A SURVEY OF CYBERCRIME IN THE UNITED STATES

By Aaron Burstein

Several commentators have questioned whether cyberlaw is a meaningful category within law.[1] Few areas of law, these critics assert, rely upon the instrument for activity as the basis for defining a body of law.[2] A natural corollary to this criticism is that using a computer to commit a crime deserves no special attention. It was precisely this instrumental distinction, however, that has proven determinative in a subset of cybercrime cases involving "unauthorized access."[3] The cases have two archetypal features: (1) behavior that clearly deprived a person of something of value, and (2) indictment under a property crime or fraud statute.[4] All too often, however, conviction appeared to rest upon "the law of harm": harm to the victim implies that she was deprived of something of value—property—and therefore was the victim of theft.[5]

Legislators have felt compelled to create new statutes to address these problems, but the analytical difficulties that computers presented to law enforcement continue to grow. A complex body of statutes and caselaw

1. *See* Frank Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (arguing that teaching the "law of cyberspace" would be as frivolous as teaching the "Law of the Horse"). *But see* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 502-03 (1999) (arguing that cyberspace poses peculiar challenges about "the limits on law as a regulator and about the techniques for escaping those limits").

2. Easterbrook, *supra* note 1, at 207.

3. *See generally* Orin S. Kerr, *The Troubling Trigger of Cybercrime* (forthcoming 2003) (manuscript on file with author).

4. *Compare* United States v. Collins, 56 F.3d 1416, 1422 (D.C. Cir. 1995) (defendant used computer to store ballroom dancing-related documents and was convicted of conversion of government property), United States v. Girard, 601 F.2d 69, 70-71 (2d Cir. 1979) (defendant Drug Enforcement Agency (DEA) agent, who downloaded and planned to sell to drug dealers files identifying undercover DEA agents, was convicted of stealing government property), *and* United States v. Seidlitz, 589 F.2d 152, 153-56 (4th Cir. 1978) (upholding conviction of former government employee who used password, after employment terminated, to download a computer program, and was convicted of wire fraud), *with* United States v. Czubinski, 106 F.3d 1069, 1074 (1st Cir. 1997) (overturning conviction of defendant IRS employee, who browsed taxpayer records without authorization, and was convicted under wire fraud statute).

5. Kerr, *supra* note 3, at 22.

comprise an identifiable area of criminal law, cybercrime, which is "the use of a computer to facilitate or carry out a traditional (criminal) offense."[6]

Cybercrime laws have developed with frequent reference to property law. Statutes such as the Computer Fraud and Abuse Act (CFAA)[7] and the Digital Millennium Copyright Act (DMCA)[8] create rights akin to a property owner's right to exclude. The basis of the property metaphor in cybercrime development, however, leads to a rather surprising limitation in the legal protection of most electronic communications. E-mail and voice mail that reside on a remote server receive substantially less protection than they would receive if they were stored at home. Thus, while the property metaphor has expanded the protection of intellectual property, data that resides on a computer in one's possession, and computer users and resources against intruders, this has led, practically speaking, to less protection for an increasing range of communications. An important factor in determining the government's ability to search communications and data is the ownership of the computer hardware that stores or transmits the data. Most Internet users store significant amounts of data on remote computers, which effectively reduces barriers to government acquisition relative to the physical counterparts of identical data.

Part I of this Note tracks the property-based analysis that has become standard in the development of cybercrime prosecutions and statutes. In Part II, this Note reviews recent substantive developments in cybercrime, and Part III reviews developments in the procedures that the government must follow to search electronc data.

---

6. Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1014 (2001). A certain class of crimes is implicitly excluded from this definition. For example, "using a computer as a blunt instrument in an assault is, obviously, not a computer crime." Douglas H. Hancock, *To What Extent Should Computer Related Crimes be the Subject of Specific Legislative Attention?*, 12 ALB. L.J. SCI. & TECH. 97, 98 (2001). Even with this limitation, such a broad definition of cybercrime has not been uniformly adopted. A special section of the Department of Justice's Criminal Division—the Computer Crime and Property Section (CCIPS)—separates "computer crime" from "intellectual property crime," at least in its title. *See* CCIPS, *What Does CCIPS Do?*, *at* http://www.cybercrime.gov/ccips.html (last visited March 15, 2003).

7. 18 U.S.C. § 1030 (2000).

8. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.).

I. THE RISE OF THE PROPERTY METAPHOR IN CYBERCRIME

The confusion that marks early cybercrime prosecutions can, in large part, be explained by the statutes that prosecutors had at their disposal: wire fraud, mail fraud, theft, and trespass. Prosecutions under statutes defining theft and trespass—property crimes—seem to have developed from cases where defendants themselves accessed computer systems, and used the output toward some criminal end. For prosecutors to define the end as criminal, however, they had to identify a property interest as well as prove that the defendant's actions deprived the owner of its property.[9] Both computer use[10] and the data stored in computers[11] were identified as property interests, but this treatment resulted in an inconsistent view of when fraud was committed or the property owner was deprived of his property. In other cases, courts drew attention to statutory ambiguities and resolved these ambiguities in favor of defendants.[12] Computer-based activities simply began to fall outside the act or *mens rea* requirements (or both) of mail and wire fraud, theft, and trespass.[13] The result was "an unsatisfying, result-oriented jurisprudence."[14]

Congress and state legislatures took note of these failures, especially the failures of prosecutions under property-based statutes, and began to define new crimes that applied to this new breed of activity. These statutes broke away from requiring prosecutors to prove literal trespass to real property or theft of personal property, but they did not leave the underlying notions of physical property far behind.[15] For the most part these new statutes outlawed "unauthorized access"[16] to computer systems. Instead of maintaining a single system of "realspace" criminal statutes—

---

9. Kerr, *supra* note 3, at 20.

10. *Collins*, 56 F.3d at 1421.

11. United States v. Girard, 601 F.2d 69, 70-71 (2d Cir. 1979); United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978); *see also* Kerr, *supra* note 3, at 18.

12. This rule of narrow construction of criminal statutes, the rule of lenity, requires that "when choice has to be made between two readings of what conduct [a legislature] has made a crime, it is appropriate, before [choosing] the harsher alternative, to require that [the legislature] should have spoken in language that is clear and definite." Dowling v. United States, 473 U.S. 207, 214 (1985) (internal quotations and citations omitted).

13. Kerr, *supra* note 3, at 20.

14. *Id.* at 15.

15. *Id.* at 26, n.118 (noting that statutes in Georgia, Virginia, Arkansas, New York, and Washington are labeled "computer trespass" laws).

16. *Id.* at 24. Kerr uses "unauthorized access" as a label for all statutes that employ access to a computer system as a trigger for criminal liability. Other variants in statutory language include "access without authorization" and "exceeding authorized access."

trespass, theft, wire and mail fraud—and encouraging artful indictments,[17] Congress passed a specialized computer misuse statute, the Computer Fraud and Abuse Act (CFAA).[18]

The definition of copyright infringement has followed a similar course. The Supreme Court once expressed doubt that "wrongful appropriation of statutorily protected rights in copyright" could be considered "theft, conversion or fraud."[19] The inherent differences between physical property and intellectual property led to the latter being "carefully defined and carefully delimited" and protected by "correspondingly exact" measures.[20] As the court in *United States v. LaMacchia*[21] noted, this careful definition of rights, coupled with narrow construction of criminal statutes, seriously limited the ability of prosecutors to use either existing copyright laws or property-based statutes to obtain convictions where defendants had used new technology to commit acts with motives that simply were not within the contemplation of legislatures at the time they passed the relevant laws. The No Electronic Theft Act (NETA),[22] which was passed to "reverse the practical consequences of *United States v. LaMacchia*,"[23] only tweaked the *mens rea*[24] requirements for criminal copyright infringement, and thus could do little to halt unauthorized copying *ex ante*.[25]

---

17. *See id.* at 23 (citing a former state prosecutor's argument that charging computer crimes under theft statutes "require[s] that the victim produce evidence of an injury other than that which he is really concerned").

