# TAKING SMALLER BYTES PROTECTS CONSTITUTIONAL RIGHTS:

## *Addressing the Novel Problem Posed by Deleted Data*

by:


Justin A. Thornton
Law Offices of Justin Thornton
1615 L Street, NW, Suite 1200
Washington, DC 20036
(202) 778-0559
JAT@ThorntonLaw.com
www.lawyers.com/ThorntonLaw

&

Mark H. Allenbaugh
Staff Attorney
United States Sentencing Commission
One Columbus Circle, NE, Suite 2-500
Washington, DC 20002
(202) 502-4216
MAllenbaugh@ussc.gov
www.ussc.gov

# TAKING SMALLER BYTES PROTECTS CONSTITUTIONAL RIGHTS: ADDRESSING THE NOVEL PROBLEM POSED BY DELETED DATA

JUSTIN A. THORNTON*
&
MARK H. ALLENBAUGH**

> Do not join those who drink too much wine or gorge themselves on meat, for drunkards and gluttons become poor, and drowsiness clothes them in rags.
>
> -*Proverbs* 23: 20 - 21 (New International Version).

> Now that the decision of today gives open sesame to all wire-tappers, what is to be the attitude of all telephone users in Pennsylvania? Will they approach a telephone with trepidation, fearful of the unknown gluttonous ear at the wire-tap ready to devour all that is to be said? And when the omnivorous wire-tapper has gorged on family secrets, business confidences and government material, what will he do next?
>
> -*Commonwealth v. Chaitt*, 112 A.2d 379, 393 (Pa. 1955) (Musmann, J., dissenting).

## I. INTRODUCTION

In the current era of hyper-evolving technological change, the ancient Greek virtue of *sophrosyné*, or self-control,[1] still plays just as central and essential a role as ever in the administration of just governance.[2] With the increasing presence of law enforcement in cyberspace, the necessity for government to abstain from over-indulgence and exercise self-control is paramount. Necessarily, as the "information age" matures and technology becomes more complex, governmental law enforcement policies continue to be presented with the challenge of determining just how much information is required to effectively combat computer crime, all the while respecting the Fourth Amendment's guarantee against unwarranted searches and seizures.[3] Over-indulging in the acquisition of private information jeopardizes the public's trust in the integrity of law enforcement, as expressed by Justice Mussman's dissent in *Commonwealth v. Chaitt*, cited above. In contrast, acquiring too little information places criminal enterprises beyond the reach of the law, which threatens not only the economic security of industries and nations, but with the advent of cyberterrorism, the physical security of virtually everyone.[4]

As criminal enterprises increasingly exploit computer technology to facilitate their ends, and concomitantly, law enforcement utilizes the same technology to detect, investigate, and prosecute such criminal enterprises, it becomes imperative that zealous law enforcement does not devolve into gluttonous governmental intrusion. As Professor Laurence Tribe has noted, "[n]ew technologies should lead us to look more closely at just what values the Constitution seeks to preserve."[5] With respect to the exercise of governmental authority, the virtue of temperance surely is one of those values implicit within the Constitution but made explicit in

Fourth Amendment jurisprudence.

To be sure, the challenges new technologies present both to law enforcement and the courts are nothing new. Indeed, from the introduction in the earlier Twentieth Century of systolic blood pressure tests, made famous in *Frye v. United States*,[6] to pen registers and wiretaps, the balance between temperate law enforcement and gluttonous governmental intrusion always has been difficult to ascertain. As Justice Brandeis observed in his oft-quoted dissent in *United States v. Olmstead*,[7]

> The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. 'That places the liberty of every man in the hands of every petty officer' was said by James Otis of much lesser intrusions than these. To Lord Camden a far slighter intrusion seemed 'subversive of all the comforts of society.' Can it be that the Constitution afford no protection against such invasions of individual security?[8]

In light of the current climate of concern created by the government's revelation of its "Carnivore"[9] and "Echelon"[10] programs, this article focuses on a particular and increasingly important technological issue wherein the scope of protection afforded by the Constitution remains rather vague: that is, the protection afforded to deleted computer data. Part II discusses what appears to be the only reported United States Circuit Court of Appeals case discussing directly the applicability of the Fourth Amendment to the recovery of "deleted" data from computer hard drives and diskettes. Finally, Part III concludes by noting some other potential problems with respect to the recovery of "deleted" data. In light of the fact that, as the Department of Justice asserts, there is "[n]o bright line rule indicat[ing] whether an expectation of privacy is constitutionally reasonable,"[11] it is certain that new technologies will continue to dim whatever rule—if any—there may be.

