

THE FOURTH AMENDMENT RIGHT TO DELETE

*Paul Ohm**

Replying to Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

For years the police have entered homes and offices, hauled away filing cabinets full of records, and searched them back at the police station for evidence. In Fourth Amendment terms, these actions are entry, seizure, and search, respectively, and usually require the police to obtain a warrant. Modern-day police can avoid some of these messy steps with the help of technology: They have tools that duplicate stored records and collect evidence of behavior, all from a distance and without the need for physical entry. These tools generate huge amounts of data that may be searched immediately or stored indefinitely for later analysis. Meanwhile, it is unclear whether the Fourth Amendment's restrictions apply to these technologies: Are the acts of duplication and collection themselves seizure? Before the data are analyzed, has a search occurred?

Today, tools can detect heat released from buildings,¹ recreate images displayed on distant computer monitors,² determine what is typed on a keyboard by listening to the distinct sounds of the keypresses,³ and eavesdrop on WiFi Internet communications traveling through the air. Handheld GPS units can monitor and store our movements around town,⁴ and web browsers keep detailed records of the websites we have visited.⁵ Tomorrow will surely bring new tools that are more invasive,⁶ easier to use, and able to work from greater distances.

* Associate Professor, University of Colorado School of Law. Thanks to Pierre Schlag and Phil Weiser for their helpful comments.

¹ See *Kyllo v. United States*, 533 U.S. 27 (2001).

² Allegedly, a technology called TEMPEST can capture and decode the radio emanations leaving a computer monitor from afar in order to recreate the images displayed. See Christopher J. Seline, *Eavesdropping on the Compromising Emanations of Electronic Equipment: The Laws of England and the United States*, 23 CASE W. RES. J. INT'L L. 359, 361-62 (1991).

³ See Elizabeth Woyke, *Is Someone Listening to Your Typing?*, BUS. WK., Oct. 3, 2005, at 18.

⁴ See *United States v. Bennett*, 363 F.3d 947, 952 (9th Cir. 2004) (describing use of a seized GPS unit's "backtrack" feature to demonstrate that defendant's boat had traveled from Mexico).

⁵ See Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 542 (2005).

⁶ In one sense, these technologies are *less* invasive: you have no idea you are being watched. Having your keystrokes decoded is much less disruptive than having your living room turned upside down. Thanks to Pierre Schlag for this point.

Fourth Amendment cases are surprisingly difficult to apply to tools used in a surveillance two-step: collect the data now, analyze the data later (sometimes, much later). Prior to data analysis, has a search occurred? In *Kyllo v. United States*,⁷ the Court held thermal imaging of a home to be a search.⁸ But what would have been the result if the police had stored the information without looking at it? Similarly, what if the police lawfully seize a suspect's GPS device and copy the device's internal memory without viewing the record of past movements? Have searches yet occurred in these situations?

Professor Kerr's description of the forensic analysis of computers⁹ provides a straightforward fact pattern with which to examine these questions. The forensic analysis of a computer almost always begins with the creation of a bit-by-bit, exact copy — called a “mirror image” or an “image” — which preserves all of the data found on the computer's hard drive. In his article, Professor Kerr argues that unless and until data from the image are exposed, no search has occurred.¹⁰ He worries that during the time after the image is made and before it is analyzed, the Fourth Amendment may not apply since the owner of the original drive has not been deprived of a possessory interest under his reading of *Arizona v. Hicks*.¹¹

Although he decries this “creepy,” “Orwellian” result,¹² if anything, Professor Kerr underestimates (or undersells) the threat to privacy of constitutionally unregulated imaging. At the same time, his attempt to distinguish *Hicks* is a bit unconvincing and arguably unnecessary. In *Hicks*, the Supreme Court held that the police did not seize the serial number inscribed on the bottom of stereo equipment by copying it down, since the act of copying did not interfere with the owner's possessory interest in the serial number or equipment.¹³ *Hicks* relies on the standard definition of seizure — meaningful interference with a possessory interest — a definition rarely satisfied when the police grab digital evidence.

