The University of Chicago Law School Roundtable

Volume 1 | Issue 1 Article 20

1-1-1993

The National Stolen Property Act and Computer Files: A New Form of Property, a New Form of Theft

Todd H. Flaming

The National Stolen Property Act and Computer Files: A New Form of Property, a New Form of Theft

Todd H. Flaming[†]

Section 2314 of the National Stolen Property Act ("NSPA") imposes a fine and a jail sentence on any person who "transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud."[1] In *Dowling v United States*, the Supreme Court held that the Act's "stolen, converted or taken by fraud" language did not extend to a case of pure copyright infringement.[2] Although ostensibly a case about whether copyright infringement is equivalent to stealing, converting or taking by fraud, the opinion contains hints that the NSPA does not apply at all to the taking of purely intangible property.

What happens to a person who uses his computer to connect to another person's computer without permission through the use of a modem and instructs that person's computer to download a confidential file?[3] Like pure copyright infringement, there is not the kind of "physical" taking involved that there would be were the person to break into the victim's home and steal data disks. However, unlike pure copyright infringement, an uninvited intrusion into the victim's privacy occurs, albeit through the use of analog signals over the phone lines.

---

† B.A. 1988, Loyola Marymount; J.D. 1993, The University of Chicago. The author is currently an associate with Schopf & Weiss in Chicago.

1 National Stolen Property Act, 18 USC § 2314 (1990) (the "Act" or "NSPA").

2 *Dowling v United States*, 473 US 207, 228 (1985).

3 Using a personal computer attached to a device called a "modem" (modulator/demodulator), any person can use phone lines to connect to another computer that also has a modem which is waiting to answer incoming calls. The modem translates digital information (the computer's information) into analog signals and broadcasts them over a phone line. The receiving modem answers the phone, waits for a signal that another computer is calling (like a fax machine), and then establishes a link. Once connected, the caller can usually instruct the answering computer to list the computer files it contains and to send them over the phone line to his computer.

Lower courts confronting this problem have read *Dowling* in two conflicting ways. One side considers *Dowling* a case about tangibility and holds that for a person's misconduct to fall under the NSPA, he must take a "physical thing" from someone else and transport that thing across state lines. The other side reads *Dowling* as a case about copyrights, holding that copyright infringement is better left to the copyright laws than to statutes dealing with stolen property.

This Comment argues that the latter view is preferable. The *Dowling* opinion stresses the existence of another federal statutory scheme—the copyright laws—that covers cases of pure copyright infringement. The opinion argues that the existence of such a scheme evidences an intent to deal with copyrights exclusively through that scheme.[4] While courts have generally been reluctant to recognize complex forms of property, a great deal of case law interpreting the NSPA extends its coverage well beyond the realm of purely physical property. To read into the NSPA the requirement of physical tangibility creates incongruities in its application with some absurd results. To read the NSPA to cover theft via modem fits with the purposes of the Act. More importantly, reading the NSPA to cover computer files provides a foundation for preserving basic property rights at a time when society is on the verge of abandoning paper as a medium of storage.

Part I of this Comment outlines the *Dowling* decision and the lower court decisions confronting theft over the phone lines. Part II addresses the arguments of the lower courts interpreting *Dowling* as applied to theft of computer files and concludes that *Dowling* is more properly read as a case about copyrights, not a case about tangibility. Part III argues that the purpose of the NSPA is consistent with that reading of *Dowling* and that recognition of property rights in computer files will be essential to preserving the current status of property rights that courts recognize in information. Finally, Part IV applies the NSPA to a hypothetical case of theft via modem and addresses the question of valuation.

---

[4] *Dowling*, 473 US at 228.

I. *DOWLING* AND THE COMPUTER FILE THEFT CASES

A. *Dowling*

In *Dowling v United States*,[5] the Supreme Court held that mere copyright infringement does not constitute stealing, converting or taking by fraud as defined in the NSPA. The defendant compiled a collection of bootleg recordings of Elvis Presley songs and subsequently transported the phonorecords across state lines.[6] The government argued that the act of infringing a copyright is sufficiently similar to stealing, converting, or defrauding someone out of property that the NSPA should apply to transporting phonorecords which contain material in violation of the copyright statute. The Court refused to consider the government's second argument that Dowling had "obtained the source material through illicit means."[7] Therefore, the government's only argument was that Dowling's unauthorized use of recordings to which he had legitimate access was a form of theft.[8]

The Court rejected the government's comparison of copyright infringement with stealing and noted that all cases interpreting the NSPA involved physical goods, wares or merchandise that were themselves stolen.[9] The opinion then reasoned that the NSPA's requirement that the goods, wares or merchandise be "'the same' as those 'stolen, converted or taken by fraud' seems clearly to contemplate a physical identity between the items unlawfully obtained and those eventually transported, and hence some prior physical taking of the subject goods."[10]

---

[5] 473 US 207.

[6] Id at 210-11.

[7] Id at 215 n 7. The Court chose to ignore this alternative basis for finding statutory theft for three reasons. First, the counts in the indictment upon which Dowling was convicted contained only allegations of copyright infringement. Second, the Ninth Circuit on appeal based its decision solely on copyright infringement as opposed to "any theory of illegal procurement." Third, even if the stipulated testimony had contained enough evidence to establish wrongful procurement of the source material, no one had addressed the evidentiary issue of valuation up to that point. Id.

[8] There was no argument "that Dowling wrongfully came by the phonorecords actually shipped or the physical materials from which they were made," or "that the objects that Dowling caused to be shipped, the bootleg phonorecords, were 'the same' as the copyrights in the musical compositions that he infringed by unauthorized distribution of Presley performances of those compositions." Id at 214.

[9] Id at 216.

[10] Id.

The Court devoted the remainder of the opinion to addressing the unique characteristics of a copyright. It pointed out that a copyright "comprises a series of carefully defined and carefully delimited interests to which the law affords correspondingly exact protections."[11] It observed that a copyright owner does not have complete control over the copyright, that § 107 of the Copyright Act contains a "fair use" exception and that § 115 grants compulsory licenses in nondramatic musical works.[12] The Court also pointed out that one who arrogates the use of an author's protected work neither assumes "physical control over the copyright" nor "wholly deprive[s] its owner of its use."[13] The Court concluded that copyright infringement "fits but awkwardly within the language Congress chose [in the NSPA]."[14]

Having decided that copyright infringement fits awkwardly within the statutory language, the Court considered the purposes of the NSPA. It noted that the NSPA serves to fill the gaps where state enforcement is inadequate to address a particular type of crime and that federal law already fills the gap where copyright infringement is concerned.[15] The Court noted: "the premise of § 2314—the need to fill with federal action an enforcement chasm created by limited state jurisdiction—simply does not apply to the conduct the Government seeks to reach here."[16] The Court found an additional reason to hesitate before extending the NSPA to cover this case in Congress's reliance on principally civil remedies where copyright infringement is concerned.[17] In short, the Court found copyright infringement to be sufficiently different from stealing, converting and taking by fraud that the NSPA should not apply to it.

B. Computer File Theft

The holding in *Dowling* is unclear. Although purportedly a case about the meaning of "stolen, converted or taken by fraud," the "physical taking" language can be read to suggest that only physical goods come under the protection of the NSPA. Does that

---

[11] Id.

[12] Id at 217, citing *Harper & Row, Publishers v Nation Enterprises*, 471 US 539, 547 (1985).

[13] *Dowling*, 473 US at 217.

[14] Id at 218.

[15] Id at 220-21.

[16] Id at 221.

[17] Id at 221-25.

mean that files on a computer do not come under the protection of the NSPA? Two recent cases have reached opposite conclusions in interpreting the *Dowling* decision as applied to this question.