18. 18 U.S.C. § 1030 (2000).

19. Dowling v. United States, 473 U.S. 207, 216 (1985).

20. *Id.*

21. 871 F. Supp 535, 536-37, 543 (D. Mass. 1994) (granting defendant's motion to dismiss charge of wire fraud, 18 U.S.C. § 1843, for making unauthorized copies of computer software and distributing them free of charge, because "copyright is unique and distinguishable from the indisputably broad range of property interests protected by the mail and wire fraud statutes").

22. Pub. L. No. 105-147, 111 Stat. 2678 (Dec. 16, 1997) (codified as amended at 17 U.S.C. § 506(a) (2000) and 18 U.S.C. § 2319 (2000)).

23. H.R. REP. NO. 105-339, at 3 (1997).

24. NETA created two subparagraphs in the definition of criminal copyright infringement. 17 U.S.C. § 506(a)(1) preserved the old provision, which defined criminal infringement as "infring[ing] a copyright willfully for purposes of commercial advantages or private financial gain." 17 U.S.C. § 506(a)(2), the NETA provision, defines criminal copyright infringement in terms of a statutory threshold for the value of the works distributed: "Any person who infringes a copyright willfully by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000, shall be" liable for criminal infringement.

25. *See* Katyal, *supra* note 6, at 1006.

The DMCA changed this temporal lag in copyright enforcement by borrowing a page from the CFAA. In effect, the DMCA granted copyright owners a kind of property right: the right to control access to copyrighted works.[26] As the discussion of the first criminal prosection under the DMCA shows,[27] copyright owners can encrypt their works, thus placing them in "the electronic equivalent of . . . a locked room,"[28] and the government will prosecute entities that manufacture the tools required to break into these "locked rooms." Recognizing that many commercially deployed encryption schemes would not withstand the attacks that mass-market distribution of copyrighted works would draw, Congress conferred legal protection upon the encryption measures themselves.[29]

Thus, intellectual property crimes have begun to bridge the gap between the disparate laws that constitute cybercrime. The DMCA's creation of legal protection substantially expands to copyright owners the kind of property right that lurks behind the CFAA and related state laws. Congress' decision to award copyright holders a real property-inspired right in their works, however, falls short of providing a single, unifying theme for cybercrime, for two reasons. First, other "traditional" crimes that have arguably become easier to commit because of digital technology resist property-based remedies. The property-based notion of having a right to restrict access, or to exclude unwanted parties, does not have an obvious analogue in the area of child pornography, for example. The second and more important limitation on the appeal of property-based laws to govern online activities is that the adoption of the property metaphor does not usurp the property reality in the investigation of crimes. This limitation in the development of procedural law is explored in Part III of this Note.

---

26. *See* 17 U.S.C. § 1201(a)(1)(A) (2000) (stating that "[n]o person shall circumvent a technological measure that effectively controls access to" a copyrighted work); *Id.* § 1204(a)(1) (2000) (providing criminal punishment for "any person who violates section 1201 . . . willfully and for purposes of commercial advantage or private financial gain").

27. United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002). *See infra* Part II.D.

28. David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 686 (2000) (citing H.R. REP. NO. 105-551, pt. 1, at 17 (1998)).

29. *See* Peter S. Menell, *Envisioning Copyright Law's Digital Future*, 46 N.Y.L. SCH. L. REV. 63 (2003).

II. THE SUBSTANTIVE LAW OF CYBERCRIME: THE TENACITY OF THE REAL PROPERTY METAPHOR

Not all cybercrime presents such stark questions about the coverage of criminal statutes. Computers often reduce the deterrent effect of nonlegal regulators of crime—the threat of physical harm, "perptration costs," and social norms[30]—but do not change the underlying harm. The computer-based element of these "traditional" crimes has not required new laws. Recent developments in these traditional crimes are discussed in Part II.A. Many other kinds of cybercrime, however, have been defined by new statutes, and these statutes often betray an underlying real property-based mindset. The extent to which the quintessential cybercrime statute, the Computer Fraud and Abuse Act (CFAA), displays this conception is reviewed in Part II.B. Intellectual property laws have also begun to adopt a version of the property owner's right to exclude. Congress pushed trade secret law in this direction with the Economic Espionage Act (EEA); recent developments under this law are reviewed in Part II.C of this Note. Finally, Congress' most blatant move to import real property concepts to intellectual property crimes is the Digital Millennium Copyright Act (DMCA), which is discussed in Part II.D of this Note.

A. "Traditional" Crimes

Child pornography provides a prime example of how existing law has proven capable of handling some forms of cybercrime,[31] though the ease of distributing child pornography across national borders has prompted the development of new law enforcement strategies.[32] Indeed, attempts to expand the reach of the existing law have run afoul of constitutional concerns.[33] The medium of distribution of child pornography does not changed the underlying harm, potential psychological and physical danger to the children who are the subjects of the pornography. Current United States law maintains its focus on punishing people who traffic in child pornography, regardless of how the images are distributed.

Other "traditional" crimes that have received attention as cybercrimes also appear to have done so because computers reduce some of the

30. Katyal, *supra* note 6, at 1006-10.

31. 18 U.S.C. § 2252 (2000).

32. Katyal, *supra* note 6, at 1028-31.

33. Ashcroft v. Free Speech Coalition, 535 U.S. 234, 256-58 (2002) (invalidating as overbroad those provisions of the Child Pornography Prevention Act of 1996 that banned any image which "appears to be of a minor engaging in sexually explicit conduct" or which "conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct").

deterrents to committing them by the usual means. "Cyberstalking,"[34] for example, drew the attention of former Vice President Gore,[35] and led to several convictions under both the interstate communications statute[36] and the more recent interstate stalking statute.[37] Defendants in these cases took advantage of the Internet's ability to "lower the barriers to harassment," lack of physical confrontation, and ability to use remarks from third parties to conduct their harassment,[38] but the laws under which they were prosecuted make no special reference to online activities. Similarly, the Department of Justice has been actively prosecuting Internet-related identity theft, gambling, fraud, and prescription drug sales.[39]

A more striking example of the scale of some "traditional"[40] crime operations on the Internet is evident from the arrests resulting from "Operation Buccaneer."[41] On December 11, 2001, CCIPS and Customs Service agents simultaneously executed more than 100 search warrants[42] against individuals who were suspected of being involved in "warez"[43]

---

34. "Cyberstalking occurs when someone is threatened or harassed online." Katyal, *supra* note 6, at 1034.

35. *See* CCIPS, *Prosecuting Crimes Facilitated by Computers and the Internet*, § F, *at* http://www.cybercrime.gov/crimes.html#IXf (last visited Feb. 21, 2003); *see also* Janet Reno, *Cyberstalking: A New Challenge for Law Enforcement and Industry: A Report from the Attorney General to the Vice President*, http://www.cybercrime.gov/cyberstalking.htm (1999) [hereinafter *Cyberstalking Report*].

36. 18 U.S.C. § 875 (2000).

37. *Id.* § 2261A.

38. *See Cyberstalking Report*, *supra* note 35.

39. *See generally* CCIPS, *Prosecuting Crimes Facilitated by Computers and by the Internet*, *at* http://www.cybercrime.gov/crimes.html (summarizing applicable laws and noteworthy prosecutions) (last visited Feb. 21, 2003).