But there is another sense in which courts have construed seizure, embodying a previously unidentified Fourth Amendment interest: the right to delete. This right can be found in the Constitution once one looks beyond physical-property-based notions of seizure, which fit so poorly in the digital world, in favor of an approach that asks: “Can a digital copy cause the same negative effects as physical dispossession?”

⁷ 533 U.S. 27 (2001).

⁸ See *id.* at 27.

⁹ Kerr, *supra* note 5.

¹⁰ *Id.* at 550.

¹¹ 480 U.S. 321, 324 (1987).

¹² Kerr, *supra* note 5, at 559.

¹³ *Hicks*, 480 U.S. at 324.

The answer is yes; when an owner loses control of a copy of her data, she loses the ability to dispose of or alter that data, which I contend causes a form of seizure. This is analogous to the property right to destroy, which is tied to the rights of dominion and control. The Fourth Amendment prohibition on unreasonable seizure should protect these rights and provide a constitutional right to delete.

The right to delete explains why imaging is seizure without requiring *Hicks* to be overruled or otherwise conflicting with existing jurisprudence.¹⁴ It will also help determine the Fourth Amendment status of the ongoing data collection of heat emanations, keypresses, monitor images, WiFi communications, GPS tracks, web browsing records, and new technologies yet to be invented. Ultimately, a physical-property-based reading of Fourth Amendment seizure fails to properly translate the Amendment's protections to intangible, digital property.

I. THE DANGEROUS CONSEQUENCES OF UNLIMITED GOVERNMENT IMAGING

Perhaps Professor Kerr assumes the risk of unfettered government imaging is obvious, but he underplays the downside. He seems mollified by the fact that even if a hard drive's data are not seized when imaged, any subsequent look at the data on the image will constitute a search and usually require a warrant. A search may not have occurred, however, in one particularly critical and timely situation: data mining.

Data mining describes a broad set of techniques used to find patterns in large collections of data.¹⁵ Some consider it to be an important tool for detecting and preventing acts of domestic terrorism.¹⁶ If hard drive imaging is not a search or seizure, "the government could freely generate copies of our hard drives and indefinitely retain them in government storage."¹⁷ Agents could fill many government warehouses with the innocent and incriminating data of tens of thousands of computers once thought to hold evidence of a crime. If agents want to mine this data without a warrant, a Fourth Amendment search may not have occurred for two reasons.

First, if a search does not occur until data is exposed to investigators, as Professor Kerr contends, the data mining system could be con-

¹⁴ In this essay, I am attempting to look at Fourth Amendment seizure and new technology in a way that least disturbs existing case law. This is not an attempt to overhaul the theoretical underpinnings of search and seizure in light of new technology.

¹⁵ See generally Lee Tien, *Privacy, Technology, and Data Mining*, 30 OHIO N.U. L. REV. 389 (2004).

¹⁶ See *id.* at 392 n.10.

¹⁷ Kerr, *supra* note 5, at 559.

figured to report the existence of “hits” without revealing the results. An analyst could, for example, feed the newly discovered e-mail address of a known terrorist into the data mining program and ask — in a strictly yes/no sense — whether there are patterns of correspondence involving that address anywhere in the database.¹⁸ Armed with a positive result, investigators could then ask a magistrate for a warrant to expose only information pertaining to the hit. Second, the expected users of the data store — national security analysts and others charged with preventing domestic terrorism — are less likely to be deterred by the threat of suppression because their focus is on *ex ante* prevention instead of on *ex post* prosecution.

If imaging is neither search nor seizure, law enforcement agents would have the incentive to image every hard drive they could find. Whether or not a drive was found to contain evidence, the image could be loaded into the data store. The government could end up indefinitely possessing the private correspondence (e-mail), reading habits (web traffic), lists of associates (instant messenger buddy lists), most private thoughts (diaries), and financial information (Quicken databases) of thousands (or more) of people.

II. IMAGING AS FOURTH AMENDMENT SEIZURE: THE RIGHT TO DELETE

These risks diminish greatly, however, if courts rule that hard drive imaging is a Fourth Amendment seizure.¹⁹ They can reach this conclusion, I contend, without reversing prior rulings. Seizure is traditionally defined as that which “meaningfully interfere[s]” with a “possessory interest.”²⁰ In contrast, search is defined as the government’s intrusion into a person’s reasonable expectation of privacy.²¹ In rough terms, search is about privacy rights, and seizure is about property rights.²² However, in some contexts, seizure has an extra-property sense and describes invasions of privacy, most notably in the bugging and wiretap cases. Nobody is dispossessed of their words or voice when they are illegally recorded, yet courts have described wiretapping

¹⁸ This assumes that the yes/no test itself is not a Fourth Amendment search under the exposure test.

