OREGON LAW REVIEW

2011

VOLUME 90
NUMBER 1

Articles

MAX STUL OPPENHEIMER*

Cybertrash

* Professor, University of Baltimore School of Law; Faculty, The Johns Hopkins University Carey School of Business; B.S., Princeton University, *cum laude*; J.D., Harvard Law School. The author would like to thank his research assistant, Kristen Schrock Boston, University of Baltimore School of Law 2011; Professor Brian Kernighan of the Princeton University Computer Science Department; Bijal Shah of the University of Baltimore Law School library; and Sandy Marinaro of the Stevenson University library, for their assistance in the preparation of this Article. The Article was supported by a grant from the University of Baltimore.

INTRODUCTION

Information stored in a physical object receives the same Fourth Amendment protection as the physical object in which it is stored.[1] As information moves online, it becomes independent of physical objects, and therefore traditional rules must be reexamined. Others have argued persuasively,[2] and courts appear receptive to the argument,[3] that online communications and data should receive the same protection as their analogs embodied in the physical world. Even assuming that this conclusion will be universally accepted, a troubling consequence remains: the clear weight of authority holds that Fourth Amendment protection does not apply to information embodied in discarded physical trash.[4] If this rule for discarded physical trash translates into cyberspace, then even if online communications and data are protected, "cybertrash"—deleted e-mails and other files—is not protected.

---

[1] *See, e.g.*, United States v. Karo, 468 U.S. 705 (1984); Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279 (2005).

[2] *See, e.g.*, David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205 (2009); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004).

[3] *E.g.*, United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010); *In re* United States, 665 F. Supp. 2d 1210, 1213 (D. Or. 2009).

[4] While Couillard and Mulligan conclude that undeleted files are protected, Couillard, *supra* note 2; Mulligan, *supra* note 2, "undiscarded trash" is also protected, but loses its protection when discarded, *see infra* Part II.

This Article begins with a summary of the development of Fourth Amendment theory and the evolution of its theoretical basis from protection of property against physical trespass to protection of individuals against violations of their expectation of privacy.[5] The Article then analyzes the application of theory to the special case of physical trash.[6] The Article next explores what is meant by trash by looking at the broader context of disposal of physical materials and comparing various legal models for rights in discarded materials.[7] Finally, the Article evaluates the models and concludes that cybertrash is fundamentally different from physical trash and should be accorded Fourth Amendment protection notwithstanding the denial of such protection for physical trash.[8]

I
THE FOURTH AMENDMENT

The Fourth Amendment is, of course, the starting point for any analysis of protection against search and seizure. It provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[9]

The theory underlying the Supreme Court's interpretation of the Fourth Amendment has evolved,[10] running from a literal reading applying the Fourth Amendment to "persons, houses,[11] papers, and

---

[5] *See infra* Part I.

[6] *See infra* Part II.

[7] *See infra* Part III.

[8] *See infra* Part IV.

[9] U.S. CONST. amend. IV. The Fourth Amendment is applicable to the states by virtue of the Due Process Clause of the Fourteenth Amendment. Mapp v. Ohio, 367 U.S. 643, 655 (1961) ("[E]vidence obtained by searches and seizures in violation of the Constitution is . . . inadmissible in a state court.").

[10] For a detailed analysis of the development of Fourth Amendment interpretation, see Madeline A. Herdrich, Note, California v. Greenwood*: The Trashing of Privacy*, 38 AM. U. L. REV. 993 (1989). For an analysis of the confusion caused by the Supreme Court's different tests, see David P. Miraldi, Comment, *The Relationship Between Trespass and Fourth Amendment Protection After* Katz v. United States, 38 OHIO ST. L.J. 709 (1977).

[11] Hester v. United States, 265 U.S. 57, 59 (1924) (denying protection to open fields); Smith v. Maryland, 442 U.S. 735, 741 (1979) (denying protection to telephone lines running to a house).

effects" to an expectation of privacy test.[12] Running throughout this evolution is the common thread of protection of privacy and dignity interests against arbitrary and invasive acts by the government.[13] However, the meaning of "invasive" has historically evolved in response to technological advances, and technological changes have been dramatic since the Supreme Court's most recent venture into Fourth Amendment theory.[14]

A. The Physical Trespass Theory

Early Fourth Amendment cases were property based and held that the Fourth Amendment only prohibited searches that involved a common-law trespass by government officials.[15] A corollary, the "open fields" doctrine, which was applied in *Hester v. United States*,[16] was based on a reading of the Fourth Amendment as literally limited to people, houses, papers, and effects, and not to open fields beyond the home.[17] This reading relied on the common-law distinction between "curtilage," which had been "traditionally defined as the protected area immediately surrounding the home, into which [the] intimate activities [of the home were] extended," and "open fields," which implicated more relaxed rules of trespass.[18]

The Supreme Court did not perceive defining the limits of the curtilage as difficult. In *Oliver v. United States*, the Court noted:

---

[12] United States v. Chadwick, 433 U.S. 1, 11 (1977) ("[A] fundamental purpose of the Fourth Amendment is to safeguard individuals from unreasonable government invasions of legitimate privacy interests, and not simply those interests found inside the four walls of the home." (footnote omitted)); Katz v. United States, 389 U.S. 347, 351–52 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (citation omitted)).

[13] Camara v. Mun. Court, 387 U.S. 523, 528 (1967).

[14] The most recent detailed exploration of Fourth Amendment theory was in the 1967 case, *Katz*, 389 U.S. at 349–59, discussed *infra* Part I.C.

[15] *Hester*, 265 U.S. at 59; Goldman v. United States, 316 U.S. 129, 134–36 (1942) (noting that Fourth Amendment protection does not extend to open fields but does extend to the area immediately surrounding the home).

[16] 265 U.S. at 59.

[17] William C. Heffernan, *The Fourth Amendment Exclusionary Rule as a Constitutional Remedy*, 88 GEO. L.J. 799, 828–29 (2000).

[18] Carrie Leonetti, *Open Fields in the Inner City: Application of the Curtilage Doctrine to Urban and Suburban Areas*, 15 GEO. MASON U. C.R. L.J. 297, 299 (2005).

> Most of the many millions of acres that are "open fields" are not close to any structure and so not arguably within the curtilage. And, for most homes, the boundaries of the curtilage will be clearly marked; and the conception defining the curtilage—as the area around the home to which the activity of home life extends—is a familiar one easily understood from our daily experience.[19]

The Court offered the following refinement of the curtilage definition in *United States v. Dunn*: the area that "is so intimately tied to the home itself that it should be placed under the home's 'umbrella' of Fourth Amendment protection."[20] The definition is, of course, circular; defining the curtilage as that area protected by the Fourth Amendment is less than helpful in answering the question of whether the Fourth Amendment applies. The Court did, however, list four factors for determining whether an area was within the curtilage: (1) proximity to the home, (2) whether the area was within an enclosure surrounding the home, (3) the uses to which the area was put, and (4) the steps taken to protect the area from observation by passersby.[21]

The *Oliver* and *Dunn* decisions predate the World Wide Web,[22] so it is not surprising that the "familiar" conception of curtilage supposed in those cases breaks down when applied to cyberspace[23] and that the four *Dunn* factors do not translate well to analysis of cyberspace.

---

[19] 466 U.S. 170, 182 n.12 (1984).

[20] 480 U.S. 294, 301 (1987).

[21] *Id.* at 302–03. For an analysis of the difficulty of applying the concept of curtilage to high-density urban locations, see Leonetti, *supra* note 18.

[22] A November 12, 1990, internal CERN (the European Organization for Nuclear Research) memo from Tim Berners-Lee of its Computing and Network Division and R. Cailliau of its Electronics and Computing for Physics Division is widely regarded as the blueprint for what would become the World Wide Web. *See* T. Berners-Lee & R. Cailliau, *WorldWideWeb: Proposal for a HyperText Project*, WORLD WIDE WEB CONSORTIUM, http://www.w3.org/Proposal.html (last visited Aug. 5, 2011). The predecessor of the Internet (Arpanet) already existed but was not widely available. Even the CERN plan for the World Wide Web was, at that stage, limited: "The project will not aim . . . to do research into fancy multimedia facilities such as sound and video." *Id.* The first use of the term "World Wide Web" occurred in October 1990. Dan Connolly, *A Little History of the World Wide Web*, WORLD WIDE WEB CONSORTIUM, http://www.w3.org/History.html (last visited Aug. 5, 2011).

[23] The Court had, of course, dealt with electronic extensions of the home in wiretapping cases. *See, e.g.*, Silverman v. United States, 365 U.S. 505 (1961).

In addition, an aspect of general trespass law is the principle that there can be no trespass against abandoned property,[24] an aspect that features critically in the trash cases discussed below.[25] In the physical world, abandonment requires "both [the] owner's intent to abandon . . . property and . . . some affirmative act or omission demonstrating that intention."[26] The more challenging of these two requirements is the finding of intent to abandon,[27] a challenge that is especially difficult in cyberspace.