1. *United States v Riggs.*

Two men, Riggs and Neidorf, devised a plan to acquire Bell South Telephone Company's E911 file that was stored on Bell South's computer system in Atlanta.[18] The E911 file was a text file that contained Bell South's procedures for installation, operation, and maintenance of emergency 911 services; services for handling emergency calls to police, fire, ambulance; and other emergency services for municipalities. Using a computer with a modem, Riggs dialed into Bell South's computer without authorization and downloaded[19] the file. Riggs used other people's account numbers and passwords both to gain access to the computer and to disguise himself while online. Riggs then uploaded the file over an interstate network to a bulletin board in Lockport, Illinois.[20] Neidorf downloaded the file from the Lockport bulletin board, altered it and later published the altered version in his newsletter, *Phrack*.[21] The government alleged that the file was worth about eighty thousand dollars, well above the NSPA minimum.[22]

Counts III and IV of the indictment charged Riggs and Neidorf with violating § 2314.[23] The court rejected Neidorf's argument that he did not fall within the NSPA because he only sent electric impulses over the wire. The court likened the trans-

---

[18] *United States v Riggs*, 739 F Supp 414, 416-17 (N D Ill 1990). The facts are set out at pages 416-17.

[19] "Downloading" means instructing the computer a person calls to send a computer file over a modem to that person's computer. The opposite, "uploading," involves sending a file to the computer called over the modem. See *Riggs*, 739 F Supp at 417 n 3.

[20] A bulletin board is a computer which users can call using a computer with a modem. The board allows users to upload files for others to use or to download files others have left there. For a good discussion of the workings of bulletin boards, see Elizabeth McGinnis, *BBS 101*, Online Access 6 (May 1993).

[21] Neidorf sent the file back to the bulletin board for Riggs' approval before publishing it.

[22] For an excellent discussion of the case, see Bruce Sterling, *The Hacker Crackdown* 250-82 (Bantam Books, 1992), which contains a copy of the edited version of the E911 file at pages 262-73. The file contains very little technical information and is primarily an administrative document. The government's figure appears to have been far off the mark. During the trial the defense introduced evidence that, to the surprise of a testifying prosecution witness, the information was available to the public for about thirteen dollars. Id at 282.

[23] Previous counts charged the defendants with wire fraud.

fer of the text file over the line to the transfer of money by wire, which courts had previously found to be encompassed by the NSPA.[24]

The more interesting question in *Riggs* was whether the proprietary information contained in the E911 text file constituted "goods, wares or merchandise" under the Act. The court noted that the law was well-settled that the NSPA applied to theft of a tangible medium where intangible property was attached to it—for example, a chemical formula written on a piece of paper.[25] The court then reasoned that using a modem to steal the information, rather than Bell South's own data disk, should be no different.[26] The court distinguished *Dowling* on the ground that the *Dowling* Court never construed the meaning of "goods, wares [or] merchandise."[27] Additionally, the *Riggs* court reasoned that to read a tangibility requirement into the definition of "goods, wares [or] merchandise" would lead to absurd results. The court provided an example of such an absurd result: the NSPA would not apply to a trucker who steals a colorless, odorless, tasteless gas by pumping it into his truck and transporting it across state lines.[28]

As to whether the text file was "stolen, converted or taken by fraud," the court distinguished *Dowling* by reading the case as a case about copyrights: "As *Dowling* and *Smith* recognized, the copyright holder owns only a bundle of intangible rights which can be infringed, but not stolen or converted. The owner of confidential, proprietary business information, in contrast, possesses something which has clearly been recognized as an item of property."[29] The court also rejected Neidorf's argument that, like the Copyright Act, the Computer Fraud and Abuse Act was intended to be the only statute governing the area of computer abuse. The

---

[24] *Riggs*, 739 F Supp at 420.

[25] *Riggs*, 739 F Supp at 420-21. The court cited *United States v Greenwald*, 479 F2d 320, 322 (6th Cir 1973) (chemical formulae attached to piece of paper); *United States v Bottone*, 365 F2d 389, 393 (2d Cir 1966) (patented process attached to piece of paper); *United States v Lester*, 282 F2d 750, 754-55 (3d Cir 1960) (geophysical maps); and *United States v Seagraves*, 265 F2d 876 (3d Cir 1959) (same facts as *Lester*).

[26] *Riggs*, 739 F Supp at 420-21.

[27] Id at 421 n 9.

[28] Id at 421.

[29] Id at 422-23.

court looked to the legislative history and found no evidence that Congress intended it to be the exclusive statute governing computer crime.[30]

2. *United States v Brown.*

The Tenth Circuit reached a conclusion opposite that of *Riggs*, finding that computer source code[31] does not constitute "goods, wares, [or] merchandise" under the NSPA.[32] Brown left employment as a programmer with a company called The Software Link ("TSL"). Federal investigators later obtained a warrant to search Brown's home and found a hard disk and three binders containing the source code for PC-MOS/386, a computer program developed by TSL. Because the government could not prove that Brown stole the hard disk from TSL, the court assumed that Brown merely copied the code onto his own disk.

The Tenth Circuit held that in light of *Dowling*, the NSPA does not apply to purely intangible property.[33] The government's argument attempted to distinguish the case from *Dowling* on the ground that Brown, unlike the defendant in *Dowling*, must have physically taken the code from TSL, as TSL never released the source code to anyone in the public.[34] The court rejected this argument, because it read *Dowling* as holding that the NSPA only applies to "physical 'goods, wares or merchandise.'"[35] The opinion made no attempt to distinguish *Riggs* on the basis of the type of computer file stolen (for example, a source code file instead of a text file). Hence, the *Brown* opinion is directly contrary to the *Riggs* holding.

II. WHAT *DOWLING* REALLY MEANS

Whether the NSPA applies at all to a case of pure computer file theft depends on whether one adopts the *Riggs* or *Brown*

---

[30] Id at 423.

[31] In general, source code is just a text file with a computer program written in it in a language that human beings can read (or stored in a binary format, but able to be read by human beings with the use of a translator). When the programmer is finished, he "compiles" the source code file with a "compiler," turning it into binary language that the computer can read. At that point the source code text file has been transformed into a workable computer program.

[32] *United States v Brown*, 925 F2d 1301, 1308-09 (10th Cir 1991). The facts of the case appear at pages 1302-03, and 1305-07.

[33] Id.

[34] Id at 1307.

[35] Id at 1308-09.

reading of *Dowling*. The *Riggs* opinion suggests that *Dowling* is only a case about copyrights. Under this reading, there is room to use § 2314 to prosecute a person for transporting or transmitting unauthorized copies of computer files across state lines. However, the *Brown* opinion suggests that *Dowling* limits the application of the NSPA to cases involving theft of some tangible item. Under this reading, the only possible prosecutions are those for items such as stolen data disks. For example, assume an employee steals a source code file worth well in excess of $5,000 from his company and moves to a new state. Under the *Riggs* reading of *Dowling*, the NSPA applies to his conduct. However, under the *Brown* reading of *Dowling*, whether the NSPA applies or not turns on whether he travelled across state lines with the files on his own diskettes or the company's diskettes. Under *Brown*'s reading, in other words, one can avoid prosecution under the NSPA by simply copying the files onto his own diskette.

The *Riggs* reading of *Dowling* makes sense. While some of the language in *Dowling* about tangibility lends support to the Tenth Circuit's argument in *Brown*, the relevant language is in dicta and none of it directly limits the Act's application to physical goods. Furthermore, requiring tangibility under the NSPA casts doubt on a long line of cases holding that electronic funds transfers fit under the NSPA. Moreover, viewed in a broader context, it appears that the *Dowling* Court was getting at something other than naked tangibility.

A. Separate Elements of the Violation

The *Brown* opinion obscures the distinction between the issue of whether an item is the sort of property covered by the statute and the issue of whether the acts used to acquire an interest in that property are covered by the statute. However, it is important to distinguish the two and to address the elements of a NSPA violation separately.

The Court in *Dowling* defined the elements of a violation of the NSPA:

> Section 2314 requires, *first*, that the defendant have transported "goods, wares, [or] merchandise" in interstate or foreign commerce; *second*, that those goods have a value of "$5,000 or more"; and, *third*, that the defendant "kno[w] the

same to have been stolen, converted or taken by fraud."[36]

Because the Court emphasized the need for precision in construing criminal statutes,[37] and because it stressed that the elements of the violation are separate, interpretation of *Dowling* requires a careful reading of the opinion with respect to both.