¹⁹ For one thing, owners of seized data can bring a motion under FED. R. CRIM. P. 41(g) to return the property.

²⁰ *Arizona v. Hicks*, 480 U.S. 321, 324 (1987) (quoting *Maryland v. Macon*, 472 U.S. 463, 469 (1985)).

²¹ See *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

²² See, e.g., *Texas v. Brown*, 460 U.S. 730, 747–48 (1983) (Stevens, J., concurring) (“The Amendment protects two different interests of the citizen — the interest in retaining possession of property and the interest in maintaining personal privacy. A seizure threatens the former, a search the latter.”).

as both a search and a seizure.²³ Perhaps the wiretap courts are being sloppy, describing what is only a search as a seizure. But, more compellingly, perhaps a seizure is not limited to physical dispossession. As Professor Kerr points out, intangible computer data has a way of exposing fissures in some of our bedrock understandings of the Fourth Amendment.²⁴

To determine whether the constitutional limit on unreasonable seizure protects anything other than physical possessory interests, it helps to ask the question, why is dispossession important? Cases like *Hicks* view dispossession as a simple matter of rivalry: if you have my locked box, I can't have it too. But in the age of nonrivalrous, perfect digital copying, this view of dispossession seems tautological and unhelpful.

The approach I suggest is to ask whether nonrivalrous copying can produce similar negative effects to rivalrous dispossession. One negative effect of physical dispossession is it keeps the owner from altering, destroying or otherwise changing the state of his property. If you take my box full of letters, I am dispossessed of them, which harms me because I cannot give away, alter, or destroy them. I have lost the ability to control my property. This not only diminishes the value of my property, but it also invades my privacy.

The text of the Fourth Amendment seems broad enough to protect this "right to destroy" or, in the computer context, "right to delete" by its terms through its prohibition on unreasonable seizure. It is not surprising that the Bill of Rights would protect such a right. There is a long tradition of recognizing the right to destroy in property law. As Lior Strahilevitz has discussed, at various times in legal history courts have identified the right to destroy property as one of the "bundle of rights" intrinsic to physical possession.²⁵ This right is tied to the rights of dominion and control. Although the right to destroy may seem culturally or economically unsavory, it is protected because without the extreme ability to change, delete, or destroy, virtually nothing will be left of the rights of dominion and control.²⁶ Furthermore, the right to delete assures computer users that their words can be in some sense undone. This provides a sense of privacy that may lead to more candor in discussing sensitive matters electronically, and the increased candor benefits all of society, not only the owners of the data.

²³ See, e.g., *Katz*, 389 U.S. at 353 (holding electronic voice surveillance to be a "search and seizure"); *Berger v. New York*, 388 U.S. 41, 59 (1967) ("[T]he statute's failure to describe with particularity the conversations sought gives the officer a roving commission to 'seize' any and all conversations.").

²⁴ Kerr, *supra* note 5, at 533–34.

²⁵ Lior Strahilevitz, *The Right To Destroy*, 114 YALE L.J. 781, 794 (2005).

²⁶ See *id.* at 794–95 (describing the right to destroy as an extreme version of the rights to exclude, use, and control subsequent alienation).

A Fourth Amendment right to delete explains the reasoning and conclusions of the wiretapping courts. Although a wiretap does not dispossess me of my words, once it records my private conversation, my words have been in a sense taken from me — the wiretap deprives me of the ability to conceal or otherwise destroy those words. The right to delete can also explain cases that have held video recordings to be seizures under the Fourth Amendment.²⁷

The right to delete explains why data (such as e-mail messages) disclosed to a third party implicate the Fourth Amendment if they are acquired by police in real time,²⁸ but perhaps not if they are acquired from storage.²⁹ Real-time surveillance is somehow seen as a greater violation of privacy than snapshot surveillance, which can be explained by the right to delete.