B. Relaxation of the Physical Trespass Requirement

The transition of Fourth Amendment theory from trespass to expectation of privacy began with the recognition that a narrow view of what constituted a trespass translated into a broad scope for warrantless searches.

In *Silverman v. United States*, the traditional requirement of a physical trespass to trigger Fourth Amendment protection was relaxed in response to technological advances.[28] Police had obtained evidence by using an electronic listening device.[29] The Court found no physical trespass but invalidated the search as an intrusion on a constitutionally protected area.[30] The approach is similar in theory to that taken in *United States v. Dunn*, which, while involving physical space, used language broadly defining curtilage as the area within which "intimate activity associated with 'the sanctity of a man's home and the privacies of life'" takes place.[31]

---

[24] Hester v. United States, 265 U.S. 57, 58 (1924) (upholding the warrantless seizure of whiskey bottles dropped by the defendant during a police chase because the bottles were abandoned).

[25] *See infra* Part II.

[26] Hoelzer v. City of Stamford, 933 F.2d 1131, 1138 (2d Cir. 1991).

[27] Although intent may be inferred if supported by facts, Baglin v. Cusenier Co., 221 U.S. 580, 597–98 (1911), it may also be defeated by facts showing that surrender of possession was not accompanied by an intention to give up ownership, Saxlehner v. Eisner & Mendelson Co., 179 U.S. 19, 34–35 (1900).

[28] 365 U.S. 505, 511–12 (1961).

[29] *Id.* at 506.

[30] *Id.* at 511–12.

[31] United States v. Dunn, 480 U.S. 294, 300 (1987) (quoting Oliver v. United States, 466 U.S. 170, 180 (1984)); *see also supra* notes 20–21 and accompanying text. The core language of "the sanctity of a man's home and the privacies of life" was taken from *Boyd v. United States*, 166 U.S. 616, 630 (1886). Courts have also recognized Fourth Amendment protection in common areas within apartment complexes, hotels, and motels.

Had the evolution of Fourth Amendment theory stopped there it would be tempting to argue that the protected area of curtilage extends beyond physical space. Under this view, the rise of cloud computing[32] could be seen as extending the traditional protection of the physical home into cyberspace. David Couillard advances the theoretical underpinning for recognition of this "virtual curtilage":

> Modern Internet users enjoy access to digital calendars, photographs, address books, correspondence in the form of e-mail messages, and diaries in the form of personal blogs. Such a list of items may sound familiar—it includes the same materials deemed "highly personal" by the Supreme Court . . . . The fact that such items are digital rather than physical should not change their status as highly personal objects . . . .[33]

This status, Couillard argues, is sufficient to bring at least certain Internet activities within the curtilage, which, before *Katz v. United States*, would establish Fourth Amendment protection and, under *Katz*, would be at least a factor supporting protection.[34]

However, while the transitional case of *Silverman* and its progeny still referred to concepts of trespass within the curtilage, the connection became strained in later cases in the face of technological advances that blurred the notions of trespass, the curtilage, and physical reality itself. The strain ultimately became too great in *Katz*, which abandoned the requirement of physical trespass theory as a prerequisite to invoking Fourth Amendment protection and replaced it with the current expectation of privacy test.[35]

See, e.g., United States v. Fluker, 543 F.2d 709, 716–17 (9th Cir. 1976) (common hallway of an apartment building); United States v. Carriger, 541 F.2d 545, 550 (6th Cir. 1976) (common area of an apartment building); Fixel v. Wainwright, 492 F.2d 480, 484 (5th Cir. 1974) (fenced yard of a multiunit apartment building). *But see* United States v. Holland, 755 F.2d 253, 255–56 (2d Cir. 1985) (no expectation of privacy in common hallway or lobby of an apartment building).

32 The term "cloud computing" arises from the use of a cloud icon as a symbol for the Internet in flow charts. It refers to a system in which data and software are stored remotely and accessed through the Internet rather than being located on the user's computer. Google's Gmail service is an example of a widely used cloud-computing application. *See infra* Part III.A.4.

33 Couillard, *supra* note 2, at 2219–20 (footnotes omitted).

34 *Id.* at 2220.

35 Katz v. United States, 389 U.S. 347, 353, 360 (1967). Trespass may still be relevant to the determination of the reasonableness of the expectation of privacy under the current *Katz* test. *Oliver*, 466 U.S. at 183 ("The existence of a property right is but one element in determining whether expectations of privacy are legitimate."). For an example of application by lower courts, see *United States v. Stevenson*, 396 F.3d 538, 546 (4th Cir.

C. The Expectation of Privacy Theory

The expectation of privacy analysis was explicitly decoupled from the concept of trespass within the curtilage in *Katz v. United States*.[36] In *Katz*, the area searched was nowhere near the defendant's home and was not owned by the defendant—the challenged evidence was obtained by wiretapping a public telephone booth.[37] The Court held the evidence improperly obtained because "the Fourth Amendment protects people, not places"[38] and what an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected," noting that the defendant had sought to exclude "the uninvited ear."[39]

Justice Harlan's concurring opinion is frequently cited as the clearer statement of the holding of the case: "My understanding of the rule that has emerged from prior decisions is that there is a twofold

---

2005) ("[T]he proper test for abandonment is not whether all formal property rights have been relinquished, but whether the complaining party retains a reasonable expectation of privacy in the [property] alleged to be abandoned. In making that determination, however, it is still relevant to consider a defendant's property interest." (alterations in original) (internal quotation marks and citation omitted)). For a further discussion of *Katz* and the expectation of privacy theory, see *infra* Part II.

[36] *Katz*, 389 U.S. at 353. For a detailed analysis of *Katz* and cases interpreting *Katz*, see Herdrich, *supra* note 10, at 1000–06. For attempts to distill guidance from *Katz*, see James A. Bush & Rece Bly, Note, *Expectation of Privacy Analysis and Warrantless Trash Reconnaissance After* Katz v. United States, 23 ARIZ. L. REV. 283, 287–88 (1981) (identifying seven *Katz* factors: (1) defendant's own conduct, (2) strength of physical barriers, (3) number of people with access, (4) number of people outside enclosure, (5) social inhibitions, (6) sensory enhancing, and (7) defendant's control of enclosure), and Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1080 (1987) (identifying three *Katz* factors: (1) place of intrusion, (2) nature and degree of intrusion, and (3) object of surveillance); *cf.* Rosemarie Falcone, Note, California v. Ciraolo*: The Demise of Private Property*, 47 LA. L. REV. 1365, 1371 (1987) (concluding that *Katz* provides no clear guidance).

[37] 389 U.S. at 348.

[38] *Id.* at 351. Concurring, Justice Harlan stated:

> I join the opinion of the Court, which I read to hold only (a) that an enclosed telephone booth is an area where, like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy; (b) that electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment; and (c) that the invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant.

Id. at 360–61 (citations omitted). Justice Harlan's concurrence was ultimately adopted by the Court in *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

[39] *Id.* at 351–52.

requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[40]

Not surprisingly, the focus in subsequent cases applying this two-pronged expectation of privacy test has tended to lie on the second, more objective prong of determining what society is willing to respect.[41]

In *Oliver v. United States*, police recovered marijuana plants from an open field on which the defendant had posted a "No Trespassing" sign.[42] Under the classic trespass cases, the sign would have been irrelevant—a search of open fields would have been viewed as permissible. The *Oliver* Court reached the same conclusion, but found it necessary to consider the effect of the "No Trespassing" sign. Although recognizing that the sign evidenced the defendant's personal desire for privacy, the Court held that society in general did not recognize the privacy of open fields and therefore a warrantless search was not improper.[43]

The expectation of privacy theory recognizes a special case comparable to the trespass theory's special case for abandoned property: voluntarily[44] conveying information to a third party

---

[40] *Id.* at 361 (Harlan, J., concurring); Hudson v. Palmer, 468 U.S. 517, 525 n.7 (1984); *Smith*, 442 U.S. at 740.

[41] The very subjectivity of the first prong and the unique "ownership" of proof (the person asserting a Fourth Amendment right could always claim to have had an expectation of privacy, and proof of a contrary mental state would be difficult) make it a less useful test than the second prong. However, this emphasis on the second prong is not without its critics. Professor LaFave argues that "[i]t would be a perversion of *Katz* to interpret it as extending protection only to those who resort to extraordinary means to keep information regarding their personal lives out of the hands of the police." WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.6(c) (4th ed. 2004). Professor LaFave further argues that in the cyberworld "password protection, and perhaps encryption of data should be no less reasonable than reliance upon locks, bolts, and burglar alarms, even though each form of protection is penetrable." *Id.* § 2.6(f) (quoting Randolph S. Sergent, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1200 (1995)). That view has been accepted by at least one lower court. *See* United States v. D'Andrea, 497 F. Supp. 2d 117, 121–23 (D. Mass. 2007).

[42] 466 U.S. 170, 173 (1984).