1. Goods, Wares or Merchandise.

The Tenth Circuit in *Brown* started with the premise that "*Dowling* holds that § 2314 applies only to physical 'goods, wares or merchandise.' Purely intellectual property is not within this category."[38] However, two aspects of *Dowling* suggest that the *Brown* court overstated the holding of the case. First, the *Dowling* Court only addressed the issue of whether the copyright infringement at issue fit within the language of "stolen, converted or taken by fraud."[39] The Court never had to decide what the phrase "goods, wares [or] merchandise" means. Further, Dowling never challenged that the items were goods under the statute.[40] Therefore, any language in the opinion to the effect that the statute only covers tangible "goods, wares or merchandise" is dictum.

More importantly, the *Dowling* Court never actually stated that only tangible goods fit under the NSPA. *Brown* cites to page 216 of the *Dowling* opinion for its conclusion that the Court held that the phrase "goods, wares [or] merchandise" only includes

---

[36] *Dowling*, 473 US at 214 (emphasis added).

[37] Id at 213 ("[W]hen assessing the reach of a federal criminal statute, we must pay close heed to language, legislative history, and purpose in order strictly to determine the scope of the conduct the enactment forbids.").

[38] *Brown*, 925 F2d at 1307. The *Brown* court is not alone in this conclusion. See Note, *The National Stolen Property Act and its Applicability to Property Rights in Computer Source Code—Do Rights Exist?*—United States v. Brown, *925 F.2d 1301 (10th Cir. 1991)*, 11 Temple Envir L & Tech J 155 (1992).

[39] The court stated: "We must determine, therefore, whether phonorecords that include the performance of copyrighted musical compositions for the use of which no authorization has been sought nor royalties paid are consequently 'stolen, converted or taken by fraud' for purposes of § 2314." *Dowling*, 473 US at 215-16.

[40] The opinion notes: "Dowling does not contest that he caused the shipment of goods in interstate commerce, or that the shipments had sufficient value to meet the monetary requirement. He argues, instead, that the goods shipped were not 'stolen, converted or taken by fraud.'" Id at 215. If Dowling meant to argue that the records themselves were not stolen, but that what was stolen, the intellectual property, was not "goods," he might have made this argument directly. There was no dispute that Dowling did not steal the material used to makes the records. Therefore, everyone understood that Dowling was not being prosecuted for theft of the records themselves. The issue in the case was whether the intellectual property was "stolen" through the process of copyright infringement.

tangible items. The relevant portion of that page contains no direct statement to that effect. The relevant passage reads: "But these cases and others prosecuted under § 2314 have always involved physical 'goods, wares, [or] merchandise' that have themselves been 'stolen, converted or taken by fraud.'"[41] This passage refers only to previous cases. Before the *Dowling* decision there were no decisions about theft of computer files. Moreover, the statement is inclusive, but not necessarily exclusive. The sentence does not say: "As has always been the case, to fit under the Act goods must be tangible." In fact, the Court did not use the term "tangible" or "physical" in order to modify or limit the phrase "goods, wares [or] merchandise" anywhere in the opinion.

Therefore, although the *Brown* court read *Dowling* to hold that the phrase "goods, wares, [or] merchandise" includes only tangible items, the *Dowling* opinion does not support such a reading. Given the *Dowling* Court's careful statement of the issue before it[42] and its emphasis on the need to be precise in construing a criminal statute,[43] the *Riggs* court's reading of *Dowling* on goods, wares or merchandise is more accurate.

2. Stolen, Converted or Taken by Fraud.

It is more plausible to read *Dowling* as holding that under the NSPA only tangible items may be "stolen, converted or taken by fraud," than that the goods, wares or merchandise themselves must be tangible. The *Dowling* Court noted:

> by requiring that the 'goods, wares, [or] merchandise' be 'the same' as those 'stolen, converted or taken by fraud,' the provision seems clearly to contemplate a physical identity between the items unlawfully obtained and those eventually transported, and hence some prior *physical taking* of the subject goods.[44]

This statement comes close to holding that only a taking of physical goods falls under the meaning of "stolen, converted or taken by fraud."

However, such a reading is problematic for three reasons.

---

[41] Id at 216.

[42] Id at 215-16.

[43] Id at 213.

[44] Id at 216 (emphasis added).

First, the opinion contains no direct language stating that only physical goods may be taken. The phrase "physical taking of subject goods" is strikingly different from a possible alternative wording: "taking of physical goods." In other words, "physical taking" is not equivalent to a taking of physical goods. This reading makes sense given the next sentence in the opinion: "In contrast, the Government's theory here would make theft, conversion, or fraud equivalent to wrongful appropriation of statutorily protected rights in copyright."[45] The act of "physical[ly] taking" appears to be something "[i]n contrast" to an act of purely wrongful appropriation as defined in the copyright statute.[46]

Second, reading *Dowling* as grafting a requirement of a taking of physical goods onto the NSPA is problematic, because the opinion assumes that Dowling had proper access to the recordings. The opinion carefully assumes away any facts suggesting that Dowling came across the recordings through illicit means. The Court noted:

> The Government argues in the alternative that even if the *unauthorized use* of copyrighted musical compositions does not alone render the phonorecords contained in these shipments 'stolen, converted or taken by fraud,' the record contains evidence amply establishing that the bootleggers obtained the source material through illicit means. . . . For several reasons, we *decline to consider* this alternative basis for upholding Dowling's convictions.[47]

In other words, the Court took the case on the assumption that Dowling did not use illicit means to acquire the Presley recordings. Because the Court explicitly refused to address the issue of whether "illicit means" of acquiring the intangible property might result in a different decision, the question is, at a

---

[45] Id.

[46] Perhaps a valid distinction between theft via modem or copying and copyright infringement is the reverse of Neidorf's own argument (Neidorf was a defendant in the *Riggs* case): that electric impulses carrying the file over the phone line or onto the disk actually are tangible items, and causing them to flow over the wire or onto the disk is a form of "physical taking" or carrying off in a way that merely infringing a copyright (which involves no similar form of physical carrying off) is not.

[47] *Dowling*, 473 US at 215 n 7 (emphasis added). The Court refused to consider the Government's alternative argument; because the counts in the indictment were founded exclusively on copyright infringement, the Court of Appeals rested its decision solely on copyright infringement, and even if there had been enough evidence in the record to support the argument, no one had addressed the issue of valuation under the alternative theory. Id.

minimum, still open.[48]

Third, reading *Dowling* as requiring a taking of physical goods is problematic, because the *Dowling* Court devoted the majority of its attention to the nature of a copyright as something distinct from a right to property under the common law. The Court addressed the narrow issue of whether copyright infringement constitutes stealing, converting or taking by fraud under the statute. The Court was never asked to address anything more than that. The Court's narrow focus on copyright suggests that any language applying the case to something beyond copyright is dictum.

The narrow focus on copyright also means that the case can be read as holding only that the extensive statutory scheme set up to create, regulate and enforce copyright protection was designed to operate as a closed system. Three aspects of the Court's reasoning support this argument. First, the Court addressed the history and purpose of the NSPA, concluding that "the premise of § 2314—the need to fill with federal action an enforcement chasm created by limited state jurisdiction—simply does not apply" to copyright infringement.[49] The Court based this conclusion on the observation that the Constitution grants Congress the authority to legislate directly in the area of copyrights and that Congress did so by carefully defining both the rights and their enforcement in the Copyright Act.[50] Second, the Court went further, basing its holding on the history of copyright infringement provisions as chiefly providing civil remedies and providing criminal remedies

---

[48] One might argue that this alone distinguishes the case from a case of pure computer file theft. In other words, copyright infringement is different from gaining control over property without authorized access to the material. Consider three examples: (1) an unauthorized intruder steals the victim's car from his house; (2) an unauthorized intruder copies the victim's computer files onto the intruder's own disks and leaves with the disks; (3) a record producer fails to seek permission when he records a song to which he had proper access. If we ask whether something was "tak[en]" as the Supreme Court understands the concept in the *Dowling* opinion, the answer is unclear. However, in the first two cases the thief gains unauthorized access to the victim's premises. Indeed, the *Brown* opinion recognizes this problem: "It is true that the intellectual property involved in the instant case was more nearly 'stolen, converted or taken by fraud' in the sense that it was at no time freely presented to the public as had been the recordings in *Dowling*." *Brown*, 925 F2d at 1307-08. However this distinction is shaky. First, it does not account for a case of pure conversion (for example, an employee who fails to return backup disks of company files after he is fired and no longer has a right to possess them). Second, the physical act of recording without permission copyrighted material to which one has proper access is in itself a form of unauthorized access.