E-mail revealed through a snapshot is as incriminating (and conversely as private) as the owner has allowed it to be. The owner has made hundreds of privacy assessments about whether to keep or delete old messages. The messages that remain reflect individual, intentional decisions not to delete. Paranoid criminals will delete all incriminating messages as soon as they are read, and those messages will likely never be seen by police conducting snapshot surveillance.³⁰ In contrast, evidence revealed through real-time, continuous surveillance is outside the control of the person surveilled. E-mail wiretaps typically copy all incoming and outgoing e-mail messages before they ever arrive at the user's inbox,³¹ meaning the police can read every message belonging to the account owner, even the paranoid owner. Surveillance perfection — the counter to the right to delete — explains why the Fourth Amendment may apply to real-time surveillance and not snapshot surveillance.

²⁷ See *Ayeni v. Mottola*, 35 F.3d 680, 688 (2d Cir. 1994), *abrogated on other grounds* by *Wilson v. Layne*, 526 U.S. 603, 618 (1999).

²⁸ *Cf. Berger*, 388 U.S. at 51 (holding that capturing a conversation sent over a telephone line is a Fourth Amendment search).

²⁹ Stored e-mail messages are entrusted to third parties (ISPs), and arguably may be obtained from those third parties without implicating the Fourth Amendment. *Cf. United States v. Miller*, 425 U.S. 435, 443 (1976) (holding that depositor had no reasonable expectation of privacy in the contents of checks and deposit slips given by the depositor to a bank). *But see* Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1292 n.45 (2005) (criticizing the *Miller* holding and distinguishing e-mail messages from bank records). Congress has passed laws premised on the conclusion that e-mail messages stored with an ISP lack the full protection of the Fourth Amendment. *See, e.g.*, 18 U.S.C. § 2703(b) (2000 & Supp. II 2002) (providing that communications can be compelled with a subpoena or court order).

³⁰ Never say never. Sometimes the traces of deleted e-mail messages remain on servers for days, weeks, or indefinitely. Also, the snapshot may be taken after a message has arrived and before the user has had a chance to decide whether to delete it.

³¹ *See United States v. Councilman*, 373 F.3d 197, 219 (1st Cir. 2004) (Lipez, J., dissenting) (describing the method with which law enforcement agents typically execute e-mail wiretap orders), *rev'd on reh'g*, 418 F.3d 67 (1st Cir. 2005) (en banc).

Like the real-time surveillance of an e-mail inbox, a bit-by-bit image prevents future deletion and modification. The image preserves all of the contents of every file in the hard drive. Obviously, the owner can still delete the original copies of the files, but the police have frozen the status quo by limiting his ability to control which files they can access. He is dispossessed of one of the bundle of rights in his property, and to deny that this is a seizure stretches the plain meaning of the word.³²

Seizure defined as a meaningful interference with the right to delete cannot explain all of the past cases without a slight modification. Courts have consistently held that it is not a seizure (nor a search) to copy or record evidence in plain view. Whether this exception makes sense in all situations is beyond the scope of this essay, but it is consistent with the right to delete. Once the police are in a position to see items in plain view, the right to delete those things has already been lost. For example, courts have held that photographing a search scene is not a seizure,³³ nor is using a GPS-enabled locator to track the movements of a car along the public streets of a city.³⁴

This exception explains *Hicks*. Although the bottom of the stereo equipment was not in plain view at first, the police moved the equipment slightly — an act ultimately ruled to be an unconstitutional search — which exposed the serial number to plain view.³⁵ If instead *Hicks* had involved a technology that could pull the serial number out from within the equipment without touching it, it would have implicated the right to delete and, in my opinion, the use of that technology would have been a seizure. Similarly, if, as Professor Kerr argues, individual files on a hard drive are “closed containers” for Fourth

³² The Fourth Amendment may not forbid *every* interference with the right to delete. Following the *Hicks* test, the test should be: has there been a *meaningful interference* with the right to delete?