[43] *Id.* at 176–81.

[44] At least one district court has taken an expansive view of "voluntary." In *United States v. Hamilton*, 434 F. Supp. 2d 974, 979 (D. Or. 2006), the court found no reasonable expectation of privacy in home energy usage because the homeowner "voluntarily" conveyed this information to the utility company by merely using the electricity.

surrenders any expectation of privacy in the information.[45] Thus, if a person voluntarily conveys information to a third party, the government can obtain this information from the third party without violating the conveying party's privacy interests.[46] The Supreme Court upheld the use of pen registers to record outgoing telephone numbers in *Smith v. Maryland*, because the telephone user "voluntarily conveyed numerical information to the telephone company," exposing the information to the phone company's equipment.[47] A district court has applied similar reasoning to conclude that a homeowner had no reasonable privacy expectation in his or her home energy usage records because the homeowner voluntarily conveyed this information to the utility company by merely using the electricity.[48] Similar reasoning also led the Ninth Circuit to find no expectation of privacy in the address fields of e-mails.[49]

The issue of voluntary conveyance features prominently in the application of the Fourth Amendment to trash.

---

[45] United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("[W]hen an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities . . . . Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information."); United States v. Miller, 425 U.S. 435, 443 (1976) (noting that a bank customer has no reasonable expectation of privacy in records he voluntarily conveys to the bank, such as deposit slips, because "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government").

[46] Even if the government obtains the information by violating the third party's privacy interests, the person conveying the information has no standing to assert the third party's claim. *See generally* Rakas v. Illinois, 439 U.S. 128 (1978); Kerr, *supra* note 1, at 293–94.

[47] 442 U.S. 735, 744 (1979) ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.").

[48] *Hamilton*, 434 F. Supp. 2d at 980 (rejecting an argument that electricity use records revealed intimate facts about the home, making the action a search under *Kyllo v. United States*, 533 U.S. 27 (2001)).

[49] United States v. Forrester, 512 F.3d 500, 510–11 (9th Cir. 2008). The Ninth Circuit found an expectation of privacy in the content of text messages. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 907 (9th Cir. 2008). One reading that reconciles these cases is that content remains protected while the address information, analogous to an envelope, is open to the public and not protected.

II
SEARCH AND SEIZURE OF TRASH

Trash has proven difficult to fit into Fourth Amendment analysis.[50] While the Fourth Amendment protects property within the curtilage, and trash is typically placed at the edge of the curtilage in a container protecting it from public view (suggesting protection under a protected area analysis), it is also left with the expectation that a third party will take possession of it, thereby calling into question the reasonableness of any expectation of privacy.

The Supreme Court addressed this conflict in *California v. Greenwood*, where a search warrant was issued based on evidence obtained from trash that the defendant had placed outside the curtilage for removal.[51] While the Court upheld the warrant, it rejected the theory that the search of the trash was proper solely because the trash had been abandoned,[52] instead holding that trash was not protected by the Fourth Amendment because there could be no objective expectation of privacy—society would not consider it reasonable to have a subjective expectation of privacy in trash.[53] The Court noted that its conclusion was justified because "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public"; the voluntary surrender of trash to a third party (the garbage collector) renounces control over the property; and the police need not avert their eyes from what is readily accessible to the public and a third party.[54]

A contemporary review of the case summarizes its import:

---

[50] For a compilation of cases reflecting the struggle, see LAFAVE, *supra* note 41, § 2.6(c).

[51] 486 U.S. 35, 38 (1988). For an analysis of *Greenwood* and cases involving trash, see Kimberly J. Winbush, Annotation, *Searches and Seizures: Reasonable Expectation of Privacy in Contents of Garbage or Trash Receptacle*, 62 A.L.R.5th 1 (1998). For a detailed analysis of *Greenwood*, critical of the decision, see Herdrich, *supra* note 10.

[52] As a matter of general property law, abandonment of personal property relinquishes ownership to any subsequent finder or, by escheat, to the state. RESTATEMENT (FIRST) OF PROP.: ABANDONMENT § 504 (1944).

[53] *Greenwood*, 486 U.S. at 40.

[54] *Id.* at 40–41 (footnotes omitted). The *Greenwood* Court later cited *Katz v. United States*, 389 U.S. 347, 351 (1967), for the proposition that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Greenwood*, 486 U.S. at 41 (internal quotation marks omitted).

> Prior to . . . *Katz v. United States*, the [Fourth Amendment] extended only to unauthorized physical intrusions . . . into a "constitutionally protected area." *Katz* replaced this property-based test with an amorphous inquiry into whether the intrusion violated a "reasonable expectation of privacy." The new inquiry was two-pronged, extending [Fourth Amendment] protection to those interests in which a person manifests a subjective expectation of privacy that society recognizes as objectively reasonable. . . . Last Term, in *California v. Greenwood*, the Court found an asserted expectation of privacy in the contents of garbage bags left for collection outside the curtilage to be unreasonable. . . . *Greenwood* therefore stands for the proposition that trash searches require *no* justification.[55]

Greenwood's focus on the expectation of privacy rather than abandonment is surprising given the Court's repeated recognition of Fourth Amendment protection for closed containers regardless of location.[56] In dissent, Justice Brennan challenged the conclusion that society would not recognize as reasonable an expectation of privacy in trash, citing a local ordinance that appeared to protect the privacy of trash in general[57] and a century of cases protecting closed

---

[55] *Search and Seizure—Garbage Searches*, 102 HARV. L. REV. 191, 191–99 (1988) (footnotes omitted).

[56] In container search cases, the Supreme Court has repeatedly acknowledged that an individual has an expectation of privacy in a sealed container regardless of its nature. *See* United States v. Ross, 456 U.S. 798, 822 (1982) (stating that there is no distinction between "worthy" and "unworthy" containers); Robbins v. California, 453 U.S. 420, 428 (1981) (upholding an expectation of privacy in green opaque plastic wrapping); Arkansas v. Sanders, 442 U.S. 753, 766 (1979) (finding an expectation of privacy in an unlocked suitcase); United States v. Chadwick, 433 U.S. 1, 11 (1977) (recognizing an expectation of privacy in a locked footlocker).

[57] *Greenwood*, 486 U.S. at 45–46 (Brennan, J., dissenting). The Cheektowaga, New York, ordinance made it "unlawful and a violation of this article for any person without authority from the Town to collect, pick up, remove or cause to be collected, picked up or removed any rubbish." CODE OF THE TOWN OF CHEEKTOWAGA, NEW YORK § 206-7(E) (2005). Several states currently recognize privacy protection for trash under state constitutional provisions: Hawaii (State v. Tanaka, 701 P.2d 1274, 1276 (Haw. 1985)); Michigan (United States v. 987 Fisher Rd., 719 F. Supp. 1396, 1406–07 (E.D. Mich. 1989); MICH. CONST. art. I, § 11); New Jersey (State v. Hempele, 576 A.2d 793, 799–804 (N.J. 1990); N.J. CONST. art. I); New Mexico (State v. Granville, 142 P.3d 933, 944 (N.M. Ct. App. 2006); N.M. CONST. art. 2, § 10); Oregon (State v. Campbell, 759 P.2d 1040, 1049 (Or. 1988); OR. CONST. art. I, § 9); Vermont (State v. Morris, 680 A.2d 90, 100 (Vt. 1996); VT. CONST. ch. 1, art. XI); and Washington (State v. Hendrickson, 917 P.2d 563, 571 (Wash. 1996); WASH. CONST. art. 1, § 7). Indiana requires reasonable suspicion of criminal activity before police can conduct a trash-pull and also requires the police to remove the garbage in the same manner as the collector. Litchfield v. State, 824 N.E.2d 356, 363–64 (Ind. 2005).

containers.[58] In Justice Brennan's view, a garbage collector should be treated like a bailee, whose possession of personal effects in closed containers does not defeat the owner's Fourth Amendment right to protect the contents of the container.[59]

As Gordon MacDonald has observed,

> *Greenwood* suggests at least three approaches to analyzing trash cases, but fails to indicate which it ultimately regards as controlling. The first . . . was an application of *Katz*, under which the Court concluded that the defendant's privacy expectations were unreasonable. Second, . . . because the defendants "knowingly exposed" their garbage, their privacy expectations were necessarily defeated. Third, the Court, at least implicitly, endorsed a "bright line" test under which no privacy expectations can attach to garbage left outside the curtilage. . . . Two of the approaches . . .—the bright line and the knowing exposure tests—are inconsistent with a faithful application of the other approach—the *Katz* expectation of privacy test. The bright line test depends on the property based concepts of abandonment and curtilage. *Katz* forcefully rejected such property notions as controlling."[60]

The third of these approaches—the *per se* rule—is easiest to deal with. Professor LaFave finds fault with the argument that trash is no longer protected simply because it has been conveyed to the trash collector; in his view, the conveyance "might support the conclusion the police can enlist the aid of the garbage hauler . . . but it hardly means that the police may themselves intrude. There is no principle in Fourth Amendment jurisprudence to the effect that the police are free to do what *some* individual has been authorized to do."[61] Lower courts likewise appear troubled by a *per se* rule, focusing instead on either the public accessibility/constitutionally protected area inquiry or the reasonableness of the expectation of privacy inquiry.[62]

---

[58] *Greenwood*, 486 U.S. at 46–48 (citing *Ross*, 456 U.S. at 822–23; *Robbins*, 453 U.S. at 427; *Sanders*, 442 U.S. at 762 n.9; *Chadwick*, 433 U.S. at 11; *Ex parte* Jackson, 96 U.S. 727, 733 (1877)).