## II. UNITED STATES V. UPHAM

In February of 1997, United States Customs agents were monitoring an Internet chat room as part of an undercover child pornography investigation.[12] During the course of the investigation, the agents received from someone within the chat room numerous images depicting child pornography. From the records of an Internet service provider, the agents were able to determine that the images were sent from a computer owned by one Kathi Morrissey. Shortly thereafter, the agents obtained a warrant, and on March 21, 1997, conducted a search of Morrissey's home and seized her computer and numerous diskettes.[13] According to the First Circuit,

> Using a computer utilities program and the "undelete" function, the government was able to recover form the computer's hard disk and the diskettes some 1,400 previously deleted images of minors engaged in sexually explicit conduct. These images included the relatively small number of images that the agents had received in Buffalo in February 1997 from Morrissey's computer.[14]

During subsequent investigation, it was discovered that although Morrissey owned the computer, a live-in boyfriend of Morrissey's was the primary user of the computer and was the one who, in fact, had sent the child pornography to the agents during the undercover investigation.[15] In May of 1997, Troy Upham, Morrissey's (now former) live-in boyfriend was indicted on four counts of "transporting in interstate commerce computer graphic images of minors engaged in sexually explicit conduct" pursuant to 18 U.S.C. § 2252(a)(1),[16] and one count of possession of "1,400 images of minors engaged in sexually explicit conduct" pursuant to 18 U.S.C. § 2552(a)(4)(B).[17] Upham unsuccessfully moved to suppress the evidence of the 1,400 "deleted" images and thereafter was convicted by a jury on all five counts.

Although Upham appealed on a variety of issues, the First Circuit found that only the issue regarding the validity of the district court's denial of Upham's motion to suppress warranted full discussion. Specifically, Upham argued "that the warrant was too broad and that its scope was exceeded when the government recovered from the hard drive and diskettes the images that had previously been deleted."[18] The warrant listed, in part, the following items to be seized: "[1.] Any and all computer software and hardware, . . . computer disks, disk drives. . . . [2.] Any and all visual depictions, in any format or media, of minors engaging in sexually explicit conduct [as defined by the statute]."[19]

The First Circuit rejected Upham's argument that the warrant was not sufficiently particular so as to comply with the Fourth Amendment. In doing so, the court noted that with regard to the particularity requirement, there are in fact two issues involved: "one is whether the warrant supplies enough information to guide and control the agent's judgment in selecting what to take, and the other is whether the category as specified is too broad in the sense that it includes items that should not be seized."[20] According to the court, as the warrant called specifically for the seizure of computer equipment, "[t]he problem [wa]s not imprecision but arguable overbreadth."[21] Nevertheless, "the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images."[22] The court specifically noted the impracticality presented by an on-site search of the defendant's hard drive in light of the fact that "the mechanics of the search for [the 'deleted'] images later performed off site could not readily have been done on the spot."[23] Consequently, the warrant also was not overbroad inasmuch as it apparently was necessary to seize the equipment in order to conduct the search.

The First Circuit, however, questioned the validity of the government's alternative argument that "the second paragraph [of the warrant], allowing seizure of the unlawful images, alone justifie[d] the seizure of the equipment regardless of the first paragraph,"[24] which called for the seizure of the computer equipment. Although a warrant containing only that paragraph "would permit an on-site search of any 'container' that might reasonably have the images concealed 'inside'--including the computer and any disks," the court emphasized that "there is some division in the case law as to whether and when the police may seize and remove from the premises items. . . not named in the warrant merely in the reasonable hope that a search of those items later on will lead to recovery of the items that are named."[25] Indeed, the court allowed that "there might be legitimate doubt" whether a warrant to search a home for a murder weapon would allow the police to "cart off the entire contents of the house, including the refrigerator, for purposes of a later search."[26]