Imagine the police use a computer program that scans Internet traffic for particular text strings. If they find a match, a search has occurred. But it is arguable that the program has not seized every single packet flowing through the program. Although the user lost the ability to delete his communications during the fraction of a second that they were held by the program, this de minimis interference with the right to delete would not rise to the level of seizure. This temporal component and other questions of scope suggest future work beyond the scope of this essay. Nevertheless, any definition of “meaningful interference with the right to delete” and any temporal requirements are met when the police image and keep a copy of a hard drive.

³³ See *Bills v. Aseltine*, 958 F.2d 697, 707 (6th Cir. 1992). Photographing items in plain view allows much greater police scrutiny. On the other hand, the police could instead remain on the scene, studying every minute detail; the photograph helps avoid this greater intrusion, but in return, allows for a more searching inquiry.

³⁴ See *United States v. McIver*, 186 F.3d 1119, 1128 (9th Cir. 1999); cf. *United States v. Knotts*, 460 U.S. 276, 281 (1983) (“A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”).

³⁵ *Arizona v. Hicks*, 480 U.S. 321, 327 (1987).

Amendment purposes,³⁶ a mirror image which reproduces everything inside every closed container seizes those things not in plain view.

Professor Kerr ultimately concludes that imaging is a seizure, but his solution is wholly unsatisfactory. While recognizing other possible approaches, he notes that in order to make an image, the computer itself is seized through the connection of cables and by the turn of the screw.³⁷ This, he hopes, protects us from unfettered government imaging. The problem with this approach is it hitches our constitutional protection to today's technology. In a future world where the magnetic bits encoded on the surface of a hard drive platter can be lifted through the air without the use of cables, Professor Kerr's analysis would lead to the flawed conclusion that a seizure has not occurred.

III. CONCLUSION: THE RIGHT TO DELETE BEYOND HARD DRIVE IMAGING

The right to delete has consequences beyond computer forensics. It informs how the Fourth Amendment should be construed in the face of new technology. Any time law enforcement uses a "collect/copy now, analyze later" technology, they may be performing a Fourth Amendment seizure.

Today, the right to delete is rarely encountered in the physical world. A search of a house is a snapshot search, even if it takes hours to conduct. After the police pack up and leave the scene, the contents of the closed containers left behind are unseized, destructible, and deletable.

In contrast, indulge in science fiction momentarily: Imagine the police develop a tool that can reproduce physical objects. Every molecule of every apple, teapot, and credenza — including the molecules of the contents of the credenza — can be perfectly duplicated with this machine, a Star Trek replicator on steroids. If the tool is used during the lawful search of a house to reproduce every item in every closed container in the house and the resulting copy is stored — picture a vast warehouse with a replica of the house and all of its contents — what is the result? Is the reproduction and storage a separate Fourth Amendment event, and if so, is it a search or a seizure? If the replicated objects are "beamed" directly into the warehouse, the doors to the warehouse locked, and all people forbidden to enter for any reason, courts would probably hold that a search has not yet occurred, using the same "exposure" theory that Professor Kerr advances for computer searches. There is a good argument that no "reasonable expectation of privacy" has yet been invaded.

³⁶ Kerr, *supra* note 5, at 554–55.

³⁷ *Id.* at 560–61.

But it defies belief that a constitutional amendment designed to protect privacy and to regulate the power of the state would say nothing about this technology. Courts would likely conclude that the Fourth Amendment's prohibition on unreasonable seizure forbids this use of the tool. Even though the occupant of the house is not physically dispossessed of anything, it ignores plain meaning to assert that nothing has been seized. The right to delete explains this conclusion: the police have frozen the status quo; they can obtain another warrant to search their copy of the closed credenza at a later time, and the owner has lost his right to dispose of the items in the credenza. These items have been seized.

Finally, the right to delete forces us to think of "search" and "seizure" as two complementary but distinct types of government intrusion. Too often, courts and commentators refer to "SearchAndSeizure" as if it were one monolithic category of government action. In fact, seizure has historically been construed as an act that affects our property rights, not our privacy rights, while search has been the chief invader of privacy. In today's world of technology, the police increasingly have the ability to invade our privacy — by depriving us of the ability to delete — without ever searching in the traditional sense. The wisdom of the Constitution's drafters fills the gap between privacy and property if we recognize the modern, privacy-protecting role of the prohibition on unreasonable seizure.