[59] *Id.* at 55 (Brennan, J., dissenting).

[60] Gordon J. MacDonald, Note, *Stray* Katz*: Is Shredded Trash Private?*, 79 CORNELL L. REV. 452, 469 (1994) (footnote omitted).

[61] LAFAVE, *supra* note 41, § 2.6(c) (footnotes omitted). He further notes: "In coming onto the curtilage and taking the trash, the collector is doing exactly what the householder contemplated." *Id.* In most jurisdictions, methods of trash disposal are limited by law, *see, e.g.*, MD. CODE ANN., Criminal Law § 10-110(c) (LexisNexis 2002), leaving few options for protecting trash from searches.

[62] United States v. Segura-Baltazar, 448 F.3d 1281, 1289 (11th Cir. 2006) (no bright-line rule for trash search cases); United States v. Hedrick, 922 F.2d 396, 399 (7th Cir.

Courts applying the "constitutionally protected area" test focus on whether trash placed at a curbside is abandoned and therefore not within the constitutionally protected area of the home.[63] At least one court has concluded, in the context of a civil dispute over ownership of trash, that disposal of trash abandons neither the trash itself nor the expectation of privacy with respect to its contents. *Sharpe v. Turley* involved the ownership of documents produced in an earlier case.[64] In that case, plaintiff's attorney (Turley) had subpoenaed documents that a nonparty (Sharpe) had taken from the defendant's trash dumpster.[65] At the conclusion of the case, Turley turned the documents over to the defendant rather than returning them to Sharpe, and Sharpe sued, arguing that the documents had been abandoned by the defendant and therefore Sharpe owned them.[66] The court granted summary judgment for Turley, holding that the documents had not been abandoned and noting that the dumpster was on the defendant's property and the defendant had contracted with a private party to convey trash from the dumpster to a private landfill.[67] This control indicated that the defendant had not intended to abandon the trash.[68]

Courts applying the "expectation of privacy" test focus on whether one could have an expectation of privacy in trash that has been left by the curb. Some state courts have found that the reasonableness of an expectation of privacy is enhanced by ordinances that prohibit

---

1991) (expectation of privacy must be evaluated notwithstanding intent to convey the garbage to the garbage collector). Some cases appear to combine the two analyses, finding that placing trash out for collection is abandonment and therefore inconsistent with an expectation of privacy. *See, e.g.*, United States v. Vahalik, 606 F.2d 99, 101 (5th Cir. 1979); United States v. Mustone, 469 F.2d 970, 972 (1st Cir. 1972); Winbush, *supra* note 51. ("The vast majority of courts have ruled that when garbage is located in a place accessible to the public, the individual who placed that garbage for collection either abandoned it or has no reasonable expectation of privacy therein, thus rendering any search and seizure of that trash lawful.").

[63] *See, e.g.*, United States v. Espriella, 781 F.2d 1432, 1437 (9th Cir. 1986) (holding that garbage placed outside for collection is abandoned property); *Vahalik*, 606 F.2d at 101 (holding that placing garbage out for collection is abandonment, which terminates any reasonable expectation of privacy); *Mustone*, 469 F.2d at 972 (expectation of privacy inconsistent with abandonment). The concept of protected areas may be traced back to *Hester v. United States*, 265 U.S. 57 (1924).

[64] 191 S.W.3d 362, 364 (Tex. App. 2006).

[65] *Id.*

[66] *Id.* at 366–67.

[67] *Id.* at 368.

[68] *Id.*

interference with trash containers,[69] even though this argument was rejected by the Supreme Court in *Greenwood*.[70] Some courts simply reject the argument that merely intending to convey the garbage to the trash collector is enough to defeat an expectation of privacy,[71] while others find that placing trash by the curb indicates intent to surrender privacy even in the face of clear efforts to prevent disclosure. In *United States v. Kramer*, the Seventh Circuit sustained an inside-the-curtilage search by holding that the protection of the Fourth Amendment does not extend to discarded garbage:

> Of course people sometimes do not want others to see things—*e.g.*, magazines, financial records, correspondence, doctor bills—that they sometimes throw away. But people can easily prevent this by destroying what they want to keep secret before they discard it, or by not discarding it. Defendant could have burned *or shredded* his drug records before he discarded them or kept them hidden somewhere inside his house.[72]

Many commentators likewise assumed that actions such as shredding would invoke Fourth Amendment protection against warrantless searches of trash, and several courts have based rulings upholding warrantless searches of trash on the argument that one wishing to preserve privacy could have shredded documents prior to disposing of them.[73]

However widely held, this assumption that shredding protects trash from warrantless searches is not the law and, in fact, has been rejected by the one circuit court that has ruled on the issue. In *United States v.*

---

[69] *See, e.g.*, State v. Hempele, 576 A.2d 793, 805 (N.J. 1990) (regulations against garbage picking support expectation that garbage will remain private). *But see* Rikard v. State, 123 S.W.3d 114, 121 (Ark. 2003) (city ordinances against garbage rummaging were not created to give citizens an expectation of privacy in their garbage).

[70] *See supra* notes 51–59 and accompanying text.

[71] *See, e.g.*, United States v. Hedrick, 922 F.2d 396, 399 (7th Cir. 1991) ("The *Greenwood* Court did not base its decision solely upon the conveyance of the garbage to the collector."). Of course, once actually conveyed to the garbage collector, trash would lose any privacy protection. *See supra* notes 44–49 and accompanying text.

[72] 711 F.2d 789, 792 (7th Cir. 1983) (emphasis added).

[73] *See, e.g.*, *id.*; United States v. Terry, 702 F.2d 299, 309 (2d Cir. 1983); State v. DeFusco, 620 A.2d 746, 753 n.19 (Conn. 1993). More generally, in distinguishing discarded trash from cord blood stem cells, one commentator noted, "If the owner of the article, item, or material did not want it to be accessible to others, he or she could burn, shred, or dispose of the trash in any number of other ways that would render the items useless." Kimberly J. Cogdell, *Saving the Leftovers: Models for Banking Cord Blood Stem Cells*, 39 U. MEM. L. REV. 229, 246 (2009).

Scott, the court upheld a warrantless search, seizure, and reconstruction of shredded documents that had been placed in the defendant's trash, rejecting the argument that shredding demonstrated an expectation of privacy.[74]

The *Scott* trial court found persuasive authority for a reasonable privacy interest in shredded documents[75] and met *Greenwood*'s observation that "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public"[76] with its own observation that "it is not 'common knowledge' that snoops and scavengers may retrieve shredded materials and then 'painstakingly reconstruct' them to learn the contents."[77] On appeal, the First Circuit acknowledged, "The fact that the abandoned property was partially destroyed by shredding . . . constitut[ed] evidence of [Scott's] subjective desire or hope that the contents be unintelligible to third parties," but the court concluded that this subjective desire "does not change the fact that it is as a result of [Scott's] own actions that the shredded evidence was placed in the public domain."[78] "[I]mplicit in the concept of abandonment is a renunciation of any reasonable expectation of privacy in the property abandoned."[79] The First Circuit concluded that Scott "discarded [his] garbage in an area particularly suited for public inspection and consumption. . . . The Fourth Amendment . . . does not protect appellant when a third party expends the effort and expense to solve the jigsaw puzzle created by shredding."[80]

As Gordon MacDonald notes,

---

[74] 975 F.2d 927, 929 (1st Cir. 1992) (holding that because the "trash [was] left for collection in a public place and over which its producer had relinquished possession," the defendant also relinquished any expectation of privacy). Clearly, the court must have been evaluating the privacy expectation from an objective perspective rather than the subjective intent of the defendant. For a detailed analysis of the *Scott* case, see MacDonald, *supra* note 60, at 452–56.

[75] United States v. Scott, 776 F. Supp. 629, 632 (D. Mass. 1991) (citing Pleasant v. Lovell, 876 F.2d 787, 802 (10th Cir. 1989)).

[76] California v. Greenwood, 486 U.S. 35, 40 (1988) (footnotes omitted).

[77] *Scott*, 776 F. Supp. at 632.

[78] *Scott*, 975 F.2d at 929.

[79] *Id.* (quoting United States v. Mustone, 469 F.2d 970, 972 (1st Cir. 1972)).

[80] *Id.* at 930 ("At most, appellant's actions made it likely that most third parties would decline to reconstitute the shredded remnants into a legible whole."); *see also* Cogdell, *supra* note 73.