[49] Id at 221.

[50] Id at 218-21.

only after careful deliberation.[51]

Third, the Court used as an example a case of pure copyright infringement with no reference to illicit taking of the property. The Court, toward the end of its opinion, noted that extending the NSPA might have "broad consequences . . . both in the field of copyright and in kindred fields of intellectual property law."[52] The Court offered a hypothetical case involving a case of copyright infringement which it considered to be out of the reach of the NSPA. The hypothetical case involved *The Nation* magazine publishing excerpts from President Ford's unpublished memoirs. Notably, the Court did not mention how *The Nation* acquired the manuscript, but stressed only the copyright violation.[53]

Although full of language suggesting that intellectual property does not fall under the scope of the NSPA, *Dowling* contains no language explicitly limiting the NSPA to a taking of physical goods. Also, the opinion explicitly limits its holding to a case in which the copyright infringer did not gain access to the material through illicit means. Most importantly, *Dowling* is devoted primarily to establishing that the copyright statute does not contain enforcement gaps, and is designed to operate as a closed system. Given this reading of *Dowling*, the *Brown* court's conclusion that the NSPA cannot cover intangible property may be premature.

B. Other Intangible Property Cases

There is dicta in *Dowling* that supports the *Brown* court's conclusion that the NSPA does not apply to intangible property. However, good reasons exist to believe that the *Dowling* holding was not intended to reach beyond copyright law. If one were to accept the *Brown* reading, *Dowling* narrows application of the NSPA to the taking and transportation of physical objects. If so, *Dowling* either overrules a long line of cases applying the NSPA to electronic funds transfers or renders application of the NSPA anomalous. Also, under this reading, in intangible property cases the NSPA protects only the medium (the diskette) and not the message (the file).

---

[51] Id at 221-26.

[52] Id at 226.

[53] Id.

1. Wire Transfer Cases.

The difficulty with reading the *Dowling* case to hold that only physical goods may be taken is that it runs counter to a line of cases reaching the opposite conclusion. In an early case, *United States v Levy*,[54] the Fifth Circuit held that the NSPA was broad enough to account for a change in form of securities moved into interstate commerce. The defendant wrote checks from a company bank account and deposited them into a bank account across state lines. The defendant was technically authorized to write the check, but did not have permission to do so.[55] He argued that while the money itself may have been obtained by fraud, because he had authority to write the checks, the checks themselves were not obtained by fraud.[56] The court, rejecting his characterization, reasoned:

> Read literally the statute would require that the very object taken by fraud be transported in interstate commerce. However, such a narrow reading of the statute would clearly frustrate the purpose of Congress: Congress had in mind preventing further frauds or the completion of frauds partially executed.[57]

Consistent with this reasoning, in *Lagerquist v United States*,[58] the court held that bank checks fit within the language of the NSPA, even though they were not stolen, but obtained through the sale of fraudulently obtained goods.

In a more recent case, *United States v Kroh*,[59] the Eighth Circuit held that funds obtained through wire transfer directly from a defrauded bank were covered under the NSPA's "stolen, converted or taken by fraud" language. The defendant in *Kroh* used fraudulent financial statements to obtain loans from three banks. He had the banks directly deposit the loan funds electronically to his bank in another state.[60] The court rejected the defendant's argument that the NSPA did not apply because he never had physical possession of the money before it was trans-

---

[54] 579 F2d 1332, 1337 (5th Cir 1978).

[55] Id at 1335-36.

[56] Id at 1335-37.

[57] Id at 1337.

[58] 820 F2d 969, 971 (8th Cir 1987).

[59] 896 F2d 1524, 1529, rehearing granted, vacated on other grounds, 904 F2d 450 (1990).

[60] Id at 1526-28.

ferred across state lines. The court found that while there was no physical taking of the funds, the means used to obtain the goods were irrelevant.[61] The court cited a passage in an earlier case, *United States v Gilboe*, which also involved an electronic wiring of funds: "'we suspect that actual dollars rarely move between banks. . . . If anything, the means of transfer here were essential to the success of the fraudulent scheme.'"[62] In response to the defendant's argument that *Dowling* precluded such a conclusion, the *Kroh* court explained:

> The statement [in *Dowling*] on which Kroh relies ("the provision seems clearly to contemplate . . . some prior physical taking of the subject goods") is not indicative of a requirement that literal possession occur prior to the act of transportation. Rather, it suggests only that copyright infringement does not result in the property deprivation that section 2314 is intended to punish."[63]

To read *Dowling* to apply only where the defendant had possessed physical goods would be to open a loophole in the NSPA for theft via electronic transfer. Because the Court has never granted certiorari to any of the longstanding series of cases reaching the same result,[64] the Eighth Circuit's conclusion in *Kroh* that the case should be read as a case about copyrights is reasonable.

In order for a court to avoid overruling the wire transfer cases, it would have to distinguish computer files. Why computer files should be singled out is something the *Brown* court did not answer. Computer files store information traditionally stored in other media. Money is transferred between banks through the use of bookkeeping entries without ever moving a physical equivalent in cash.[65] To treat theft of computer files without taking of physical goods differently than theft of money via wire transfer would be anomalous.

---

[61] Id at 1529; see also *United States v Goldberg*, 830 F2d 459 (3d Cir 1987); *United States v Wright*, 791 F2d 133 (10th Cir 1986); *United States v Gilboe*, 684 F2d 235 (2d Cir 1982).

[62] *Kroh*, 896 F2d at 1529, citing *Gilboe*, 684 F2d at 238.

[63] *Kroh*, 896 F2d at 1529, citing *Dowling*, 473 US at 217-18.

[64] See, for example, *United States v Gilboe*, 684 F2d 235 (2d Cir 1982), *cert denied*, 459 US 1201 (1983).

[65] Jonathan R. Macey and Geoffrey P. Miller, *Banking Law and Regulation* 53-54 (Little, Brown, 1992) ("EFT avoids the inefficiencies and delay associated with the physical transport of checks.").

2. Medium Versus Message.

The *Brown* conclusion also has the odd result of punishing theft via a particular medium regardless of the message. For example, assume Thief 1 uses his own diskette to steal a computer file worth $10,001, and Thief 2 steals a diskette worth $1 containing a file worth $10,000. Under the *Brown* reading of *Dowling*, Thief 2 may be prosecuted under the NSPA for theft of $10,001 worth of property, while Thief 1 may not be prosecuted under the NSPA at all.[66] Yet all other things equal, the conduct of the first thief results in the same social loss.

Once a component of the property, no matter how small, meets the tangibility requirement, the remaining components, no matter how intangible, are considered property under the NSPA. Even where almost the entire value of the item transported is attributable to its intangible component, the item is considered property under the Act, and taking the item renders it stolen as defined by the Act. In *United States v Bottone*,[67] the Second Circuit relied upon trade secret law in confirming a conviction for interstate transportation of stolen property where the defendants transported across state lines copies of a manufacturing process for bacterial cultures along with actual bacterial cultures. The court found sufficient physical connection between goods stolen and goods transported because of the carrying of the actual bacterial cultures across state lines, but rejected the need for such an analysis.[68] A broad reading of *Bottone* suggests that transporting between states a copy of the information explaining the process alone (without transporting any stolen physical object) satisfies the NSPA's property requirement. To what extent the broad reading of the case is good law after *Dowling* is unclear. But the *Dowling* opinion cited with approval *United States v Greenwald*,[69] which held that a piece of paper containing chemical formulae can be considered "goods, wares, [or] merchandise" under the Act, even though the paper itself was almost worthless without the formulae.[70]

Perhaps the court was trying to draw a line between the case

---

[66] I borrow this example from one given to me by Professor David Friedman. Friedman's example uses $20,000 for the value to Thief 1. I use different values to illustrate the lack of any economic difference between the cases.