40. Citing an example of a sweep of alleged participants in an Internet-based copyright infringement operation may appear to be at odds with the use of copyright law to illustrate some of the difficulties in defining cybercrime. Operation Buccaneer is relevant, however, because the convictions do not involve NETA or more recent copyright developments, but rather alleged violations of the well-established rights of copyright holders to reproduce, 17 U.S.C. § 106(1) (2000), and distribute, 17 U.S.C. § 106(3) (2000), copies of their works.

41. For an overview see CCIPS, *Operation Buccaneer*, *at* http://www.cybercrime.gov/ob/OBMain.htm (Oct. 7, 2002).

42. Press Release, CCIPS, Federal Law Enforcement Targets International Internet (Dec. 11, 2001), *at* http://www.cybercrime.gov/warezoperations.htm (last visited Mar. 14, 2003).

43. "Warez" refers to "illegally copied and distributed commercial software." Arista Records, Inc. v. MP3Board, Inc., 2002 U.S. Dist. LEXIS 16165, *34 (S.D.N.Y. 2002).

operations. The sweep resulted in seventeen convictions, most of them arising from guilty pleas to conspiracy counts.[44]

Operation Buccaneer reveals that the size and sophistication of warez operations have increased since *LaMacchia*,[45] but the threat of criminal prosecution has not eradicated these operations. One convict, Chris Tresco, stated that his "motivation was purely and simply putting technology to work."[46] If Tresco's motivation is widely held by warez conspirators,[47] then a severe disconnect is likely to remain between the increasingly severe criminal penalties for copyright infringement, and the perception of the threat of these sanctions.

B. The Computer Fraud and Abuse Act

Existing laws did not extend so readily to threats to computer systems as they did to threats against people or the value of copyrights. Early efforts to apply theft and trespass laws frequently failed,[48] yet the temptation in many legislatures to apply a property law structure to computer system access proved strong. From this failure of imagination at the federal level, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA)[49] was born. The CFAA defines a variety of civil and criminal violations arising from "access[ing] a computer without authorization or exceeding authorized access."[50] Despite strong criticism that the CFAA's failure to define "access"[51] renders it incoherent and

---

44. CCIPS, *Operation Buccaneer Defendant Chart*, *at* http://www.cybercrime.gov/ob/Dchart.htm (Jan. 27, 2003).

45. United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994).

46. Slashdot Interview, *Former DrinkOrDie Member Chris Tresco Answers*, *at* http://interviews.slashdot.org/interviews/02/10/04/144217.shtml?tid=123 (Oct. 4, 2002).

47. By no means are all technologists impressed by these displays. A remark by Ken Thompson, a pioneer of the Unix operating system, is apposite: the "misguided use of a computer is no more amazing than drunk driving of an automobile." Ken Thompson, *Reflections on Trusting Trust*, 27 COMM. ACM 761 (1984), *available at* http://www.acm.org/classics/sep95/.

48. *See generally infra* Part II. More recently, however, civil plaintiffs have had some success with property-based theories, especially trespass to chattel. *See* Intel Corp. v. Hamidi, 94 Cal. App. 4th 325 (2001), *review granted*, 43 P.3d 587 (Cal. Mar. 27, 2002); eBay v. Bidder's Edge, 100 F. Supp. 2d 1058 (C.D. Cal. 2000); CompuServ, Inc. v. Cyberpromotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

49. Pub. L. 98-473, 98 Stat. 1837, 2190 (Oct. 12, 1984) (codified as amended at 18 U.S.C. § 1030 (2000)).

50. 18 U.S.C. §§ 1030(a)(1)-(5) (2000).

51. The CFAA does define "exceeds authorized access," but not in a way that helps determine when access occurs, or by what means authorization is to be ascertained. 18 U.S.C. § 1030(e)(6) ("'exceeds authorized access' means to access a computer with au-

broader than intended,[52] the CFAA remains the statute of choice in a broad range of criminal computer misuse cases. As discussed below, it is possible that the CFAA's range will become even broader.

One of the most typical roles of the CFAA is in the prosecution of virus,[53] worm,[54] and Trojan horse[55] writers. In a particularly disruptive and expensive episode, David L. Smith, who created and released the "Melissa" virus in 1999, was sentenced to twenty months in federal prison.[56] Smith had earlier pled guilty to violations of 18 U.S.C. § 1030(a)(5)(A)[57] and 18 U.S.C. § 1030(a)(2).[58] Smith's conviction points to the breadth of the meaning of "unauthorized access" that the landmark

---

thorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter").

52. Kerr, *supra* note 3, at 26.

53. A virus is a "program that searches out other programs and 'infects' them by embedding a copy of itself in them." The corrupt program often performs malicious acts, such as deleting files, on the host computer before it is discovered. Even worse, when programs that contain a virus execute, they often spread copies of the virus to other computers. Eric S. Raymond, *The New Hacker's Dictionary*, Version 4.0.0, *at* http://www.jargon.8hz.com/jargon_37.html#TAG1916 (July 25, 1996).

54. A worm is a program that a "program that propagates itself over a network." Raymond, *supra* note 53, *at* http://www.jargon.8hz.com/jargon_38.html#TAG2005. The difference between a worm and a virus is that a worm is a complete, standalone program, whereas a virus is a piece of code that must be executed by a host program. A worm, however, may need to exploit a security weakness in another program in order to gain access to a remote computer.

55. A Trojan horse is a "malicious, security-breaking program that is disguised as something benign." Raymond, *supra* note 53, *at* http://www.jargon.8hz.com/jargon_35.html#TAG1840. A program that has been infected by a virus is an example of a Trojan horse, whereas the corrupt, infectious code itself is the virus.

56. Press Release, CCIPS, Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison (May 1, 2001), *at* http://www.cybercrime.gov/melissaSent.htm (describing further the details of how the virus spread to "untold numbers of computers and computer networks" and caused an estimated $80 million in damage).

57. Section 1030(a)(5)(A) creates liability for "[w]hoever . . . knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."

58. Section 1030(a)(2) creates liability for

> [w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U. S. C. § 1681 et seq.); (B) information from any department or agency of the United States; or (C) information from any protected computer if the conduct involved an interstate or foreign communication.

case of *United States v. Morris*[59] established: exploiting a weakness on one system can give rise to a massive number of unauthorized accesses to other systems,[60] a phenomenon rather remote from the real property underpinnings of many unauthorized access statutes.

The vision of property rights that underlies the CFAA not only remains intact but could become even stronger. The day may soon be at hand when it will be possible to violate both the CFAA and the Digital Millennium Copyright Act (DMCA)[61] during a single access of a copyrighted work. Some proposed systems for providing digital works would not distribute copies of the works at all, but would instead offer access to the works in remote "rights lockers."[62] The technological measures restricting access fall within either 17 U.S.C. § 1201(a) or (b), or both. The more interesting case would be if a technological measure fell under section 1201(b), because that section does not ban the circumvention of usage controls. It appears likely, however, that this act of circumvention would fall under a CFAA provision; § 1030(a)(2)(C)[63] appears to be the most applicable. It is possible that some property interest of the consumer, and would-be intruder, would preclude application of the CFAA, if a court adopted a "logical"[64] view of the purchased work. As the discussion in Part III indicates, however, the applicable statutes preclude this "logical" view, forcing courts to rely heavily upon the physical configuration of computer equipment when confronting cybercrime. In the preceding hypothetical, the physical view of the distribution of information subjects a person to criminal liability under multiple statutes. That situation remains hypothetical, but it only slightly extends the current reality of how the wide physical distribution of computer components alters the rights of individuals and the government to access electronic

59. 928 F.2d 504, 510-11 (2d Cir. 1991) (holding that individuals with some authorized access to protected computers could still be liable for acts of "unauthorized access").