> The [court] was onto the right idea—that there are affirmative privacy-seeking steps to protect an individual's interests even under an abandonment analysis. Unfortunately, the court failed to carry its reasoning to its logical conclusion. It is hard to conceive what act, beyond "mere" shredding, would evince an intent to retain privacy.[81]

III
IMMANENT TRASH, DISPOSAL IN GENERAL, AND CYBERTRASH

It is tempting to translate the trash cases into other areas where property is discarded. The appeal is obvious, if superficial: all of the cases deal with the consequences of a decision to dispose of property. The natural temptation to import the physical trash rules into the law of cybertrash is amplified by the choice of a trash can as the icon for file deletion in the ubiquitous Apple and Microsoft Windows operating systems. Implicit in the argument for portability is the assumption that the disposal decision is the same in all cases. To determine whether the physical trash cases appropriately translate to cybertrash, it is helpful to analyze, as potential models, other areas where the translation has been attempted, approaching the ultimate question of the degree of protection afforded cybertrash by first looking at how the degree of protection for discarded material in general is determined, using the examples of immanent trash, wastewater, and shed genetic material. With that background, it will be possible to define trash in a relevant way and use that definition to develop a generalized rule and apply it to cybertrash. As discussed below,[82] the result is a dual rule, and one that separates cybertrash from the other forms of disposal.

A. Potential Models and Problems in Translation

1. Immanent Trash

As discussed in detail above, the degree of protection afforded to trash is unsettled and still in search of a clear theoretical basis. Commentators,[83] as well as the *Greenwood* Court itself,[84] disagree on

---

[81] MacDonald, *supra* note 60, at 488.

[82] *See infra* Part III.B.

[83] *Compare* Cogdell, *supra* note 73, at 245–46 ("Presumably, if one throws something in the trash, the nature of its content is open to the public."), *with* Hope Lynne Karp, Note,

the intent involved in disposal of trash, and the requisite level of intent may well have changed over time. *Greenwood* would have been an uncontroversial decision had the case arisen in the prior century. As Professor Strasser notes,

> [B]efore the twentieth century . . . [o]bjects of no use to adults became playthings for children. Broken or worn-out things could be brought back to their makers, fixed by somebody handy, or taken to people who specialized in repairs . . . items beyond repair might be dismantled, their parts reused or sold to junk men. This trade in used goods amounted to a system for reuse and recycling . . . scavenging was essential to that system, a chore and a common pastime for poor children, who foraged for shreds of canvas or bits of metal on the docks, for coal on the railroad tracks, and for bottles and food on the streets and in the alleys.[85]

This system remained in place until the turn of the century, when municipal sanitation workers did away with the need for "swill children."[86] Thus, it would have been unsurprising to conclude that there was no expectation of privacy in trash in the nineteenth century—the norm was that disposal of trash was intended to surrender ownership to anyone who wanted to take possession. The development of a system of public garbage collection and disposal did not begin in the United States until the late-nineteenth century,[87] and as late as 1891 *Scientific American* reported, "There is probably not a city of any size in the United States where the disposal of wastes is satisfactory."[88] However, by 1984,[89] the norm was not only formalized governmental pickup of trash, but in many states and

---

Trash: A Matter of Privacy?, 20 PACE L. REV. 541, 547 (2000) ("[The information contained in trash] is conveyed to the garbage collector for the purpose of eliminating it from one's life—forever.").

[84] *Compare* California v. Greenwood, 486 U.S. 35, 35–45 (1988), *with id.* at 45–56 (Brennan & Marshall, JJ., dissenting).

[85] SUSAN STRASSER, WASTE AND WANT: A SOCIAL HISTORY OF TRASH 12, 13 (1998).

[86] *Id.* at 13.

[87] Martin V. Melosi, GARBAGE IN THE CITIES: REFUSE, REFORM, AND THE ENVIRONMENT 23 (rev. ed. 2005).

[88] *Disposal of Refuse in American Cities*, SCI. AM., Aug. 29, 1891, at 136.

[89] The search of trash in *Greenwood* took place in April 1984, although the case did not reach the Supreme Court until 1988. *Greenwood*, 486 U.S. at 37.

municipalities, laws that forbade third parties to interfere with this governmental function.[90]

Cybertrash has no such history. There was never a time when owners of electronic files expected that others might take possession of the files uninvited.

2. Wastewater

Wastewater is a broad category of material that is discarded. A thread of search and seizure cases involving wastewater may help clarify the underlying principles of disposal cases in general.

In *Riverdale Mills v. Pimpare*, Riverdale Mills discharged wastewater into a municipal sewer system after pretreatment in its private, on-site, treatment system.[91] The Environmental Protection Agency (EPA) took samples from a manhole located in a public street between the private treatment system and the municipal system.[92] Using reasoning similar to the argument that trash left at the curb for pickup is no longer private, the court held that the EPA's sampling did not violate Riverdale Mills' Fourth Amendment rights because the wastewater had left Riverdale Mills' property and was "irretrievably" flowing into the public sewer, where any member of the public could sample it.[93]

In *United States v. Spain*, the EPA sampled at the location where Crown Chemical's sewer lines joined the public sewer system.[94] The court held that this sampling did not constitute a search, citing *Riverdale* and noting that "the facts of this case are even more compelling . . . because the EPA tested Crown's wastewater *at the exact point* where that wastewater became public property."[95]

In *United States v. Hajduk*, the court applied the *Riverdale* principle to hold that samples taken beyond the discharger's property did not require a warrant, but those taken on the discharger's property did, distinguishing between locations where the discharger had the

---

[90] Elizabeth Gibson, *Law Closes in on Bexley's Trash Man*, THE COLUMBUS DISPATCH, Jan. 19, 2009, http://www.dispatch.com/content/stories/local/2009/01/19/trash_man.ART_ART_ 01-19-09_B1_21CJ3BA.html (last visited Aug. 5, 2011).

[91] 392 F.3d 55, 56–57 (1st Cir. 2004).

[92] *Id.* at 58.

[93] *Id.* at 64.

[94] 515 F. Supp. 2d 860, 864 (N.D. Ill. 2007).

[95] *Id.* at 868.

power to prevent flow to the public sewer and those where it did not.[96]

These cases appear to draw a line at the point where the waste stream has been irrevocably committed to reaching an area from which the public cannot be excluded. If this is the guiding principle, then cybertrash should be safe. Notwithstanding its location beyond the physical boundary of the house, and notwithstanding its accessibility by third parties, it is not accessible to the public.

3. Shed DNA

If the term "discarded" is viewed broadly, then another category of routinely discarded material is DNA that is constantly shed in the form of hair and skin cells. "[W]e can't go anywhere . . . without leaving a bread-crumb trail of identifying DNA matter."[97] Judge Kozinski, dissenting in *United States v. Kincade*, warned, "If we have no legitimate expectation of privacy in such bodily material, what possible impediment can there be to having the government collect what we leave behind, extract its DNA signature and enhance CODIS to include everyone?"[98] Yet DNA is routinely collected from crime scenes without raising Fourth Amendment issues, and collecting this "abandoned" DNA has been held not to require a warrant.[99] Courts have also approved warrantless collection of DNA samples obtained by police who retrieved them from items deliberately given to suspects.[100]

Whether there is a general rule equating shed DNA with trash (and therefore exposing it to warrantless search and seizure) is as yet undecided. A number of states have enacted legislation protecting DNA as property,[101] but in the absence of specific legislation, the law

---

96 396 F. Supp. 2d 1216, 1226–27 (D. Colo. 2005).

97 United States v. Kincade, 379 F.3d 813, 873 (9th Cir. 2004) (Kozinski, J., dissenting).

98 *Id.*

99 *See* Mincey v. Arizona, 437 U.S. 385, 392 (1978); *Kincade*, 370 F.3d at 819; State v. Perry, 502 So. 2d 543, 556–57 (La. 1986).

100 *See* People v. Ayler, 799 N.Y.S.2d 162, *5 (N.Y. App. Div. 2004) (denying motion to suppress evidence obtained from DNA on cigarettes offered to defendant during a police interview); Richard Willing, *Police Dupe Suspects into Giving up DNA*, USA TODAY, Sept. 11, 2003, at A3; Richard Willing, *As Police Rely More on DNA, States Take a Closer Look*, USA TODAY, June 6, 2000, at 1A.