Finding that the warrant was neither too imprecise nor overbroad, the First Circuit then turned to the issue of whether the recovery of the deleted images was outside the scope of the warrant. The court noted that "until the deleted information is actually overwritten by new information, the old information can often be recovered. . . ."[27] The court held that such recovery of the deleted data was not outside the scope of the warrant: "The seizure of unlawful images is within the plain language of the warrant; their recovery, after attempted destruction, is no different than decoding a coded message lawfully seized or pasting together scraps of a torn-up ransom note."[28]

Interestingly, the court took pains to reject explicitly the government's argument that "by deleting the images, Upham 'abandoned' them and surrendered his right of privacy" much as one does when placing trash on a public street.[29] According to the court, although "[a]nalogy is a hallowed tool of legal reasoning," the analogy between trash and deleted computer data was "false."[30] Thus, according to the First Circuit, although deleted computer data are not analogous to abandoned trash, deleted computer data are analogous to encrypted messages or torn-up ransom notes, and as such, did not require issuance of a further warrant.

Within this hallowed battle between legal analogies, it is not clear why the First Circuit found convincing some analogies, but not others, inasmuch as the court merely stated *ipso facto* its assessment of the analogies' tenability; some analogies just appeared to correspond better with the court's intuition than others. Neither analogy, however, appears to be any more intuitive than the government's failed attempt to analogize deleted computer data to abandoned trash. As for the court's first analogy, it plausibly can be argued that deleted computer data wholly are unlike coded, or encrypted, data inasmuch as encrypted computer data are meant to be preserved for future reference and preserved manifestly in a private manner. In contrast, deleted computer data simply are meant to be destroyed (with the privacy question left open). Moreover, to argue—as did the First Circuit—that deleted computer data literally are analogous to "decoding a coded message *lawfully seized*" is to beg the question as to whether the message was seized lawfully in the first place. Indeed, as the First Circuit noted, whether an object is lawfully seized depends on the specifications of the warrant, and not so much on the nature of the evidence sought.[31] Thus, it is far from obvious that the analogy to encrypted data is cogent.

As for the court's second analogy, it also can be argued that deleted computer data are not analogous to a torn-up ransom note, for what is a torn-up ransom note if not trash? Indeed, in *United States v. Scott*,[32] cited by the panel in *Upham* in support of this analogy, the First Circuit discussed the issue of whether "the shredding of private documents attaches a constitutionally recognizable privacy expectancy which follows the shredded remnants. . . even after they become public garbage."[33] Although the *Scott* panel answered the question in the negative, it began its analysis by noting "that what we are dealing with here is trash. More important is the fact that at the time the challenged evidence came into the hands of the authorities, it was public trash."[34] Consequently, if the First Circuit is to be consistent, the analogy to the torn-up ransom note fails; per the precedent the *Upham* panel cited, a torn-up ransom note simply is nothing more than trash. In light of the above, both analogies, which are the "hallowed tools of legal reasoning," are, at best, questionable; at worst, the analogies simply fail with the result that *Upham* was decided wrongly.

Despite acknowledging earlier the fact that a warrant to search does not necessarily imply a warrant to seize, the First Circuit concluded its analysis by noting that "[t]he warrant process is primarily concerned with identifying what may be searched or seized—not how—and whether there is sufficient cause for the invasion of privacy thus entailed."[35] Be that as it may, the reason why the *method* of searching or seizing items pursuant to a warrant traditionally has not been an issue likely stems from the fact that searches and seizures primarily have involved tangible items—for example, file cabinets[36]—and not such things as deleted computer data. Unlike the search and seizure of file cabinets and the like, computer hard drives contain not just a mixture of various files that may or may not be called for by the warrant, but also files that may be in various states of informational degradation, i.e., although some "deleted" files may easily be recovered by use of an "undelete" function (as was the case in *Upham*), others may have been partially or substantially overwritten thereby requiring the use of more sophisticated and invasive methods of data recovery. In such cases, the *method* used can become essential to determining "whether there is sufficient cause for the invasion of privacy thus entailed," and indeed, whether the scope of the warrant has been breached.