[67] *United States v Bottone*, 365 F2d 389, 393 (2d Cir 1966).

[68] Id at 393-94.

[69] *Greenwald*, 479 F2d at 322.

[70] *Dowling*, 473 US at 216.

where the piece of paper itself (probably worth a few pennies) was stolen and where the piece of paper was not stolen. But, as the Eighth Circuit, in its post-*Dowling Kroh* opinion reasoned, "[t]he aim of the statute is to punish the act of fraud; the method by which the perpetrator transports the fruits of the fraud in interstate commerce is irrelevant."[71] That the method of transportation has no important consequences suggests that *Dowling* should be read as a case about copyright law, and not as a case importing a tangibility requirement into the NSPA.

III. READING THE NSPA TO COVER COMPUTER FILES

That computer files lack common law intellectual property protection is no surprise. We are only beginning to see the large-scale use of computers, and the computer itself is a relatively recent technology. To expect the common law to have adapted to this new technology is roughly equivalent chronologically to expecting the common law to have adapted to the use of outer space.

On the other hand, waiting for law, either state or federal, to fill the gap is problematic. A uniform state common law defining the status of computer files does not exist and probably will not exist for some time.[72] Computer crimes can be, and often are, easily accomplished across jurisdictional boundaries. State law enforcement authorities lack the expertise and resources to address multijurisdictional computer crimes. Nothing fills this gap. Private companies tend not to expend resources to seek out computer criminals, and federal computer crime legislation tends to be very specialized, narrowly addressing particular offenses.[73]

The NSPA offers the courts an alternative. The statute is designed to counter types of theft that prosper as a result of enforcement problems created by state boundaries. By recognizing the application of "goods, wares [or] merchandise" to computer information, federal courts can provide a model for the development of state law in the area, largely overcoming the inevitable problem of the development of fifty separate bodies of law. Furthermore, development of a body of law focused on com-

---

[71] *Kroh*, 896 F2d at 1529.

[72] Meanwhile, state legislators have enacted a variety of laws designed to prevent computer crime. These laws vary greatly from state to state. See Seth E. Lipner and Stephen Kalman, *Computer Law: Cases and Materials* 539-44 (Merrill Publishing, 1989).

[73] For an argument that special legislation is not necessarily the proper response to computer crime, see Colin Tapper, *"Computer Crime": Scotch Mist?* 1987 Crim L Rev 5.

puter files provides an analogue for future technologies. Moreover, federal recognition that computer files are a form of "property" may have positive effects in other now-emerging areas of the law. For example, if a computer file is "property," Fourth Amendment protections more easily apply. This Section develops these arguments.

A. "Property" Under the NSPA

Courts look to law outside the NSPA to define what is property within the meaning of the Act. Generally, there are only a few ways information can qualify as property under the NSPA.[74] *Dowling* appears to foreclose copyright and patent law as avenues to status as statutory property, at least where the only "theft" is infringement as defined by the copyright and patent statutes. Generally, the most likely route to defining computer files as property is through trade secret law.[75] Trade secret law is a creature of state law.[76]

Unfortunately, trade secret law is a patchwork of uncertain case law developed in a variety of jurisdictions. The state law of trade secrets, although made more uniform by the Restatement of Torts' and Uniform Trade Secrets Act's informal codifications of the area of law, is inconsistent and complex.[77] Trade secret law became increasingly unpredictable in the 1980s and 1990s as a result of rapid technological advancement.[78]

In general, to acquire trade secret protection a party must show that the information is eligible for protection, is secret, and

---

[74] Mike Godwin, *Some "Property" Problems in Computer Crime Prosecution*, Cardozo Law Forum 24 (Aug 24, 1992).

[75] For a long time there was doubt whether a person had a "property" interest in information protected as a trade secret. See Arthur H. Seidel and Ronald L. Panitch, *What the General Practitioner Should Know about Trade Secrets and Employment Agreements* 12-13 (ALI, 1979), citing *E.I. du Pont de Nemours & Co. v Masland*, 244 US 100 (1917). However, the Supreme Court recently held trade secrets to be property rights protectable under the Constitution. *Ruckelshaus v Monsanto Co.*, 467 US 986, 1004 n 9 (1984); see also Donald S. Chisum and Michael A. Jacobs, *Understanding Intellectual Property Law* § 3A at 3-4 (Matthew Bender, 1992).

[76] Godwin, Cardozo Law Forum at 24 (cited in note 74). This Comment does not address the more specialized case of breach of a confidential relationship.

[77] Chisum and Jacobs, *Intellectual Property* § 3A at 3-5 (cited in note 75). The Second Restatement of Torts (1979) does not address the issue of trade secrets because, according to the editors, trade secret law has developed sufficiently as a separate body of law. However, tort principles still govern this body of law. See *Amoco Production Co. v Lindley*, 609 P2d 733, 743 n 4 (Okla 1980); Lipner and Kalman, *Computer Law* 208 (cited in note 72).

[78] Chisum and Jacobs, *Intellectual Property* § 3A at 3-5 (cited in note 75).

has commercial value.[79] As for eligible information, just about any "concrete" information can qualify.[80] In cases of pure industrial espionage or outright theft, the misconduct may engender sanctions regardless of whether the information technically qualifies as eligible, secret, and having commercial value.[81]

Although trade secret law is a body of law developed by states, there are federal cases which have relied upon trade secret law to establish the property element of a federal crime.[82] For example, in *United States v Bottone*,[83] trade secret law formed the basis of a conviction under the NSPA for transporting copies of information about the manufacturing process for bacterial cultures, as well as samples of the cultures themselves, across state lines. *Bottone* is authority for the proposition that stolen trade secrets can constitute the intangible portion of property as defined in the NSPA, whether or not there must also be stolen physical property accompanying the intangible "property."[84]

The use of trade secret law to establish the property element of a NSPA conviction is important for three reasons. First, trade secret law has always been especially adaptive to new technologies. Trade secret law has evolved from its early nineteenth century ancestry significantly, if not primarily, in response to new technologies.[85] Thus it seems particularly well-suited as a foundation upon which to build a law of computer file property protection.

Second, trade secret law adapts functionally, rather than analogically—that is, it "reflects policy judgments about how to encourage innovation, competition, and consumer welfare and ethical notions about proper business behavior."[86] A court would

---

[79] Id § 3C at 3-14.

[80] See id § 3C at 3-15 through 3-19 for a more thorough description of property eligible for protection. A traditional requirement is that the information be more "concrete" than an idea, theory, possibility or emotion, and relatively specific in its intended implementation. Many courts no longer focus on concreteness.

[81] Id § 3A at 3-5. See, for example, *Continental Data Systems, Inc. v Exxon Corp.*, 638 F Supp 432, 441-43 (E D Pa 1986).

[82] Godwin, Cardozo Law Forum at 24 (cited in note 74).

[83] 365 F2d 389 (2d Cir 1966). See the discussion of this case in text accompanying notes 67-68.

[84] Whether *Dowling* overrules *Bottone* to the extent that *Dowling* may not have allowed a conviction under the NSPA for transporting copies of the information alone is unclear, but it does not affect this analysis.

[85] Chisum and Jacobs, *Intellectual Property* § 3A at 3-3 through 3-5 (cited in note 75).

[86] Id § 3A at 3-4.

not be steering a new course if it were to adapt trade secret principles to the world of computers using policy judgments as measuring sticks.