60. Kerr, *supra* note 3, at 43.

61. Pub. L. No. 105-304, 112 Stat. 2860, 1 (1998); *see also* discussion *infra* Part II.D.

62. Nic Garnett & Tomas Sander, *What DRM Can and Cannot Do . . . and What It Is or Isn't Doing Today*, *at* http://www.cfp2002.org/fairuse/garnett.pdf (last visited Mar. 14, 2003).

63. 18 U.S.C. § 1030(a)(2)(C) makes it a crime to "intentionally acces[s] a computer without authorization . . . and thereby obtai[n] . . . information from any protected computer if the conduct involved an interstate or foreign communication."

64. I borrow this term from the more technological context of computer systems, where a "logical" disk volume is one that appears to the user to be one hard disk, but is in fact made of several distinct disks.

data. As the *ElcomSoft*[65] case shows, the idea of "unauthorized access" is becoming part of criminal copyright law.

C. The Economic Espionage Act

Congress has realized that keepers of trade secrets, like proprietors of computer systems, often have an interest in exercising the power to exclude. It has responded by offering protection that is partly colored by a property right.[66] The Economic Espionage Act (EEA),[67] the first federal statute to protect trade secrets, defined two crimes: economic espionage and theft of trade secrets. These crimes differ primarily in the beneficiary of the misappropriation. Economic espionage,[68] used in an indictment for the first time this year,[69] outlaws appropriation of a trade secret with the intent or knowledge that the appropriation will benefit a foreign power. The trade secret theft statute[70] bans identical conduct but does not require a foreign beneficiary of the misappropriation.

The most striking provisions in the EEA are the identically worded §§ 1831(a)(2) and 1832(a)(2), which create criminal liability for a person who "*without authorization* copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret."[71] In contrast to state civil trade secret misappropriation statutes, which generally require that the secret be obtained by "improper means,"[72] the EEA takes a more property-based approach by making the authorization by the trade secret owner, or lack thereof, the basis for

65. *See* discussion *infra* Part II.D.

66. Geraldine Szott Moohr, *The Problematic Role of Criminal Law in Regulating Use of Information: The Case of the Economic Espionage Act*, 80 N.C. L. REV. 853, 853, 862 (2002); James H. A. Pooley, Mark A. Lemley & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 194 (1997).

67. Pub. L. No. 104-294, 110 Stat. 3488 (Oct. 11, 1996) (codified at 18 U. S. C. §§ 1831-1839 (2000)).

68. 18 U.S.C. § 1831 (2000).

69. A research scientist was alleged to have stolen genetic research materials from the Cleveland Clinic Foundation and to have transported them to RIKEN, a research institute operated by the Japanese government. Press Release, CCIPS, Scientist Pleads Guilty to Providing False Statements Regarding Trade Secret Theft from Cleveland Clinic Foundation (May 1, 2002), *at* http://www.cybercrime.gov/serizawaPlea.htm.

70. 18 U.S.C. § 1832 (2000).

71. *Id.* § 1831(a)(2); *Id.* § 1832(a)(2). (emphasis added).

72. Pooley, Lemley & Torren, *supra* note 66, at 192.

liability.[73] Moreover, in contrast to most states' provision of civil remedies, the EEA provides only criminal remedies.[74]

The EEA's criminal provisions and property-based themes represent a legislative endorsement of an approach that prosecutors and private plaintiffs had tried to advance, but which faltered when the misappropriation of "[p]urely intellectual property"[75] was at issue. In *United States v. Brown*, for example, defendant John Brown escaped prosecution under the National Stolen Property Act (NSPA)[76] because Brown's former employer had shipped the alleged trade secrets, a computer program and software manuals from a former employer, to Brown on backup tapes that Brown himself owned.[77] The Tenth Circuit affirmed dismissal of the case, holding that the NSPA "applies only to physical 'goods, wares or merchandise' that were themselves 'stolen, converted or taken by fraud.'"[78] Without protection for the information itself, prosecutors face a gap in the criminal law.[79] The federal wire[80] and mail[81] fraud statutes, moreover, cannot "completely close the enforcement

---

73. The legislative history also contains evidence of Congress' intent to create a property-like right, insofar as possessing information without the owner's authorization can trigger liability. H.R. REP. NO. 104-788, at 8 (1996) ("The concept of control also includes the mere possession of the information, regardless of the manner by which the non-owner gained possession of the information.").

74. The penalties can be quite severe. Economic espionage is punishable by a maximum fine of $500,000, or 15 years in prison, or both. 18 U.S.C. § 1831(a)(5). Trade secret theft is punishable by a maximum fine of $5,000,000, or 10 years in prison, or both. *Id.* § 1832(a), (b).

75. United States v. Brown, 925 F.2d 1301, 1307 (10th Cir. 1991).

76. Ch. 645, § 1, 62 Stat. 806 (1948) (codified at 18 U.S.C. § 2314).

77. *Brown*, 925 F.2d at 1303.

78. It is worth noting that the construction of the NSPA adopted by the Tenth Circuit in *Brown* is not universal. *See, e.g.*, United States v. Riggs, 739 F. Supp. 414, 420 (N. D. Ill. 1991) (holding that a telephone company's computer file satisfied section 2314's requirement of "goods, wares, or merchandise," and so was protected by § 2314 from being "stolen, converted or taken by fraud"); *see also* Todd H. Flaming, *The National Stolen Property Act and Computer Files: A New Form of Property, a New Form of Theft*, 1993 U. CHI. L. SCH. ROUNDTABLE 255, 259-67 (arguing that *Dowling* applies only to copyright infringement cases, and that "any language in the opinion to the effect that the statute only covers tangible 'goods, wares or merchandise' is dictum"). At least one recent case has followed *Riggs*. *See* United States v. Farraj, 142 F. Supp. 2d 484, 490 (S.D.N.Y. 2001) (holding that "the transfer of electronic documents via the internet across state lines does fall within the purview of § 2314").

79. Pooley, Lemley & Torren, *supra* note 66, at 178.

80. 18 U.S.C § 1343 (2000).

81. *Id.* § 1341.

gap,"[82] because these statutes apply only when the victims of trade secret misappropriation are permanently defrauded of their information.[83] Although the Supreme Court suggested that a trade secret could form the basis of a legally cognizable property interest,[84] that suggestion fell far short of creating a broad right that would allow federal prosecutors to intercede in cases of nascent appropriation.[85]

The EEA may have overfilled this gap by defining crimes that could overlap with both the NSPA and with various intellectual property crimes. In June 2002, for example, two individuals pled guilty to theft of trade secret[86] counts for stealing and transporting across state lines chemical reagents that were used in immunosuppression research.[87] This activity might have been cognizable under the NSPA. Similarly, the Justice Department recently obtained a guilty plea from Robert Keppel, whom it accused of § 1832(a)(2) trade secret theft for purchasing, and subsequently selling via a Web site, copies of Microsoft certification exams.[88] The Keppel case could mark a shift in prosecutions for cases that implicate copyright's reproduction[89] and distribution[90] rights.[91] Trade secret charges,

---

82. Pooley, Lemley & Torren, *supra* note 66, at 186 (citing additional cases in which wire and mail fraud counts were dismissed).

83. *Id.*

84. Ruckelshaus v. Monsanto, 467 U.S. 986, 1003–04 (1984) ("[T]o the extent that Monsanto has an interest in its . . . data cognizable as a trade-secret property right under Missouri law, that property right is protected by the Takings Clause of the Fifth Amendment.").

