the defendant's Fourth Amendment rights to be free from an unreasonable seizure because it held for a prolonged period of time mirror images of computer-generated records that were not responsive to the 2003 search warrant *without returning them (or destroying them)* . . . ." *Id.* at 142 (Hall, J., concurring in part and dissenting in part) (emphasis added).

[50] There are several other ways of acquiring the sought-after files, but every alternative to hard-drive imaging comes with serious setbacks that outweigh its practical usefulness. *See* Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. PITT. J. TECH. L. & POL'Y 2, 7–12 (2007).

[51] *Ganias*, 755 F.3d at 135.

[52] *See* FED. R. EVID. 901(a).

[53] *See* Carlson, *supra* note 4, at 20, 2013 WL 3759817, at *2. The chances of different pieces of digital evidence having the same hash value is 1 in 18,446,744,073,709,551,616 — one is actually more likely to meet someone with identical fingerprints. *Id.* Hash results are also irreversible — that is, one cannot use the hash values to recreate the data on the hard drive. *See* GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE 55 (2008).

[54] Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 40 (2005). Salgado also mentions how the initial hash value is used as a "touchstone" for authenticating further digital forensics images when necessary. *See id.*

verified efficiently: for example, a hard drive containing 200 gigabytes of information — the equivalent of millions of pages — can be reduced to a hash value that can be printed on two lines of a page.[55] This method allows the entire hard drive to be authenticated at the highest standard and guarantees protection from evidence tampering, while only minimally intruding on any defendant's privacy interest.[56]

Any alteration to an imaged hard drive, no matter how minor, changes the hash value,[57] rendering it useless as a means of proving that the drive's contents, including responsive files, were not altered at any point. Requiring police to delete all nonresponsive files on a copied hard drive would change the hash value, and, in turn, open the government to a host of challenges on the authenticity of its electronic evidence.[58] The Department of Justice manual on these issues describes common challenges to the authenticity of electronic evidence, the most common concern being the possibility of alteration.[59] Reliability challenges have been a well-documented issue with electronic evidence since the beginning of its use in criminal proceedings, as electronic evidence is susceptible to error at every stage of processing.[60] Whereas hash values can efficiently authenticate digital evidence to what is essentially a certainty, all available alternatives are subject to some sort of vulnerability, and thus, challenges to authenticity.[61]

---

[55] PAUL, *supra* note 53, at 55.

[56] Salgado, *supra* note 54, at 42–43; *see also* Zachariah B. Parry, Note, *Digital Manipulation and Photographic Evidence: Defrauding the Courts One Thousand Words at a Time*, 2009 U. ILL. J.L. TECH & POL'Y 175, 197–201 (describing methods of authentication of digital photographs and discussing the "guarantee" that the evidence was not tampered with that hashing provides, *see id.* at 200).

[57] Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 BERKELEY TECH. L.J. 1227, 1234 (2004) ("If even one bit of data is altered — say, one space of text is added — the hash value would change."); *cf.* Salgado, *supra* note 54, at 39 ("If one altered . . . [a] photo by changing so little as one bit, the hash value of the photo would be different as well.").

[58] Federal prosecutors do have other options, but those methods mostly rely on an authenticating witness. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 198–200, 202 (3d ed. 2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [http://perma.cc/6SCV-QDJE]. However, such methods would generally be unavailable in cases like *Ganias*, where the Fifth Amendment protects the only possible authenticating witness (the defendant) from being compelled to testify.

[59] *Id.* at 202. This manual offers only two methods that seem safe from claims of alteration: hashing and physical retention of a defendant's hard drive. *Id.* at 199. The latter is more invasive to a defendant, and also presents the same problem with government retention of nonresponsive files that was at issue in *Ganias*.

[60] *See* Robert García, *"Garbage In, Gospel Out": Criminal Discovery, Computer Reliability, and the Constitution*, 38 UCLA L. REV. 1043, 1073 (1991) (outlining eight major ways that reliability problems may arise).

[61] *See, e.g.*, Ralph C. Losey, *Hash: The New Bates Stamp*, 12 J. TECH. L. & POL'Y 1, 26 (2007) ("Hash not only protects litigants from unscrupulous or negligent adversaries or experts who might try to alter computer files, it also allows both producers and recipients of productions to

Ganias's potentially burdensome effect could have been avoided entirely if the Second Circuit had issued a narrower opinion more in line with previous decisions.[62] In addressing authentication concerns, the court indicated it was "not convinced" there was no other way to authenticate digital evidence, but went on to write that "even if we assumed it were necessary to maintain a complete copy of the hard drive solely to authenticate evidence responsive to the original warrant, that does not provide a basis for using the mirror image for any other purpose."[63] It is precisely this limited purpose that the court could have explicitly reserved, allowing the retention of data to be used for authentication, but not in subsequent searches, as the government attempted in *Ganias*. Under this rule, the government would have been prohibited from searching the nonresponsive files on its imaged hard drive, including the files sought in the 2006 warrant, and in order to access those files would have needed to seize them directly from Ganias again.

Such an alternative holding is consistent with evidentiary rules and other precedent,[64] and would have addressed the court's concerns about general warrants without compromising the data authentication process. If, in fact, the "right to deletion" becomes the status quo, not only will the government's burden increase in that nonresponsive files will need to be deleted sooner rather than later, but the government will also face more challenges to the authenticity of its evidence in cases involving electronic data — burdens which simply seem unjustifiably imposed by what could have been a narrower ruling.

---

prove the original was not altered."); Marcia Hofmann, *Arguing for Suppression of 'Hash' Evidence*, THE CHAMPION, May 2009, at 20, 23 (advising defense attorneys against even attempting to argue that hash values are unreliable as indicia of authentication).

62 Prior cases addressing imaged hard drives specified that the government could seize data without ruling on whether nonresponsive files must be deleted within a certain time period, as Judge Hall noted in his separate opinion. *See Ganias*, 755 F.3d at 142 (Hall, J., concurring in part and dissenting in part) ("[T]here was little caselaw either at the time of the search or in the following years to indicate that the Government could not hold onto the non-responsive material in the way it did. Where caselaw existed, the Government complied with the guidelines for the seizure and offsite search of large amounts of documents." (citing United States v. Tamura, 694 F.2d 591, 595–96 (9th Cir. 1982))).

63 *Id.* at 139 (majority opinion).

64 *See* FED. R. CRIM. P. 41(e)(2)(B) ("A warrant . . . may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant . . . refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review."); *Ganias*, 755 F.3d at 135–36 (citing United States v. Schesso, 730 F.3d 1040, 1046 (9th Cir. 2013); United States v. Evers, 669 F.3d 645, 652 (6th Cir. 2012); United States v. Hill, 459 F.3d 966, 976–77 (9th Cir. 2006); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999)).