Third, courts should base the definition of property in the NSPA on trade secret law because courts need more flexibility in defining property than restrictive definitions provide. The Supreme Court rejected an argument that the word "stolen" in the NSPA's predecessor was confined to any common law meaning.[87] More recently, in *United States v Darrell*, the Tenth Circuit rejected an argument that to meet the definition of "stolen," the criminal act involved had to fall under the state statute's definition of "larceny," holding that the NSPA contemplated a broader definition.[88] These decisions make clear that, at least when interpreting the word "stolen," courts will not confine themselves to specific state laws and precedents.[89] The flexibility of trade secret law provides breathing room for a court trying to give life to a new form of property.

To summarize, the NSPA offers a convenient opportunity to establish a common law foundation for defining property rights in computer files so as to protect them against outright theft. Courts have historically adapted trade secret law to new technologies, they have done so functionally and not merely by analogy, and the NSPA affords a court breathing room when construing the statutory definition of property. Section 2314 could easily be read to cover theft of computer files given this framework.

B. The NSPA and Computer Files

Reading the NSPA to protect computer files as trade secrets is a particularly good idea for two reasons. First, the purpose of the NSPA was to provide a federal venue for crimes which took advantage of state boundaries to hinder effective law enforcement. Computer crimes increasingly fit this description, and computer criminals generally ignore the existence of state boundaries. Second, the extent to which a common law develops defin-

---

[87] *United States v Turley*, 352 US 407, 417 (1956).

[88] 828 F2d 644, 649 (10th Cir 1987).

[89] Presumably, the statutory language has even more leeway than recognized in these cases. The *Turley* Court stressed that "stolen" had no common law meaning, leaving room to consider the statute's purpose in defining the word. 352 US at 411-13. Similarly, the current version of the Act uses the phrase "goods, wares [or] merchandise" and does not include a single term such as "property" with an established common law meaning.

ing computer file information as property will have a significant impact on the extent to which courts recognize civil liberties in the future. This is especially important because personal information is increasingly found in computer files. A government victory in extending the NSPA to cover computer files as property could prove to be one of the most significant civil liberties victories for the coming century.

1. A Federal Solution for National Crimes.

Congress has not yet addressed the issue of computer file theft, and understandably so. When Congress enacted the original National Motor Vehicle Theft Act ("NMVTA")—the precursor to the NSPA—the design for the personal computer was not even on anyone's drawing board.[90] The NSPA existed before computer files appeared, and the new technology was simply dropped into the lap of existing law. Computer technology is evolving quickly enough that a statute crafted today and passed perhaps two years from now might be obsolete upon birth.

The *Dowling* Court placed a great deal of emphasis on the purpose of the NSPA when evaluating its applicability to copyright infringement. The purpose of the NSPA is a good starting point for evaluating its application to computer files in the absence of language clearly resolving the issue.

Section 2314 came about as an extension of the NMVTA.[91] As the Court explained in *United States v Turley*, the

> advent of the automobile [] created a new problem with which the States found it difficult to deal. The automobile was uniquely suited to felonious taking whether by larceny, embezzlement or false pretenses. It was a valuable, saleable article which itself supplied the means for speedy escape.[92]

The automobile created new problems for which state laws were inadequate. The *Turley* Court recognized that the automobile was "'the perfect chattel for modern large scale theft.' The challenge the automobile presented could best be met through use of the Federal Government's jurisdiction over interstate commerce."[93]

---

[90] National Motor Vehicle Theft Act, Pub L No 102-483, 41 Stat 324, currently codified at 18 USC § 2312 et seq (1990).

[91] Id.

[92] *United States v Turley*, 352 US 407, 413 (1957).

[93] *Turley*, 352 US at 413, citing Hall, *Theft, Law and Society*, 235 (2d ed 1952), and 58 Cong Rec 5470-78 (1919).

Congress expanded the NMVTA to the NSPA in order to extend the protections of federal law to "roving criminals" who used state boundaries to shield themselves from the jurisdictional inadequacies of state law. As then Attorney General Cummings put it, "[t]hese criminals have made full use of the improved methods of transportation and *communication.*"[94] Currently, the NSPA applies to all stolen property transported across state lines with a value of $5,000 or more.

Society is becoming increasingly dependent on the use of computers to store information previously stored in libraries and filing cabinets.[95] Huge sums of money are transferred over networks, four of which carry the equivalent of the federal budget every two to four hours.[96]

Is there a risk of crime given this emerging architecture? Judging from highly-publicized computer crime enforcement efforts, the computer crime problem might not seem very serious.[97] For example, Operation Sundevil, a federal crackdown on computer abuses in the Summer of 1990, has resulted in only one conviction.[98] The perception of the seriousness of computer crime that does exist is likely the result of a media portrayal of computer crimes which in many cases tends to overstate the seriousness of certain kinds of problems.[99] Indeed, much of what is considered to be dangerous hacking is probably just harmless pranksterism.[100]

But computer crime is becoming a serious problem. The American Bar Association Task Force on Computer Crime conducted a study in 1984 on the impact of computer crime and concluded that annual losses from computer crime range between $145 and $730 million.[101] Typical computer crimes include

---

[94] 78 Cong Rec 2947 (1934) (statement of Attorney General Cummings) (emphasis added). See *Dowling*, 473 US at 220.

[95] See notes 119-26 and accompanying text.

[96] Anne W. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 Rutgers Computer & Tech L J 1, 2 n 4 (1990).

[97] See Lance Rose and Jonathan Wallace, *Syslaw* 105-07 (P.C. Information Group, 1992). Rose and Wallace describe how the major computer prosecutions of the day have involved criminal acts which have resulted in relatively minor harm.

[98] Id.

[99] The movie "Die Hard II," for instance, portrayed a group of criminals who gained control of an airport's computers from a remote location and caused a commercial airplane to crash.

[100] Rose and Wallace, *Syslaw* at 106-07 (cited in note 97).

[101] ABA, Criminal Justice Section, Task Force on Computer Crime, *Report on Computer Crime* 38 (1984); Note, *Computer Fraud and Abuse Act of 1986: A Measured Response*

breaking into computer systems, stealing data, altering or destroying medical or financial data, spreading viruses,[102] gaining unauthorized access to and misusing personal credit and other personal and business information,[103] and similar ventures.[104] The increasing reliance on computers to store information ensures that the problem should grow significantly in the next decade.[105]

The computer crime problem is national in scope. Unauthorized access to computers often occurs from a remote computer over the telephone lines.[106] Stolen telephone access codes, use of call-forwarding through reprogramming switching stations, and use of phantom phone billing rip-off strategies have rendered long-distance charges an ineffective barrier to out-of-state and out-of-country theft.[107] Hackers with criminal inclinations have dealt a number of serious blows. Stories of hackers ignoring state boundaries involve everything from invading computers at NASA to stealing the credit information of everyone in a small town in Oregon.[108] All of this makes damaging industrial espionage possible.[109]

The lack of federal criminal prosecutions for computer crime does not mean that the problem is not serious. Prosecuting com-

---

to a Growing Problem, 43 Vand L Rev 453, 454 (1990).

[102] The most famous virus to date was a "worm" launched onto the Internet by Robert Morris, a Cornell graduate student. The worm crashed about 6,000 Internet computers. Sterling, *Hacker Crackdown* at 88-89 (cited in note 22).

[103] One company distributes a catalog boasting that it will sell confidential government computer information about anyone. Rob Johnson and Bill Husted, *We Point Out Weaknesses*, The Atlanta Journal and Constitution A1 (May 24, 1992).

[104] Rose and Lance, *Syslaw* at 108 (cited in note 97).

[105] Note, 43 Vand L Rev at 454-55 (cited in note 101).

[106] Computer Fraud Legislation, Hearing Before the Subcommittee on Criminal Law of the Senate Committee on the Judiciary, 99th Cong, 1st Sess 41-44 (1985) (statement of William G. Petty).

[107] Sterling, *Hacker Crackdown* at 49-52 (cited in note 22).