85. Press Release, CCIPS, Former Engineer of White Plains Software Company Receives Two Years in Prison for Theft of Trade Secret (Oct. 15, 2002), *at* http://www.cybercrime.gov/kissaneSent.htm (describing plea by individual offered to sell parts of employer's closely guarded source code to competitors, in violation of his employment agreement, which stated that he agreed to "forever keep secret" confidential SMARTS information that he had access to, including "software codes.") [hereinafter CCIPS *Keppel Press Release*].

86. 18 U.S.C § 1832 (2000).

87. Press Release, CCIPS, Pair Charged With Theft Of Trade Secrets From Harvard Medical School (June 19, 2002), *at* http://www.cybercrime.gov/zhuCharges.htm.

88. Press Release, CCIPS, Former Vancouver, Washington, Resident Pleads Guilty to Theft of Trade Secrets from Microsoft Corporation (Aug. 23, 2002), *at* http://www.usdoj.gov/criminal/cybercrime/keppelPlea.htm.

89. 17 U.S.C § 106(1) (2000).

90. *Id.* § 106(3) (2000).

91. Press Release, CCIPS, Former Vancouver, Washington, Resident Pleads Guilty to Theft of Trade Secrets from Microsoft Corporation (Aug. 23, 2002), *at* http://www.usdoj.gov/criminal/cybercrime/keppelPlea.htm (stating that "the sale and distribution of [the exams] violated Microsoft copyright and constituted a conversion of Microsoft proprietary information for personal gain"). *See also* Becky Nagel, *Cheet-Sheets.com Owner Pleads Guilty; May Face Jail Time*, CERTCITIES NEWS, *at*

when applicable, could prove more attractive than copyright, because the act and *mens rea* requirements for trade secret misappropriation are easier to meet. There is no need to engage in the sometimes messy task of proving copyright infringement, nor does § 1832 require prosecutors to prove that the accused acted for "commercial advantage or private financial gain."[92]

As the Keppel case shows, works may be protected under both the EEA and copyright law, but the EEA may obviate the need to stay within the "precisely defined limits"[93] of the Copyright Act's criminal provisions. These provisions—at the time that the Court wrote, at least—reflected the difference between ownership of a copyright and "the possessory interest of the owner of simple 'goods, wares, [or] merchandise,'" to prosecute copyright crimes.[94] As applied to Keppel, however, the EEA's provisions embrace both the rhetoric[95] and the legal effect[96] of real property. Previously unable to persuade courts to expand intellectual property protection on theories of "unjust enrichment" or "restitution,"[97] and certainly unable to convince courts to expand criminal penalties beyond existing statutes,[98] federal prosecutors now have at their disposal a trade secret law whose operative language is more expansive than state trade secret laws. Although this approach potentially creates grounds for challenging a statute as being unconstitutionally vague, no such challenge against the EEA has prevailed.[99]

---

http://certcities.com/editorial/news/story.asp?EditorialsID=336 (Aug. 27, 2002) (quoting the assistant United States Attorney who prosecuted the Keppel case for the proposition that § 1832 is becoming a more attractive prosecution tool in "braindump" cases).

92. 17 U.S.C. § 506(a) (2000).

93. Dowling v. United States, 473 U.S. 207, 217 (1985).

94. *Id.*

95. Section 1832 is entitled "*Theft* of trade secrets" and defines the requisite *mens rea* for a violation as "intent to convert a trade secret."

96. The value that the EEA afforded Microsoft's copyrighted certification exams was in Microsoft's right to set the terms that governed access to the exams. More specifically, "'banner' pages" shown at the beginning of MSCE and MSCD exams "require the test-taker to agree to certain terms regarding the test material including an agreement not to copy or release the test material." CCIPS *Keppel Press Release*, *supra* note 85.

97. Wendy J. Gordon, *On Owning Information: Intellectual Property and the Restitutionary Impulse*, 78 VA. L. REV. 149, 154 n.20 (1992) (discussing Feist Publ'ns v. Rural Tel. Serv. Co., 499 U. S. 340 (1991)).

98. *Dowling*, 473 U.S. at 213 (reiterating that "federal crimes, of course, are solely creatures of statute" (internal quotations and citations omitted)).

99. *See, e.g.*, United States v. Krumrei, 258 F.3d 535, 536 (6th Cir. 2001) (holding that the EEA's definition of "trade secret" in 18 U.S.C. § 1839(3) was not unconstitutionally vague as applied to defendant).

D. The DMCA

The justifications for assigning liability on the basis of unauthorized access to computer systems, or the use of trade secrets "without authorization," are less apparent in the context of copyrighted works, where wide dissemination of works is an important goal of copyright law.[100] Congress did create such a right with the DMCA. Once again, the complexities of digital computers—this time, their capacity to make and distribute perfect copies of works at almost zero cost—led Congress[101] to augment criminal copyright liability with a form of *ex ante* liability based upon circumventing the "digital walls"[102] that may protect a work. This shift in copyright law from *ex post* enforcement to *ex ante* control raised general concerns; the arrest of Russian programmer Dmitry Sklyarov[103] for alleged DMCA violations caused outrage.[104] This first test of the DMCA's criminal provisions resulted in an acquittal,[105] but *United States v. ElcomSoft* has still affirmed that the DMCA supplies copyright holders with a powerful right to exclude unwanted users from accessing their works.[106]

1. DMCA Provisions at Issue in ElcomSoft

The government based its charges against Sklyarov[107] and his employer, Elcom, Ltd. ("ElcomSoft"), on their allegedly production[108] and

---

100. *See, e.g.*, Julie E. Cohen, *Copyright and the Perfect Curve*, 52 VAND. L. REV. 1799, 1814 (2000).

101. H.R. REP. 105-551, pt. 2, at 25 (1998) ("In contrast to the analog experience, digital technology enables pirates to reproduce and distribute perfect copies of works—at virtually no cost at all to the pirate. As technology advances, so must our laws.").

102. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 435 (2d Cir. 2001).

103. Dave Wilson, *Programmer Arrested in E-Book Case; Employee of Russian Company Allegedly Distributed Software That Cracks Encryption Used for Some Electronic Books*, L.A. TIMES, July 18, 2001, part 3, at 1.

104. Lawrence Lessig, *Jail Time in the Digital Age*, N.Y. TIMES, July 30, 2001, at A17.

105. Matt Richtel, *Russian Company Cleared of Illegal Software Sales*, N.Y. TIMES, Dec. 18, 2002, at C4.

106. Since the DMCA has been analyzed in detail elsewhere, only the provisions relevant to the *ElcomSoft* case are discussed here. For more general analyses, see generally Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d. Cir. 2001); Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000); Nimmer, *supra* note 28.

107. The government deferred prosecution against Sklyarov in exchange for his agreement to testify in the trial of ElcomSoft. Pretrial Diversion Agreement, CR 01-20138 RMW, *available at* http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20011213_sklyarov_agreement.pdf (Dec. 13, 2001).

marketing[109] of the Advanced eBook Processor (AEBPR). The government alleged that the primary purpose of the AEBPR was to "remove any and all limitations on an ebook purchaser's ability to copy, distribute, print, have the text read audibly by the computer, or any other limitation imposed by the publisher."[110] On the basis of these capabilities, the government categorized the AEBPR as a technology that circumvents "rights controls,"[111] rather than a technology that circumvents an "access control"[112] measure, such as a password.[113] Some of the features that ElcomSoft advertised in connection with the AEBPR included "Advanced PDF Password Recovery," however, so the AEBPR arguably had the potential to be an access control circumvention technology.[114] Moreover, eBooks, like DVDs, are encrypted, and thus use a technological measure that falls within the meaning of section 1201(a).[115] Finally, since ElcomSoft sold the AEBPR, the alleged violation of sections

---

108. 17 U.S.C. § 1201(b)(1)(A); Indictment, United States v. Elcom Ltd., CR 01-20138 (N.D. Cal. 2001) at 5 [hereinafter *ElcomSoft Indictment*]. 17 U.S.C. § 1201(b)(1)(A) provides:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that . . . is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

109. 17 U.S.C. § 1201(b)(1)(C); *ElcomSoft Indictment*, *supra* note 108, at 6. 17 U.S.C. § 1201(b)(1)(A) provides:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that . . . is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

110. *ElcomSoft Indictment*, *supra* note 108, at 2.