Recognizing this issue, the Department of Justice's recently amended manual regarding

searching and seizing of computers discusses at length the need to articulate *in the warrant* the method to be utilized in the searching and seizing of computers and their databases: "In general. . . the keys to drafting successful computer search warrants are first to describe carefully and particularly the object of the warrant that investigators have probable cause to seize, and second *to explain adequately the search strategy* in the supporting affidavit."[37] As the Department of Justice's manual instructs, including the search strategy in the affidavit "helps to thwart claims that the agents executed the search in 'flagrant disregard' of the warrant."[38] And when a computer network, as opposed to an individual hard drive, is the target of the search, articulating the search strategy becomes even more important.

> Obtaining detailed and accurate information about the targeted computer also has important legal implications. For example, the incidental seizure of First Amendment materials such as drafts of newsletters or web pages may implicate the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, and the incidental seizure and subsequent search through network accounts may raise issues under the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2701-11. . . . To minimize liability under theses statutes, agents should conduct a careful investigation into whether and where First Amendment materials and network accounts may be stored on the computer system targeted by the search. At least one court has suggested that a failure to conduct such an investigation can help deprive the government of a good faith defense against liability under these statutes. See State Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), aff'd, 36 F.3d 457 (5th Cir. 1994).[39]

Thus, despite the First Circuit's assertion that warrants generally do not contain the methodology for the search strategy, at least in cases involving searches and seizures of computers today, the Department of Justice has articulated good policy and legal reasons why such strategies should be included in the warrant; if nothing else, the search strategies help to ensure compliance with the scope of the warrant. As the Department of Justice notes in its manual:

> Despite the common legal framework, computer searches differ from other searches because computer technologies frequently force agents to execute computer searches in nontraditional ways. . . . As a result of these uncertainties, agents cannot simply establish probable cause, describe the files they need, and then 'go' and 'retrieve' the data. Instead, they must understand the technical limits of different search techniques, plan the search carefully, and then draft the warrant in a manner that authorizes the agents to take necessary steps to obtain the evidence they need.[40]

## IV. CONCLUSION

To date, the First Circuit appears to be the only United States Circuit Court of Appeals directly to have addressed the issue of whether deleted computer data are protected by the Fourth Amendment. According to the First Circuit, although deleted computer data are not like trash, they are akin to encrypted data or shredded documents. Consequently, as neither

encrypted data nor shredded documents enjoy additional Fourth Amendment protection, neither do deleted data. Both of these analogies, however, are problematic. First, it is not obvious that deleted data are analogous to either encrypted data or shredded documents at all. As discussed above, there are important conceptual differences between deleted data, and encrypted data and shredded documents. Second, assuming that deleted data are analogous, the question of whether Fourth Amendment protection applies to encrypted data or shredded documents turns on the validity and scope of the warrant itself. As the Department of Justice itself recognizes, "agents cannot simply establish probable cause, describe the files they need, and then 'go' and 'retrieve' the data,"[41] especially if the data reside in the nebulous realm of deleted files. Consequently, it is of no help to assert that deleted data are analogous to encrypted data or shredded documents for purposes of assessing Fourth Amendment issues.

The novel issue of deleted computer data presents new challenges both to the courts and law enforcement. As we become more dependent on computer databases, and store our most private information about ourselves in them, it is important for the government to tread lightly when searching and seizing those things that have become less figuratively, and more literally, extensions of our selves. Just as a warrant to search for an item does not necessarily permit the government to search everything and seize anything in one's home, in cases involving information stored on a computer, the same limits should apply: a warrant to search for particular files should not *ipso facto* be understood as a warrant to search any and all files stored on the computer, including "deleted" files. Although the nature of searches and seizures has changed in this cyber-era, the virtue of moderation has not. Fortunately, this virtue appears implicit in the Department of Justice's revised manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Hopefully, this virtue will not remain virtual, but become expressed explicitly in Fourth Amendment case law, and thus discourage governmental gluttony: taking smaller bytes protects constitutional rights.

---

[*]Mr. Thornton is a white collar criminal defense attorney practicing in Washington, D.C. As a Department of Justice trial attorney for ten years, Mr. Thornton successfully prosecuted throughout the United States more than 75 complex criminal fraud cases. He is a recipient of the Tax Division's Outstanding Attorney Award and the IRS Assistant Commissioner's Award. In private practice since 1987, Mr. Thornton now represents individuals and businesses under investigation or prosecution for white collar criminal offenses, including tax fraud and related matters. Mr. Thornton also co-chairs the Tax Enforcement Subcommittee of the ABA's White Collar Committee, and serves as an advisor to the United States Sentencing Commission.