[108] See Richard Behar, *Surfing off the Edge*, Time 62 (Feb 8, 1993). One prank involved redirecting prison pay phone calls across state lines to a phone sex number. On June 13, 1989, anyone at the Palm Beach County Probation Department in Delray Beach, Florida, who called a certain probation officer found his call rerouted to a phone sex worker named "Tina" in New York. The switch was accomplished by a hacker who reprogrammed the software in a switching station. Sterling, *Hacker Crackdown* at 98-99 (cited in note 22). Other instances of crossing over state lines include gaining unauthorized access to White House and Pentagon computers. Mark Goodman, *Hacker for Hire*, People 151 (Oct 19, 1992).

[109] Goodman, People at 151 (cited in note 108). Goodman recounts tales of Ian Murphy, a formerly mischievous hacker who now heads a consulting company which spies on the hiring company to ensure competitors are not doing the same.

puter crime is extremely difficult. Injured companies rarely pursue criminals, often because the offending party is usually financially judgment-proof.[110] Moreover, the enforced fragmentation of the phone company has made tracking and prosecution of phone criminals next to impossible.[111]

Generally, state prosecutors fare no better. Where the case involves complicated issues which require a certain level of sophistication even to understand, requires research into tricky multijurisdictional questions, or demands that one jurisdiction devote resources to prosecute for crimes which affect other jurisdictions, law enforcement officers simply turn to the greener pastures of well-established law.[112] One of the main problems with locating and prosecuting serious computer criminals is the lack of a centralized body with the resources and expertise necessary to confront what is an extremely complex type of crime.[113] Local law enforcement officers lack the expertise and resources to prosecute crimes of this nature.[114] Making matters worse, this area of law is not only fragmented at the state level,[115] but also uncertain,[116] which makes multijurisdictional prosecutions extremely difficult.[117] Creative forms of computer theft abound; fragmentation makes law enforcement in this area nearly impossible.

Given the complex nature of computer crime, and the difficulties prosecuting multijurisdictional computer crimes with limited local resources and expertise, jurisdictional centralization is necessary. Hence, extending the NSPA to cover theft via computer is entirely consistent with the purpose of the NSPA.

---

[110] See Sterling, *Hacker Crackdown* at 62 (cited in note 22) noting that "[h]ackers are generally teenagers and college kids not engaged in earning a living."

[111] Id at 183-84.

[112] William Petty argues that these problems argue in favor of uniform federal preemptive legislation. *Computer Fraud Legislation Hearings* at 41-43 (cited in note 106).

[113] Id at 41-44.

[114] Id.

[115] Different states have passed different laws to address computer crime. These laws are far from uniform. Lipner and Kalman, *Computer Law* at 539-44 (cited in note 72); Douglas Reimer, American Bar Association, Tort and Insurance Practice Section, *The Low Side of High Tech* (1985). For example, very few states, with the exception of New York, have a statute prohibiting unauthorized copying of computer files or software. Branscomb, 16 Rutgers Computer & Tech J at 1 & 1 n 175 (cited in note 96); see also N Y Penal Law § 156.30 (McKinney 1988).

[116] Ed Krol, *The Whole Internet User's Guide and Catalog* 34 (O'Reilly & Associates, 1992).

[117] *Computer Fraud Legislation Hearings* at 41-44 (statement of Petty) (cited in note 106).

2. Broader Implications.

Even if enforcing the law were not a compelling reason for extending coverage of the NSPA,[118] the advantages of recognizing property rights against theft of computer files go beyond hindering serious industrial espionage. In fact, no one seriously claims that the NSPA could ever serve as a panacea for all computer crime. But affirmative recognition of computer information as property under the NSPA would be a good step in this uncertain area of law. What is at stake is not a new tool in the prosecutorial tool belt, but is far more fundamental: how we treat computer information in an era where pen and paper are all but obsolete.

a) *Preserving existing property rights.* The increasing obsolescence of paper is no secret. Society is becoming increasingly dependent on computers to store information.[119] More and more companies now store information about customers in computer databases.[120] Information is traded like any other good in the marketplace.[121] The most personal medical data may soon be accessible with the use of what resembles an automatic teller machine card.[122] Private

---

[118] One might argue that the injured companies, rather than society, should bear the cost of industrial espionage. This is a plausible argument, especially since countermeasures against minor intrusions into computer systems are relatively inexpensive (complicated passwords, levels of security access, data encryption, and even unplugging the modem are all fairly inexpensive means of preventing some forms of unauthorized access). However, relying on the injured company to bear the cost assumes that computer crime imposes no external costs on society at large. The AT&T phone system crash of January 15, 1990 proves otherwise. See Sterling, *Hacker Crackdown* at 1-2 (cited in note 22). Mistakes made when searching for files may accidentally crash a system. Serious injury to companies imposes costs on those who depend on the company. However, it is not clear to what extent private enforcement would be adequate.

[119] Note, *Addressing the New Hazards of the High Technology Workplace*, 104 Harv L Rev 1898, 1898-99 (1991); Office of Technology Assessment, *Critical Connections: Communication for the Future* 275-80 (1990); Note, 43 Vand L Rev at 453-55 (cited in note 101).

[120] Many companies now use a "caller-ID" service provided by the phone companies to link information about the calling consumer with the caller's telephone number. Companies such as Quaker Oats and Citibank have compiled databases with detailed information on millions of households. See Anne W. Branscomb, *Common Law for the Electronic Frontier: Computers, Networks and Public Policy* Scientific American 154 (Sep 1991).

[121] Anne Branscomb argues that the market for information alone through on-line databases represents about four billion dollars in trade each year. Branscomb, 16 Rutgers Computer & Tech L J at 2 n 3 (cited in note 96).

[122] An AT&T television commercial advertises that just such a system will be available in the near future.

information is available to anyone who can gain access to the now vast computer files which keep records on nearly everyone.[123] Add to this the fact that personal computers are becoming commonplace in the household. Even the government is entering the picture: several recent bills introduced in the House of Representatives would require the government to post information on federal bulletin boards.[124] Legal databases available to anyone with a computer and a modem carry everything from federal case law to obscure agency decisions.[125] Even general information available in libraries is now available with a modem.[126] To the extent that property protection currently available to data stored on paper is not extended to the same information stored on a computer, society has abandoned formerly available property rights merely because the information has been stored in a new container.

b) *Corresponding privacy interests.* The computer revolution extends far beyond data storage and retrieval. Electronic mail ("e-mail") has increased in popularity. People now communicate over the computer, setting up "rooms" in which they converse privately or publicly. Whole communities have been established over the phone lines using computers. Many of the people in these communities, who write to each other using e-mail and talk to each other using what resembles an electronic CB radio, have never met each other face-to-face. People even play games, such as chess or modern forms of Dungeons and Dragons, over the computer. Players know one another through

---

[123] See John Schwartz, *Big Guns for Small Targets*, Newsweek 63 (Nov 16, 1992). One author recounts a tale of using a large commercial network to acquire the phone number of Bob Dylan's ex-wife and information brokers to acquire Dan Rather's American Express bills. Jeffrey Rothfeder, *Privacy for Sale* 29, 65-69 (Simon & Schuster, 1992).

[124] See *Information Access by, of and for the People*, CompuServe Magazine 7 (April 1993). Bills include the Improvement of Information Access Act (HR 3459), introduced by US Rep Major Owens on Oct 1, 1991 (which would mandate that federal agencies make better use of computer networks in releasing information), and a similar bill (HR 2772), introduced by Rep. Charlie Rose, which would provide a Wide Information Network for Data Online run by the GPO. Information available would likely include the SEC's EDGAR system for corporate disclosure filings, the House of Representatives LEGIS system and the DOJ's JURIS system. *Information Access*, CompuServe Magazine at 7 (April 1993).

[125] Mead Data Central, which maintains a database known as "LEXIS," and West Publishing Company, which maintains a database known as "Westlaw," now provide dial-up databases which are all but essential to the practicing lawyer.