101 *See* ALASKA STAT. § 18.13.010(a)(2) (2004) ("[A] DNA sample and the results of a DNA analysis performed on the sample are the exclusive property of the person sampled

of ownership and control of DNA is unsettled. A federal district court dismissed a complaint claiming ownership of tissue that had been donated for research purposes but then used for additional commercial purposes, because "the property right in blood and tissue samples also evaporates once the sample is voluntarily given to a third party."[102]

In arguing for restrictions on the collection of abandoned DNA, Elizabeth Joh observes that "legal discussion is hampered by a misleading analogy between abandoned DNA and garbage" and that analysis of rights in DNA "should address the question of whether more appropriate analogies to abandoned DNA exist other than trash."[103] Joh notes an important distinction:

> Courts may readily find that criminals have clearly intended to renounce all privacy claims to bags containing illegal firearms or to packages of drug paraphernalia when fleeing the police, but we hardly have a realistic choice in shedding DNA. One can shred private papers or burn garbage so that no one may ever delve into them, but leaving DNA in public places cannot be avoided.[104]

Such an argument would apply to cybertrash as well. It is impossible to create electronic files without leaving traces—if not in public places, at least in places where the owner does not maintain absolute control. Files created in cyberspace are typically subject to backup procedures that are beyond the owner's control and which create copies that persist for a significant period of time after the owner deletes the original.[105]

---

or analyzed."); COLO. REV. STAT. § 10-3-1104.7(1)(a) (2009) ("Genetic information is the unique property of the individual to whom the information pertains."); FLA. STAT. § 760.40(2)(a) (2009) ("[Genetic testing results] are the exclusive property of the person tested."); GA. CODE ANN. § 33-54-1(1) (1995) ("Genetic information is the unique property of the individual tested."); LA. REV. STAT. ANN. § 22:1023(E) (2009) (describing genetic information as "property" of the person tested); OR. REV. STAT. 192.537(1) (2009) ("[A]n individual's genetic information and DNA sample are private and must be protected, and an individual has a right to the protection of that privacy.").

102 Greenberg v. Miami Children's Hosp. Research Inst., 264 F. Supp. 2d 1064, 1075 (S.D. Fla. 2003).

103 Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U.L. REV. 857, 860, 862 (2006).

104 *Id.* at 867 (footnote omitted).

105 For an example of the propagation of backup copies and the time taken to remove them, see Rajen Sheth, *Disaster Recovery by Google*, OFFICIAL GOOGLE ENTERPRISE BLOG (Mar. 4, 2010), http://googleenterprise.blogspot.com/2010/03/disaster-recovery-by-google.html, which outlines Google's backup procedures.

4. Cybertrash

A troubling argument by analogy to physical trash runs as follows: Imagine that an individual receives an e-mail and, as many individuals do, prints a copy. The next day, the individual deletes the e-mail and places the printout in the trash can and places the trash can at the curb for disposal by the municipal trash collector. Under *Greenwood*, the printout may be retrieved without a warrant. Why, the argument would continue, should a warrant be required for one form of trash but not the other?

One subissue can be disposed of easily. Storage of the deleted file at a common facility (the individual's e-mail provider or Internet service provider) should be irrelevant. Courts have recognized that Fourth Amendment protection can exist in common areas such as those found within apartment complexes, hotels, and motels.[106]

Resolving the main issue, however, requires analysis of the nature of cybertrash. Cybertrash is data—files, applications, and communications—created in cyberspace and then deleted. The volume of cyberspace data has increased dramatically with the introduction of the concept of "cloud computing": applications and data stored online and accessible remotely on what is known as a cloud platform.[107] Because the applications and data are stored online, a user can access them from anywhere with an Internet connection. Cloud platforms are offered by IBM,[108] Google,[109] and Microsoft,[110] among others.[111]

---

[106] *See, e.g.*, United States v. Fluker, 543 F.2d 709, 716–17 (9th Cir. 1976) (common hallway of an apartment building); United States v. Carriger, 541 F.2d 545, 550 (6th Cir. 1976) (common area of an apartment building); Fixel v. Wainwright, 492 F.2d 480, 484 (5th Cir. 1974) (fenced yard of a multiunit apartment building). *But see* United States v. Holland, 755 F.2d 253, 255–56 (2d Cir. 1985) (no expectation of privacy in common hallway or lobby of apartment building).

[107] *Rebooting Their Systems*, ECONOMIST, Mar. 12, 2011, at 73, 73.

[108] *IBMSmartCloud*, IBM, http://www-935.ibm.com/services/us/cloud/index.html (last visited Aug. 5, 2011).

[109] Kate Greene, *Google's Cloud Looms Large*, TECH. REV. (Dec. 3, 2007), http://www.technologyreview.com/Biztech/19785/?a=f (last visited Aug. 5, 2011).

[110] *Cloud Power*, MICROSOFT, http://www.microsoft.com/en-us/cloud/default.aspx (last visited Aug. 5, 2011).

[111] *See, e.g.*, Alex Williams, *A Bursting Market: Cisco Building APIs for Cloud Infrastructure Automation*, READWRITE, (Mar. 8, 2011, 8:45 AM), http://www.readwriteweb.com/cloud/2011/03/cisco-building-apis-for-cloud.php.

When data is placed on a cloud platform, it is typically maintained by a third party, with the maintenance including storage at mirror sites and regular backups of the data to protect against loss.[112] The owner of the data can remotely issue an instruction to delete the data, but deletion does not result in destruction.[113] Initially, it is merely an instruction to make the physical space on which the data is stored available for reuse, and until the space is reused, the data remains intact.[114] Furthermore, servers do not typically delete the files on backups, but rather periodically recycle the backup media.[115] Again, until the media is actually reused, the data remains intact.[116]

This leads to a further complication when dealing with cybertrash: the question of when and where cybertrash disposal takes place. Cybertrash is not physically stored at the owner's location, and while the owner may retain legal control over the information, it is control by virtue of contractual agreements and passwords.[117] Furthermore, the entity that has physical control over the facilities where the information is stored typically will maintain mirror sites against the possibility of power failures, fires, or other disasters and make backup copies that are stored off-site.[118] The owner's instruction to delete a

---

112 *Rebooting Their Systems*, *supra* note 107.

113 *See* SIMSON GARFINKEL, GENE SPAFFORD & ALAN SCHWARTZ, PRACTICAL UNIX AND INTERNET SECURITY 678 (3d ed. 2003) ("When a file is deleted, the contents are not immediately overwritten. Instead, the data records are added back into the freelist on disk. If they are not reused yet . . . you can still read the contents."). For an example of a cloud storage and backup policy, see the Google policy, *supra* note 105.

114 *Deleted Files Can Be Recovered*, AKDART.COM, http://www.akdart.com/priv9.html (last visited Aug. 5, 2011).

115 *Id.*

116 *See, e.g.*, *id.*

117 The physical facility operates as the agent for the owner of the data and would have a fiduciary duty to follow the owner's instructions as to disposal. Mere encryption has been held insufficient to establish the requisite expectation of privacy to invoke Fourth Amendment protection, and the refusal to recognize shredding as evidencing a sufficient expectation of privacy in *United States v. Scott*, 975 F.2d 927, 929 (1st Cir. 1992), would provide a powerful analogy to support warrantless decryption or cracking of passwords. *See supra* notes 73–81 and accompanying text.

118 *See* GARFINKEL, SPAFFORD & SCHWARTZ, *supra* note 113, at 551–52.

> It may take a week or a month to realize that a file has been deleted. Therefore, you should keep some backup tapes for a week, some for a month, and some for several months. Many organizations make yearly or quarterly backups that they archive indefinitely. After all, tape is cheap. Some organizations decide to keep their yearly or biannual backups 'forever'—it's a small investment in the event that they should ever be needed again.

file must propagate through this system to affect all of these locations.[119]

To understand why, notwithstanding the appeal of a single rule for all discarded property, cybertrash rules should not be the same as immanent trash rules requires exploration of a seemingly trivial question: What is trash?

B. What Is Trash?

Greenwood and its progeny do not attempt to define trash—they begin their analysis with the proposition that the items of interest are "trash" and then analyze where the trash was left and what expectations the prior owner and society in general might have had regarding its disposition. In the immanent world, the lack of definition is unimportant, and intuitive definitions are quite satisfactory and rarely raise issues. As valuable property moves from the tangible world to the intangible, and especially as intangible property moves from local embodiments[120] to the "cloud," the definition of trash and the rights of "trashholders" become important.

For something that is so ubiquitous, trash is remarkably undefined. There is no absolute right to create trash. The right must arise as inherent in the notion of property, which includes the right of alienation. However, neither the right to destroy[121] nor the right to

---

Id.; *see also* Google policy, *supra* note 105.

[119] Even files on one's own computer may not be under the owner's complete control, depending on the operating system. Most operating systems can be set to create automatic backup files, and most operating systems create system files that are hidden from the user and carry out functions such as creating page files to speed up access and display or creating system images that are stored on the hard drive as "hibernate" files when system power falls below a specified level. Many programs also automatically create files that facilitate their functioning without direct request by the user—for example, Internet cookies.

[120] Examples of local tangible embodiments of intangible property include data saved on a disk drive and music stored on a CD or MP3 player. The tangible embodiment and the intangible property (in this case a copyright) are distinct properties. *See generally* 17 U.S.C. § 1001 (2006).