[**]Mr. Allenbaugh is a staff attorney at the United States Sentencing Commission and serves on the Commission's Economic Crimes Policy Development team. He is a recent graduate of American University's Washington College of Law where he served as the Associate Articles Editor for the *American University Law Review*. Mr. Allenbaugh also lectures courses in the history of philosophy, logic, and business ethics at the George Washington University, Washington, D.C.

The views and arguments expressed herein solely are the authors and do not reflect necessarily the official views or opinions of the United States Sentencing Commission, or any of its staff.

[1] The Greek term *sophrosyné* was used both by Plato in *The Republic* and Aristotle in *The Nichomachean Ethics* to refer to the temperate, well-balanced individual who refrained from excess. The term also was applicable to moderate forms of government. *See* Mark Neal Aaronson, *Be Just to One Another: Preliminary Thoughts on Civility, Moral Character, and Professionalism*, 8 ST. THOMAS. L. REV. 113, 146 n.128 (1995).

[2] *See id.*

[3]*See* U.S. CONST. AMEND. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated. . . .").

[4] *See, e.g.*, Louis J. Freeh, Statement for the Record on Cybercrime, Before the Senate Committee on Judiciary (Mar. 28, 2000) (exemplifying cyberterrorism as "the use of cyber tools to shut down critical national infrastructures (such as energy, transportation, or government operations) for the purpose of coercing or intimidating a government or civilian population"), *at* http://www.usdoj.gov/criminal/cybercrime/freeh328.htm.

[5]Laurence H. Tribe, *The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier*, The Humanist, Sept.-Oct. 1991, at 15, 16.

[6]293 F. 1013 (D.C. Cir. 1923).

[7]277 U.S. 438 (1928).

[8]*Id.* at 474 (1928) (Brandeis, J., dissenting).

[9] *See* Stephen P. Smith, et. al., IIT Research Institute, Independent Review of the Carnivore System: Final Report xiv (Dec. 8, 2000) (noting that "the presence of Carnivore and its successors without safeguards as recommended. . . fuels the concerns of responsible privacy advocates and reduces the expectations of privacy by citizens at large"). "Carnivore is a software-based Internet Protocol (IP) packet sniffer that can select and record a defined subset of the traffic on the network to which it is attached." *Id.* at 1-1.

[10] "Echelon" is the code name for a vast array of eavesdropping devices located throughout the globe that are operated by the United States, the United Kingdom, Canada, Australia, and New Zealand. Echelon is thought to be "perhaps the most powerful intelligence gathering organization in the world." Echelon is capable of intercepting virtually all digital and analog communications of any type throughout the entire world. For a detailed explanation of Echelon, see http://www.echelonwatch.org/.

[11] ORIN S. KERR, UNITED STATES DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 2 (Jan. 2001) ( hereinafter "DOJ MANUAL"), *at* http//www.cybercrime.gov/searchmanual.htm.

[12] *See* United States v. Upham, 168 F.3d 532, 533 (1st Cir. 1999).

[13] *See id.*

[14] *Id.*

[15] *See id.*

[16] *Id.* at 533-34.

[17] *Id.* at 534.

[18] *Id.*

[19] *Id.* at 535.

[20] *Id.* (citations omitted).

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.* at 536 (citations and footnote omitted).

[26] *Id.*

[27] *Id.* at 537.

[28] *Id.*

[29] *Id.* at 537 n.3 (citing, *inter alia*, California v. Greenwood, 486 U.S. 35, 48 (1988)).

[30] *See Upham*, 168 F.3d at 537.

[31] *See supra* text accompanying note 26.

[32] 975 F.2d 927 (1st Cir. 1992).

[33] *Id.* at 928.

[34] *Id.*

[35] *Upham*, 168 F.3d at 537.

[36] *See, e.g.*, United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997) (permitting seizure of entire file cabinet including warrant-specified and unspecified documents), *as cited in Upham*, 168 F.3d at 536 n.2.

[37] DOJ MANUAL, *supra* note 11, at 37.

[38] *Id.*

[39] *Id.* at 36.

[40] *Id.* at 34.

[41] *Id.*