111. Jane C. Ginsburg, *Copyright and Control Over New Technologies of Dissemination*, 101 COLUM. L. REV. 1613, 1631-32 (2001) (coining this term for technologies that fall under 17 U.S.C. § 1201(b)).

112. 17 U.S.C. § 1201(a).

113. *ElcomSoft Indictment*, *supra* note 108, at 9-10.

114. O'Connell Aff., United States v. Elcom Ltd., CR 01-20138 (N.D. Cal. 2001), ¶ 11, *at* http://www.planetpdf.com/mainpage.asp?webpageid=2394 (last visited Mar. 15, 2003).

115. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd sub nom*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

1201(b)(1)(A) and 1201(b)(1)(C) formed the basis for the criminal charges against it.[116]

2. *The Legal Protection of Technological Measures in ElcomSoft*

ElcomSoft demonstrates that United States copyright law now provides criminal punishment not only for "bad acts" but also "bad machines."[117] In its defense, ElcomSoft argued that the the statutory definition of which machines are "bad" is unconstitutionally vague.[118] Citing the textual differences between the access control circumvention ban in section 1201(a) and the rights control circumvention ban in section 1201(b), ElcomSoft urged the court to consider that section 1201(b) defines "no underlying substantive provision,"[119] which "renders it impossible to determine which tools [section 1201(b)] in fact bans."[120] The court rejected this constitutional challenge.[121] Addressing ElcomSoft's argument that section 1201(b) provided no useful standard to determine which devices circumvent usage control measures, the court held that "all tools that enable circumvention of use restrictions are banned, not merely those use restrictions that prohibit infringement."[122]

This holding marks a pronounced shift in copyright law from *ex post* enforcement to *ex ante* control. Not only does the DMCA protect Adobe eBooks from devices "primarily designed"[123] or "marketed"[124] to circumvent an eBook's usage control measures, but it does so before any devices has been alleged, let alone proven, to have violated "a right of a copyright owner."[125] Although the DMCA provides some exemptions

116. *See* 17 U.S.C. § 1204 (crating criminal liability for "[a]ny person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain").

117. Nimmer, *supra* note 28, at 684.

118. *See* Motion to Dismiss Indictment for Violation of Due Process at 12 (Jan. 29, 2002), http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20020129_elcom_mtd_notice.pdf [hereinafter *ElcomSoft Motion to Dismiss*], United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1122-25 (N.D. Cal. 2002) [hereinafter *ElcomSoft*] (arguing that § 1201(b) "is not directed at unauthorized access, but at more traditional unlawful behavior," that is, "unauthorized use of copyrighted material once authorized access is obtained").

119. *ElcomSoft Motion to Dismiss*, *supra* note 118, at 13.

120. *Id.* at 17.

121. The court also rejected facial and as applied challenges to section 1201(b) based on the First Amendment, an argument that is not discussed in this Note. For the court's disposition of the Constitutional arguments, see *ElcomSoft*, 203 F. Supp. 2d at 1132-1142.

122. *ElcomSoft*, 203 F. Supp. 2d at 1124.

123. 17 U.S.C. § 1201(b)(1)(A) (2000).

124. *Id.* § 1201(b)(1)(C).

125. *Id.* § 1201(b)(1).

from the act-of-circumvention ban,[126] and creates a safety valve from the circumvention ban, commentators have questioned whether these exemptions will do much to qualify the absolute property right that would formally exist without them.[127] The criminal charges against ElcomSoft, as well as the civil lawsuit against distributors of an unauthorized DVD decryption device, have continued to make the DMCA unpopular among computer professionals[128] and have even prompted some legislators to call for reform.[129]

In addition to illustrating how broad the DMCA's circumvention device bans are, *ElcomSoft* also possesses considerable symbolic value. It represents the first test of the government's willingness to punish makers of devices that threaten the "digital walls" around digital works, and thus to enforce the legal prong that copyright holder have asserted is necessary to support technological measures used to guard commercial works.[130] A copyright holder can distribute a work to the public with access controls and usage rules—that is, with the exclusive attributes of physical property—and the government will sanction activities that might undermine the enforcement of this exclusivity.

---

126. Section 1201(a)(1)(B) exempts from section 1201(a) liability persons who "are likely to be . . . adversely affected . . . in their ability to make noninfringing uses" of works in a certain class of works identified by the Librarian of Congress. Section 1201(a)(1)(C) prescribes a procedure for determining these classes of users.

128. *See* Nimmer, *supra* note 28, at 715-41 (comparing an original version of § 1201, which showed no "special solicitude for user rights," to the version ultimately adopted into law and presenting case studies that demonstrate that the "unjustifiably broad" anti-trafficking provisions in section 1201(b) could render its exceptions largely meaningless); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 537-49 (1999) (criticizing § 1201(a)'s act-of-circumvention provisions as "unduly narrow" and the anti-device provisions as overbroad).

128. Letter from Barbara Simons and Eugene Spafford, Co-Chairs, United States Association for Computing Machinery Public Policy Committee, to Representative Rick Boucher (Oct. 31, 2002), *available at* http://www.acm.org/usacm/Letters/BoucherDMCABill.htm (citing computer security researchers' concerns that their activities run afoul of the DMCA and are not within the anticircumvention exemptions).

129. Rep. Rick Boucher (D-VA) and Rep. John Doolittle (R-CA) introduced the Digital Media Consumers' Rights Act, H.R. 5544, 107th Cong. (2002), which proposed, *inter alia*, strengthening scientific research and fair use exemptions in the DMCA.

130. *See* Dean S. Marks and Bruce H. Turnbull, *Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses*, 46 J. COPYRIGHT SOC'Y U.S. 563, 563-64 (1999) (explaining that both technological and legal protections are necessary to prevent the unauthorized duplication and distribution of digital works).

III. PROCEDURE AND CYBERCRIME

The physical property characteristics of technologically protected, widely disseminated, copyrighted works provide a stark contrast to the legal status of electronic communications in general, regardless of how strongly protected or widely disseminated they are. As discussed throughout Part III of this Note, Congress has created property-based protection for computer systems, declared that a trade secret is capable of being stolen, and created a right—whose violation may precipitate criminal penalties—for copyright holders to restrict access to and usage of their works. Congress has generally applied a property analysis in a manner that strengthens the protection of the threatened interest.

When electronic communcations play a role in a criminal investigation, however, a property-based analysis leads in exactly the opposite direction. Extending the Fourth Amendment's guarantees of security in one's "persons, houses, papers, and effects"[131] to communications that do not fit easily into any of these categories requires judicial determination. Other information to which a person might wish to restrict the government's access receives only the protection that a relevant statute, if any, offers. As electronic communications become more important in daily life,[132] on the one hand, and a more important means for criminal investigation[133] and intelligence surveillance[134] on the other, these limitations are likely to become more widely noticed. An odd dynamic has developed; the Supreme Court's extension of Fourth

---

131. U. S. CONST. amend. IV. The amendment states, in its entirety:
> 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.