[121] *See generally* 17 U.S.C. § 106A (2006) (prohibiting the destruction of certain works of art).

dispose of[122] are absolute attributes of physical property, even in the absence of third-party rights.[123]

There are several ways to categorize trash: biodegradable or not, recyclable or not, usable or not, hazardous or not. In the physical world, these categories matter, and limitations on how trash may be disposed of are imposed by statute based on these distinctions.[124] In the nonphysical world of cybertrash, only one of these distinctions matters. All cybertrash is biodegradable, recyclable, and nonhazardous. The critical division is between cybertrash that might be used by others and that which might not. To understand why this distinction matters in cyberspace, consider the reasons that people dispose of trash.

Conceptually, there are two broad categories of trash disposal: disposal that is meant merely to part with ownership and possession, and disposal that is meant to destroy the discarded trash. While *Katz* holds that the trash owner's subjective intent is insufficient to invoke Fourth Amendment protection, that intent is still relevant. In the physical world it is relevant because *Katz* requires a subjective intent to maintain privacy in addition to an expectation of privacy that society deems objectively reasonable;[125] in the cyber world, it is determinative.

1. Trash as a Surrender of Ownership

An example of trash disposal falling into the "surrender" category would be a discarded old newspaper. The owner of the old newspaper finds no further value in the property and simply wants to part with possession and, in the process of doing so, is also willing to part with ownership—the owner does not care if someone else sees value in the discarded newspaper and wishes to take possession and ownership. Similarly, if a lamp breaks and the owner does not value it sufficiently to repair it, and instead places it by the curb for trash pickup, the owner typically would not object if a passerby saw

---

122 *See generally* 42 U.S.C. § 6901 (2006) (prohibiting disposal of certain substances without a permit and compliance with government-set requirements).

123 The existence of third-party rights can, of course, limit the right to destroy or dispose of property that one owns. Examples of categories of third-party rights are liens, co-ownerships, and leases.

124 *See, e.g.*, 42 U.S.C. § 6901 (2006).

125 Katz v. United States, 389 U.S. 347, 361 (1967). *See generally supra* Part I.C.; Couillard, *supra* note 2.

sufficient value in the broken lamp and took possession and ownership in order to repair it. Case law is consistent with this general presumption and generally treats trash as abandoned property open to appropriation by others (including government investigators),[126] either by virtue of abandonment under the trespass theory[127] or surrender under the expectation of privacy theory.[128]

As discussed above, voluntarily conveying information to a third party surrenders the right to claim Fourth Amendment protection for the information.[129] While Justice Brennan criticized reliance on abandonment as a rationale for depriving trash of Fourth Amendment protection, it is one of the rationales offered by the Court in *California v. Greenwood*,[130] and if cybertrash is viewed as a disposal of ownership and possession, it is a rationale that would lead to the conclusion that cybertrash may be searched without a warrant.

2. Trash as an Instruction to Destroy

There is a second category of disposal, where the intent is not to release possession and ownership but rather to destroy the discarded item so that no one may own it. Disposal of personal documents would usually fall into this category.

The wastewater cases and, inherently, the physical trash cases, highlight an important second aspect of disposal: destruction of the link between the disposed property and its former owner. The wastewater cases illustrate one reason why it is important: when the link is broken, so is the evidentiary value of the property. Likewise,

---

126 *See, e.g.*, United States v. Redmon, 138 F.3d 1109, 1111–12 (7th Cir. 1998); United States v. Walker, 624 F. Supp. 99, 101–02 (D. Md. 1985); Rikard v. State, 123 S.W.3d 114, 119–20 (Ark. 2003); People v. Rooney, 221 Cal. Rptr. 49, 53–54 (1985); People v. Huddleston, 347 N.E.2d 76, 80–81 (Ill. App. Ct. 1976); State v. Sampson, 765 A.2d 629, 635 (Md. 2001).

127 *See supra* Part I.B.

128 *See supra* Part I.C.

129 United States v. Jacobsen, 466 U.S. 109, 114–15 (1984) (package delivered to a private carrier); Smith v. Maryland, 442 U.S. 735, 742–43 (1979) (telephone numbers called); United States v. Miller, 425 U.S. 435, 443 (1976) (bank records); United States v. Hamilton, 434 F. Supp. 2d 974, 979 (D. Or. 2006) (electricity records); *see also supra* notes 44–49 and accompanying text.

130 California v. Greenwood, 486 U.S. 35, 49 n.2 (1988) (Brennan, J., dissenting). Justice Brennan noted, "Of 11 Federal Court of Appeals cases cited by the Court . . . 7 rely entirely or almost entirely on an abandonment theory that . . . the Court has discredited." *Id.* (citations omitted); *see also Sampson*, 765 A.2d at 634 (noting that the trash cases are based less on the property concept of abandonment than on public accessibility).

the reason for seizing trash before it is mixed with others' trash is to preserve its evidentiary link to a particular individual or individuals.

Thus, where the intent associated with disposal is to destroy, it may evidence either the intent to physically destroy or simply the intent to destroy the one-to-one link between the physical object and its owner. Either is evidence of intent to maintain privacy and therefore satisfies *Katz* and the first prong of the *Greenwood* test.

IV
SEARCH AND SEIZURE OF CYBERTRASH

A. Encryption and the Curtilage

There are two arguments in favor of protection of deleted files that, under current theory, do not appear to be sufficient to establish Fourth Amendment protection.

One appealing argument is that the information is private.[131] Transmission from and to the owner is typically encrypted.[132] The argument has even been accepted in dissent that there is a general expectation of privacy in trash in general.[133] However, at least under the current "objective expectation of privacy" standard, this argument would not be sufficient. Even shredding trash has been held

---

131 In most cases the information would meet the Uniform Trade Secrets Act definition of trade secret information. *See* UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 538 (2005). The Act provides that a trade secret is created when confidential information is subject to reasonable steps to protect its confidentiality. *Id.* Password protection and encryption, in most cases, are considered reasonable steps to maintain confidentiality. *See, e.g.*, Optos, Inc. v. Topcon Med. Sys., Inc., No. 10-12016-DJC, 2011 U.S. Dist. LEXIS 22263, at *52–53 (D. Mass. 2011); I-Systems, Inc. v. Softwares, Inc., No. 01-1951, 2004 U.S. Dist. LEXIS 6001, at *46–47 (D. Minn. 2004).

132 Sensitive information may be transferred using SSL (secure socket layer) or SHTTP (secure HTTP) protocols. Data may also be encrypted prior to transmission using widely available encryption software.

133 *See* State v. DeFusco, 620 A.2d 746, 757–58 (Conn. 1993) (Katz, J., dissenting). Justice Katz argued,

> The majority suggests . . . that it is also reasonable for society to expect citizens to take affirmative steps—such as shredding or destroying—to hide garbage that they wish to keep private. How many of us, as Connecticut residents, feel the need to shred or destroy personal information before discarding it in order to protect its confidentiality? The very fact that Connecticut residents customarily discard highly personal and typically confidential information into their garbage without first shredding or destroying it, is a strong indication that they expect these items to remain private.

Id. (footnote omitted).

insufficient to establish an objective expectation of privacy,[134] and while encryption might delay interpretation of the data,[135] it does not suffice to prevent its seizure and attempt to interpret it.[136]

A second appealing approach is to update the definition of the curtilage so as to consider data stored off-site but accessible through the Internet as part of the area immediately surrounding the home, in effect bringing the ISP within the curtilage.[137] This approach was at least implicitly rejected in *Smith v. Maryland*.[138] While the focus of the case was on the absence of an expectation of privacy in information (the telephone numbers dialed by the defendant) conveyed to a third party (the phone company),[139] the information was being sent over equipment that at least in part was located in the defendant's home and all of which was connected to the defendant's home. In *United States v. Forrester*, a federal circuit court relied on

---

134 *See* United States v. Scott, 975 F.2d 927, 929 (1st Cir. 1992).

135 Shredding certainly must have delayed interpretation of the documents seized in *Scott*. *See supra* notes 74–81 and accompanying text.

136 Kerr, *supra* note 1, at 532 (traditional view that encryption does not create reasonable expectation of privacy applies to the Internet). David Couillard argues that Kerr misses the point: encryption should not be analogized to a physical lock and key but rather to opacity. Couillard, *supra* note 2, at 2226.

> Hypothetically, if a briefcase is locked with a combination lock, the government could attempt to guess the combination until the briefcase unlocked; but because the briefcase is opaque, there is still a reasonable expectation of privacy in the unlocked container. In the context of virtual containers in the cloud, however, encryption is not simply a virtual lock and key; it is virtual *opacity*.

Id. More generally, attempts to hide information have been held insufficient in several aerial surveillance cases where the information was successfully hidden from ground-level view. *See* Florida v. Riley, 488 U.S. 445, 450–51 (1989) (visible by helicopter); California v. Ciraolo, 476 U.S. 207, 209, 214 (1986) (visible by plane flying above a yard enclosed by a ten-foot fence).

137 *See* Couillard, *supra* note 2; Olmstead v. United States, 277 U.S. 438, 444–45 (1928) (protecting the new technology of personal telephone conversations). Although decided after *Smith v. Maryland*, 442 U.S. 735 (1979), *Oliver v. United States* sets forth the traditional understanding of curtilage: "the area around the home to which the activity of home life extends." 466 U.S. 170, 182 n.12 (1984). Subsequently, the Court defined the curtilage as the area "so intimately tied to the home itself that it should be placed under the home's 'umbrella' of Fourth Amendment protection." United States v. Dunn, 480 U.S. 294, 301 (1987). As discussed above, the *Dunn* definition is circular and does not compel a different result.

138 *See* 442 U.S. 735.

139 *Smith*, 442 U.S. at 744 ("[P]etitioner voluntarily conveyed numerical information to the telephone company . . . . In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.").

Smith to distinguish between the address fields in e-mails and the content of e-mail messages, holding that e-mailers "have no expectation of privacy in the to/from addresses of their messages . . . because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."[140] These cases may be seen as applications of the more general principal announced in *Horton v. California*: there is a distinction between a container and its contents, and exposure of the container to the public does not surrender the privacy of the contents.[141]

These cases may provide support for an argument establishing an expectation of privacy, but they appear to reject the concept of an expanded curtilage. Furthermore, basing Fourth Amendment protection on a redefinition of curtilage would require a retreat from the *Katz* expectation of privacy theory to the earlier physical trespass theory.

B. The Presumption of Destruction and Objective Expectations

While the relatively low percentage of personal documents in physical trash may support *Greenwood*'s conclusion that the default with respect to the physical world is an intent to—or at least indifference to—transfer, it is likely that the reverse is true in cyberspace. There, most cybertrash consists of files containing personal or private information, so the reasonable conclusion would be that the default assumption should be that disposal reflects an intent to destroy. For example, the default objective of "trashing" e-mails and files is more likely to be a desire to destroy rather than abandon. The reasons are simple: cyberproperty takes little physical space, so the incentive to dispose of it to make room is less pressing than with physical property. Cyberproperty does not decay, so the incentive to dispose of it to avoid having it spoil is not present. The reason for deleting a file is normally to make it disappear, not to transfer ownership, much less to make it available to the general public, and even less to transfer ownership to a third party who could then deny access to the original owner.[142]

---

140 United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

141 496 U.S. 128, 141 n.11 (1990) (mere seizure of container does not of itself authorize opening it without a warrant).

142 *See, e.g.*, Campbell v. Cochran, 416 A.2d 211, 222 (Del. Super. Ct. 1980).

It was therefore reasonable for the *Katz* Court to impose the dual requirements of subjective expectation of privacy and objective societal recognition of the claim to privacy, because there were two possible answers to the inquiry, what did the owner expect? It was defensible for the *Greenwood* Court to conclude that there was no reasonable expectation of privacy, and therefore no Fourth Amendment protection, with respect to physical trash, because it was possible to conclude that trash left unprotected in the open might not be considered private. In a world where there can be no question as to expectations and no ambiguity as to intent, neither result could be defended. The cyberworld is such a world.

The ambiguity of immanent trash disposal does not arise with respect to cybertrash. One would not expect "animals, small children and scavengers" to rummage through cybertrash in search of something edible or reusable. It is hard to imagine that an owner's choice to delete information was meant to release the information for possible reuse by someone else—the intent is always to make the information disappear.[143]

Nor could the second prong of the two-part test announced in *Katz* and apparently the critical inquiry regarding Fourth Amendment protection for trash—the societal acceptance of an expectation of privacy—be in doubt. Few issues in cyberspace have attracted as much attention as the risk of identity theft[144] and the related issue of government access to private information.[145] Protection against spyware is a billion-dollar-a-year industry; hundreds of articles appear annually in the popular press; the FTC website offers tips for avoiding identity theft. If society were prepared to accept as reasonable an expectation of privacy in anything, online personal information would have to be at or near the top of the list. This concern over online

---

[143] If the intent were to make the information available for use by others, it would be e-mailed or posted on a website, not deleted.

[144] *See, e.g.*, Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 ALB. L.J. SCI. & TECH. 61 (2011); Mark MacCarthy, *Information Security Policy in the U.S. Retail Payments Industry*, 2011 STAN. TECH. L. REV. 3; Gary M. Victor, *Identity Theft, Its Environment and Proposals for Change*, 18 LOY. CONSUMER L. REV. 273 (2006).

[145] *See, e.g.*, James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459 (2004); Patrick P. Garlinger, Note, *Privacy, Free Speech, and the Patriot Act: First and Fourth Amendment Limits on National Security Letters*, 84 N.Y.U. L. REV. 1105 (2009); Michael Traynor, *The First Restatements and the Vision of the American Law Institute, Then and Now*, 32 S. ILL. U. L.J. 145 (2008).

identity theft, and the resulting expectation that online transactions remain private, distinguishes cybertrash from *Greenwood*. Given the scope of concern[146] and resulting federal legislation,[147] it would be difficult to argue that society did not recognize as reasonable an expectation of privacy in electronic records and an expectation that deleting such records would result in continued privacy.

CONCLUSION: PROTECTING CYBERTRASH

The entire problem of the status of cybertrash may have arisen simply because some unnamed software engineer on Apple's Lisa development project decided to use a stylized trash can as the GUI symbol for "deleted files,"[148] but it is more likely that, regardless of the name chosen for the area in which deleted files are stored, the analogy to physical trash would have been advanced eventually. In both the physical and cyber cases, the intent is to part with ownership or control of something. There are, however, two critical distinctions that should make the application of the immanent trash decisions to cybertrash lead to a conclusion that Fourth Amendment protections apply: there is no ambiguity in the action of deleting a file, and there is no question about the reasonableness of the expectation of privacy in private files.[149]

Together, these distinctions should place deleted electronic information squarely in the protected category under *Greenwood* and therefore subject to the same Fourth Amendment protections as other

---

146 *See, e.g.*, *Identity Theft*, N.Y. TIMES, http://www.nytimes.com/info/identity-theft/ (last visited Aug. 5, 2011); Stephanie Armour, *Employment Records Prove Ripe Source for Identity Theft*, USA TODAY, Jan. 23, 2003, http://www.usatoday.com/money/workplace/2003-01-23-idtheft-cover_x.htm (last visited Aug. 5, 2011); *see also* IDENTITY THEFT NEWS ARTICLES, http://ssnfraudinfo.blogspot.com/ (last visited Aug. 5, 2011).

147 *See, e.g.*, 15 U.S.C. § 1681(a)(4) (2006).

148 As discussed above, even the term "delete" does not mean "dispose of"—it means mark the physical space on which the information is stored as available for reuse. The information is not disposed of until space is needed and the information is overwritten. This so-called slack space can be specifically selected and overwritten by specialized programs, known as file scrubbers, that offer various levels of destruction of the underlying data. These can be used on systems the owner of the information controls but not on systems under a third party's control.

149 A different result would of course be expected where the expectation of privacy was surrendered, as in the case of published files, such as those posted on Facebook or a similar website or those e-mailed to third parties. Nonconfidential disclosure to a third party surrenders the claim to an expectation of privacy. *See supra* notes 44–47 and accompanying text.

personal data. The result is constitutionally compelled and does not depend on any statute. Thus, there is no need for a new statute to extend privacy protection to cybertrash, and it is beyond Congress' power to diminish this protection.

There are, however, steps that are advisable to protect cybertrash. There is a theoretical risk of a bootstrap trap—merely announcing that there is no privacy in cybertrash would allow a government agency to argue that there could thereafter be no objectively reasonable expectation of privacy based on the rationale in *Greenwood*. Justice Brennan's conjecture that "members of our society will be shocked to learn that the Court, the ultimate guarantor of liberty, deems unreasonable our expectation that the aspects of our private lives that are concealed safely in a trash bag will not become public"[150] was the minority view. This argument would, however, completely destroy the Fourth Amendment. If accepted, it would allow the government to search any location simply by announcing ahead of time that it intended to do so.

The abandonment theory still seems viable, at least in the context of DNA.[151] Therefore, care must be taken to do nothing that might be construed as making the information public or abandoning deleted files.

Thus, files posted in public places—Facebook, LinkedIn, company websites, and the like—do not obtain protection by being deleted. A more subtle risk may be posed by form contracts with ISPs, websites, e-mail services, or employers that purport to transfer ownership of some or all of the rights in the files. Because information shared with a third party who is not under a duty of confidentiality surrenders the expectation of privacy necessary to assert Fourth Amendment protection,[152] these contracts may terminate Fourth Amendment rights in any files they cover, and again, the protection is not restored by virtue of deletion.

In the absence of these or similar affirmative acts of surrender, cybertrash should be protected by the Fourth Amendment.

---

150 California v. Greenwood, 486 U.S. 35, 46 (1988) (Brennan, J., dissenting).

151 *See* Joh, *supra* note 103.

152 *See* sources cited *supra* note 46 and accompanying text.