132. Eric M. Uslaner, *Trust, Civic Engagement and the Internet*, *at* http://www.pewtrust.org/pdf/vf_pew_internet_trust_paper.pdf (May 2001).

133. *See* Hill Decl., In the Matter of the Application of the United States of America for an Order Authorizing the Installation of a Pen Register and Trap and Trace Device Criminal No. 99-2713M (C.D. Cal. Feb. 4, 2000) at ¶¶ 2-5 (explaining the purpose and operating principles of "Carnivore," the alleged equivalent of a pen register or trap-and-trace device for e-mail), *at* http://www.epic.org/privacy/carnivore/fbi_dec.html (last visited March 15, 2003).

134. A new project funded by the Department of Defense, the Information Awareness Office, proposes to collect massive amounts of data in order to achieve "Total Information Awareness," and hence "to revolutionize the ability of the United States to detect, classify and identify foreign terrorists—and decipher their plans." Program Objective, Information Awareness Office, *at* http://www.darpa.mil/iao/TIASystems.htm (last visited Feb. 3, 2003).

Amendment beyond a property-based concept, to activities surrounded by a "reasonable expectation of privacy," did not dispose of the role of property in determining the level of protection that a given communication receives. Ownership of property is as important as ever; the ownership and physical state of computer equipment determines the showing that the government needs to conduct a search.

A. The Fourth Amendment

A pair of 1967 Supreme Court decisions initiated the application of Fourth Amendment[135] protection beyond the property-based standard[136] in the text of the amendment. In *Berger v. New York*,[137] the Court invalidated New York's eavesdropping statute[138] on the grounds that its "broad . . . sweep result[ed] in a trespassory intrusion into a constitutionally protected area."[139] In *Katz v. United States*,[140] the Court broadened Fourth Amendment protection from this explicitly property-based conception to one that incorporated a conception of a right to privacy. In his concurrence in *Katz*, Justice Harlan stated what has become the guiding principle for the constitutionality of a search: a search is unconstitutional if it violates an individual's (1) "actual (subjective) expectation of privacy"[141] and (2) "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[142] *Katz*, however, narrowed *Berger* by holding that electronic surveillance, if brief, narrowly focused, and approved in advance by a judge, could be constitutional.[143]

Subsequent cases began to limit this expansive view of the Fourth Amendment. In *United States v. Miller*,[144] the Court held that business and banking records "lack . . . any legitimate expectation of privacy"[145] once they are given to a third party, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the

---

135. *See supra* note 131.

136. Frank J. Eichenlaub, Comment, *Carnivore: Taking a Bite out of the Fourth Amendment?*, 80 N.C. L. REV. 315, 334 (2001).

137. 388 U.S. 41 (1967).

138. N.Y. CODE CRIM.PROC. § 813-a (McKinney's 1967).

139. *Berger*, 388 U.S. at 44.

140. 389 U.S. 347 (1967).

141. *Katz*, 389 U.S. at 361 (Harlan, J. concurring).

142. *Id.* at 354.

143. James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 70–71 (1997).

144. 425 U.S. 435 (1976).

145. *Id.* at 442.

confidence placed in the third party will not be betrayed."[146] In *Smith v. Maryland*,[147] the Court applied *Miller* and held that there is no legitimate expectation of privacy in the information that pen registers collect.[148] Determining the level of protection that a given form of communication should receive is a task that continues to bedevil Congress and the courts, as the following sections of this Note illustrate.

B. Statutory Framework

In Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[149] ("Title III" or the "Wiretap Act"), Congress codified the Supreme Court's holding in *Katz*. The Wiretap Act also illustrates, however, that the protections of the Fourth Amendment do not easily translate to new technologies, absent application of the Fourth Amendment by the Supreme Court. Congress has taken some measures to maintain the balance between advances in technology and the potential "evisceration of Constitutional rights"[150] that technological advances could effect.

The resulting body of electronic surveillance law is complex. The same laws govern state and private conduct and simultaneously provide civil and criminal penalties. Changes enacted under the USA PATRIOT Act (USAPA)[151] further complicate the statutes. Only a few of the many changes[152] that the USAPA effected will be discussed here.[153]

---

146. *Id.* at 443.

147. 442 U.S. 735 (1979).

148. *Id.* at 743-44 (holding that, just as a bank depositor "'assume[s] the risk' of disclosure" of the contents of financial records to third parties, so does a person "assum[e] the risk that the [phone] company would reveal to police the numbers he dialed").

149. 18 U.S.C. §§ 2510-2522 (2000).

150. United States v. Scarfo, 180 F. Supp. 2d 572, 583 (D.N.J. 2001).

151. Uniting and Strengthening America by Providing Appropriate Tools Required to the Intercept and Obstruct Terrorism, Pub. L. No. 107-56, 115 Stat. 272 (2001).

152. The final version of the Act was 342 pages long and modified fifteen statutes. Elec. Frontier Found., *Analysis of The Provisions of The USA PATRIOT Act*, *at* http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (Oct. 31, 2001).

153. Many detailed analyses of the USAPA are available. Ctr. for Democracy & Tech., *Analysis of USA PATRIOT Act by CDT and Others*, *at* http://www.cdt.org/security/usapatriot/analysis.shtml (collecting resources) (Feb. 21, 2003). Sources that are particularly relevant to the topics discussed here are CCIPS, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, *at* http://www.cybercrime.gov/s&smanual2002.pdf (July 2002) (summarizing Title III and ECPA and the procedures for conducting surveillance and gathering evidence under these laws) [hereinafter CCIPS, *Searching and Seizing Computers*] and *USA PATRIOT Act (P.L. 107-56) Amendments Made by Key Provisions to: Electronic Communications Pri-*

C. Title III and the Electronic Communications Privacy Act (ECPA)

Title III bans wiretapping by the government except in investigations of enumerated crimes,[154] and only after showing a neutral magistrate that ordinary investigative techniques are ineffective.[155] Title III also requires that investigators minimize the data that they collect and provides procedural opportunities to object to evidence collected in a wiretap before it is introduced into a criminal trial.[156] In its original form, however, Title III applied only to the interception[157] of a "wire communication," which is "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception,"[158] or an "oral communication."[159]

When computer-based communications became more common, Congress expanded Title III protection to "electronic communications."[160] In Title I of the ECPA,[161] Congress created statutory protection for electronic communications in transmission, including "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[162] Thus, the ECPA extended protection to electronic communications, but did so by creating a separate category of communications based on the underlying medium of transmission.

The distinction between wire and electronic communications is important because Title III provides a suppression remedy for illegally

---

vacy Act; Communications Act; Foreign Intelligence Surveillance Act; Computer Fraud & Abuse Act, at http://www.cdt.org/security/usapatriot/keyprovisions.pdf (Nov. 2001).

154. 18 U.S.C. § 2516.

155. *Id.* § 2518(3)(c); Dempsey, *supra* note 143, at 71-72.

156. *Id.* § 2518(5); Dempsey, *supra* note 143, at 71-72.

157. The focus on *interception* is highly significant. *See* the discussion of *Konop*, *infra* Part III.A.4.

158. 18 U.S.C. § 2510(1).

159. "'[O]ral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." *Id.* § 2510(2).

160. *See* Steve Jackson Games, Inc. v. Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994) (citing the prohibition on intercepting an "electronic communication" in 18 U.S.C. § 2511(a)).

161. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2510-2522, 2701-2716, 3121-3127).

162. 18 U.S.C. § 2510(12) (2000).

intercepted wire communications,[163] but not for illegally intercepted electronic communications.[164] It is also worth re-emphasizing that Title III applies only to the interception—the acquisition of the contents of a communication contemporaneous with transmission[165]—of wire and electronic communications; but Title III does not apply to communications in storage. Recognizing that this gap left the increasing volume of non-voice and electronic communications without Fourth Amendment or Title III protection,[166] Congress created in Title II of the ECPA protection for stored electronic communications.[167]

Until Congress passed the USAPA, wire and electronic communications became "stored" at different times. Specifically, an electronic communication entered electronic storage when "a copy of a communication [is] created at an intermediate point that is designed to be sent on to its final destination."[168] The USAPA left this definition unchanged but altered the classification of voice mail. Whereas voice mail used to be a wire communication "in transmission" until its recipient listened to it, and so was protected by Title III's suppression remedy, the USAPA placed all voice mail within the ambit of Title II of the ECPA.[169] Thus, investigators' failure to obtain the proper warrant for voice mail can no longer serve as a basis for exclusion of that evidence.[170]

---

163. *Id.* §§ 2510(11), 2515, 2518(10)(a); CCIPS, *Searching and Seizing Computers*, *supra* note 153, at 134-35.

164. § 2518(10)(c); CCIPS, *Searching and Seizing Computers*, *supra* note 153, at 134-35.

165. 18 U.S.C. § 2510(4); *Steve Jackson Games*, 36 F.3d at 460.

166. Dempsey, *supra* note 143, at 73-74.

167. Title II of the ECPA is also known as the Stored Communications Act (SCA). Konop v. Hawaiian Airlines, 302 F.3d 868, 874 (9th Cir. 2002).

168. CCIPS, Searching and Seizing Computers, *supra* note 153, at 86 (analyzing the definition of "electronic storage").

169. Uniting and Strengthening America by Providing Appropriate Tools Required to the Intercept and Obstruct Terrorism, Pub. L. 107-56, 115 Stat. 272 (2001) Uniting and Strengthening America by Providing Appropriate Tools Required to the Intercept and Obstruct Terrorism § 209, Pub. L. 107-56, 115 Stat. 272 (2001) (striking electronic storage of communications carrying a human voice from the definition of "wire communication" in 18 U.S.C. § 2510(1)). *See also* CCIPS, *Searching and Seizing Computers, supra* note 153, at 118 ("Stored wire communications (e.g. voice mails) are covered not under Title III, but instead under the ECPA provisions that also apply to stored electronic communication, or e-mails"). Even before Congress passed the USAPA, voice mail became a communication in electronic storage once the recipient had listened to the message. *See id.* at 86-87 (analyzing the definition of "electronic storage" in 18 U.S.C. § 2510(17)).

170. 18 U.S.C. § 2708 (("The [damages] remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of

Underlying the ECPA's approach to regulating government access to e-mail, account records, or subscriber information,[171] is the fact that the relevant communications are almost always stored on a computer that is not the property of the recipient of the relevant communication, or to whom the data subscription data pertains. The baseline of protection is therefore not the Fourth Amendment's guarantee of security in a person's papers or effects, but rather the rule of third-party possession, which makes unreasonable the expectation of privacy in a communication held by a third party.[172] Although this result makes sense in terms of the history[173] of third-party possession, it is incongruous with the laws discussed in Part II. of this Note. The CFAA creates the rough equivalent of a criminal trespass statute with respect to intrusions against the owner of the computer. The DMCA criminalizes penetrations of the "digital walls" around copyrighted works, no matter where they are stored. The reliance of Internet users upon third parties for almost all aspects of their activities, however, excludes them from such strong, property-based protection, regardless of the prevalent perception of e-mail as deserving of Fourth Amendment protection.

D. Judicial Anticipation of the USAPA

Despite the obvious relevance of Title III and the ECPA to criminal investigations, the differences in the statutory language regarding the interception of wire and electronic communications were first explored in civil cases. In *Steve Jackson Games v. Secret Sevice*, the Fifth Circuit was the first court to squarely confront the disparate treatment of wire communications and electronic communications. The *Steve Jackson Games* court held that "an intercept requires participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of the device."[174] Absent explicit inclusion of storage of an electronic communication in the definition of the communication, in a manner parallel to that of wire communication, the Fifth Circuit held that interception, and thus the Title III warrant requirements, apply to electronic communications only as they pass over the wires from one computer to another.

---

this chapter."); CCIPS, *Searching and Seizing Computers, supra* note 153, at 107 ("ECPA does not provide a suppression remedy.").

171. CCIPS, *Searching and Seizing Computers, supra* note 153, at 82.

172. *Id.* at 82 n.14.

173. *See id.* for a brief account of important historical cases.

174. *See* Steve Jackson Games, Inc. v. Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994) (emphasis added) (quoting United States v. Turk, 526 F.2d 654 (5th Cir. 1976)).

The Ninth Circuit was the next court to confront this issue, and in *Konop v. Hawaiian Airlines*, the court expressed its agreement with the holding in *Steve Jackson Games*.[175] The court, applying Title III and the ECPA as they stood before passage of the USAPA, noted that Congress, through the USAPA, "accepted and implicitly approved the judicial definition of 'intercept.'"[176] Thus, beginning with the notion that Konop's website was somehow his "property" would be seriously misleading. Although Congress has given statutory protection to most forms of electronic communications, those communications are not protected as ordinary property. Instead, a complex body of surveillance law, in which the ownership of the equipment on which the communication resides, plays a deciding role. Simply put, a home page is not like a home with respect to government searches and surveillance.

IV. CONCLUSION

These judicial and legislative developments draw attention to the sharp contrast between computer intrusions and disseminated intellectual property on the one hand, and the communications of individuals on the other. As shown in Part II, Congress has revised both copyright law and the quintessential cybercrime statute, the CFAA, to incorporate more explicitly the protections grounded in the concepts of real and personal property into any given piece of computing equipment, or any copy of a piece of copyrighted material. Owners of "protected computers"[177] and copyrights are acquiring ever-stronger rights against the world because Congress continues to lean on "access" to a resource as a means of regulating online behavior. This protection against unauthorized access is limited in an important way, however, because it applies to the owner of the resource.[178]

The legal protection that attaches to the owner of the machinery itself is stronger than the protection that the owner of the information enjoys. The distribution of personal information continues to decentralize, spreading among the three "legal regimes for access to electronic data"[179]—the Fourth Amendment for information stored on one's own devices, the recently amended Title III and ECPA standards for

175. *Konop v. Hawaiian Airlines*, 302 F.3d 868, 878 (9th Cir. 2002).

176. *Id.*

177. 8 U.S.C. § 1030(e)(12) (2000).

178. Thus, the fact that someone "owns" an e-mail message counts for little when that e-mail message resides in electronic storage, or on a remote computing resource. *See* CCIPS, *Searching and Seizing Computers, supra* note 153, at 85-89.

179. Dempsey, *supra* note 143, at 88-89.

communications in transmission and storage, and the ambiguous category of records stored on a remote server.[180] This trend, coupled with the USAPA's recent relaxations of the regulations governing law enforcement agents' access to communications, points to the need for Congress to ensure that procedural protections for access to electronic communications keep pace with their role in society. Whether this calls for the creation of a new property right in remotely stored communications[181] should be the subject of future debate. A more urgent challenge is to raise public awareness of exactly how divergent are the traditional protections of the Fourth Amendment from those that actually extend to most electronic communications, despite the increasingly strong protections that Congress has extended through federal rights in copyright, trade secrets, and the control of access to computer systems.

180. *Id.*

181. For an argument against this particular approach, but a persuasive case for the need to debate this question, see Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125 (2000).