[126] *Information Access*, CompuServe Magazine at 7 (cited in note 124).

this interaction, and they have formed complex communities.[127]

The location of these "communities" is even more complex. They exist in the electronic memories of a computer or several computers linked by a network such as "the net" (the Internet).[128] In the very near future, when high speed phone lines become commonplace,[129] a person will be able to put on his head a virtual reality helmet which is plugged into his computer and, using his computer, communicate with people around the country while a computer simulates a room and generates images of the other participants.[130] The same technology will allow an employee to work at home, perhaps in another state. The employee will be hooked into the company network; he will interact with others using such a helmet in the virtual reality of the company's lavish computer-simulated offices, when in actuality the "company" is a computer program generated by a mainframe computer somewhere.[131] In essence, this new "area" in

---

[127] Sterling, *Hacker Crackdown* at xi-xiv (cited in note 22).

[128] The Internet is actually "a globe-spanning system of perhaps 50,000 computers, mainframes, minicomputers and workstations for the most part, all linked by ultra-high-speed telephone lines but accessible as well by ordinary computer users via slow-speed modems." James Coates, *The network of networks beckons to determined on-line explorers*, Chicago Tribune Sec 7 p 4 (Apr 4, 1993). It was established by the Pentagon 20 years ago and eventually assumed in part by the National Science Foundation ("NSFNET"). The connected computers are mainly run by universities, military installations, and major businesses. However, many popular services such as CompuServe, America Online and Prodigy provide limited access to the "net" through the use of electronic mail. Id. An ordinary user instructs his personal computer to "dial up" the service or network computer by using a modem, and the user then interacts with programs run by the network computer he calls. For more thorough description, see John S. Quarterman, *The Matrix* (Digital Press, 1992); Ed Krol, *The Whole Internet* (cited in note 116).

[129] The current network of phone lines, which still includes copper wiring, is incapable of carrying high-speed data transmissions to ordinary households. Most modems communicate at a rate of about one to two pages of data every second. The line interference from the old wiring prevents higher speeds. Fiber optic cables, cables made of thin strands of glass so pure that you could see through a 70-mile-thick window of it, allow for much faster transmission rates. The new cable can carry the contents of the entire *Encyclopedia Britannica* every second. Telephone companies are currently working to replace the copper wire with fiber optic cables. See Philip Elmer-Dewitt, *Take a Trip into the Future on the Electronic Superhighway*, Time 50, 53 (Apr 12, 1993).

[130] Virtual reality video games using such helmets already exist in the same video arcades that once boasted of games such as Pac Man. See Don Clark and Ken Siegmann, *Virtual Reality Coming to Arcades and Theme Parks*, San Fran Chronicle C3 (Mar 16, 1993). The only obstacles to virtual reality phone conversations are time, money, and the lack of high-speed phone lines, all of which are rapidly disappearing. See note 129 and accompanying text.

[131] See *A Day in the Cyber Life, 2000 A.D.*, CompuServe Magazine 14 (Dec 1992), and a response to the article, Nina Adams, *Commuting in 2000*, CompuServe Magazine 4 (Mar 1993).

which we store information, through which we are beginning to interact, and on which we now increasingly depend is a new frontier.

William Gibson coined the term "cyberspace" for this new frontier.[132] Cyberspace presents a host of new legal problems; until the late 1980s and early 1990s issues of property and privacy in cyberspace had not made a significant appearance in legal culture.[133] And yet this new frontier is the battleground for civil liberties as we will understand them in the next century. As more and more of our lives require interaction with computers—communicating through computers over the phone lines, using networks to store electronic mail, submitting to mammoth databases which contain extremely personal information—these issues will force themselves upon us.

Seen in this light, the issue of whether computer files are property is pressing. The alternative to such a recognition is problematic. If computer files are not considered property, they are subject to attack. One potential attacker is the computer hacker turned criminal.[134] The possibility of an attack on networked computer systems is well known, and "pranks" have had somewhat serious consequences.[135] These seemingly harmless excursions give hackers a bad name. Worse yet, they make the general public timid of computers and computer networks. A great deal of the Internet is publicly-funded. Sexually explicit materials uploaded to a public node once jeopardized the funding of the entire NSFNET.[136]

If computer files are not considered property, the information stored in them becomes unprotected, and the rights which usually attach to property are absent. All of the information people store on network computers, from e-mail messages to term papers, is in control of someone other than the people who put it there. When the government searches through someone's private e-mail on a computer network, is it conducting a "search" as

---

[132] See William Gibson, *Neuromancer* (Ace Books, 1984). Gibson is generally credited with coining the term.

[133] Sterling, *Hacker Crackdown* at 57-58 (cited in note 22).

[134] I use the term "hacker" pejoratively as an unfortunate convenience. Very few "hackers" are actually troublemakers. The vast majority are bright, socially productive and creative individuals. Id at 55, 77.

[135] See notes 97 through 109 and accompanying text above.

[136] Krol, *The Whole Internet* 35 (cited in note 116). The NSFNET is a significant portion of the Internet system and is run by the National Science Foundation. See note 128.

defined under the Fourth Amendment?[137] What if the government reprograms the software which creates one of the predicted virtual reality "rooms" so as to create an invisible observer to a conversation?[138] What if a company reads its computer-users' e-mail or private files? These questions are still unanswered.

To the extent that computer storage precludes otherwise available property protections, computer storage of information may defeat privacy protections.[139] If the data and files used in e-mail or in creating a virtual reality "room" are considered the property of the users, protection of privacy is more likely.[140]

Trade secret law can only be a springboard for recognizing a

---

[137] A recent decision awarded damages to plaintiffs against the U.S. Secret Service for literally seizing the computers of a bulletin board run by Steve Jackson Games called the Illuminati Bulletin Board. *Steve Jackson Games Inc. v United States Secret Service*, 816 F Supp 432, 440 (W D Tex 1993). The Secret Service read and deleted some of the e-mail stored on the computer. Although the court found for the plaintiffs, its holding was based on the Stored Wire and Electronic Communications and Transactional Records Access Act, 18 USC §§ 2701, et seq, which allows the government "disclosure" when "there is reason to believe the contents of a[n] . . . electronic communication are relevant to a legitimate law enforcement inquiry." 18 USC §§ 2703 & 2703(d). The court's finding for the plaintiffs was more the result of a bungled Secret Service operation than a recognition of property right in stored electronic communications. The court held that the Secret Service should have asked a magistrate first; that appears to have been its mistake. 816 F Supp at 443. The "relevant" and "legitimate" language may offer a relatively low standard of protection for these forms of communication.

[138] Such an action would probably be covered under a 1986 amendment to the Electronic Communications Privacy Act. See S Rep No 541, 99th Cong, 2d Sess 13 (1986) ("Section 101(a)(3) of the Electronic Communications Privacy Act amends the definition of the term 'intercept' in current section 2510(4) of title 18 to cover electronic communications. The definition of 'intercept' under current law is retained with respect to wire and oral communications except that the term 'or other' is inserted after 'aural.' This amendment clarifies that it is illegal to intercept the non-voice portion of a wire communication."); see also *Steve Jackson Games*, 816 F Supp at 441 (citing legislative history). However, the *Steve Jackson Games* court concluded that the obstacles to the government's search and seizure were purely statutory. Congress might easily change its mind and even require operators of bulletin boards to disclose communications to the government. It enacted a similar although misnamed law, the Bank Secrecy Act, which requires a bank to retain and disclose information about its customers and their transactions to the government. The statute was upheld against a Fourth Amendment challenge in *United States v Miller*, 425 US 435, 443 (1976). Notably, the government does not even conduct a "search" under the Fourth Amendment when it installs a pen register at the phone company that records what number a person dials. *Smith v Maryland*, 442 US 735, 745-46 (1979).

[139] See *Miller*, 425 US 435, 443 (no protected privacy interest in bank records); *Smith*, 442 US 735, 745-46 (no privacy interest in telephone number dialed); *Steve Jackson Games*, 816 F Supp at 443 (privacy interest in e-mail only statutory).

[140] The Supreme Court recently reaffirmed property interests as protected along with privacy interests in *Soldal v Cook County, Illinois*, 113 S Ct 538, 544 (1992). The Court observed that interests in property and privacy are tied in Fourth Amendment analysis. Id.

broader notion of property and privacy rights in an electronic era. At a minimum, it would shape societal expectations of interests in computer information. Conversely, refusing to extend property protection for trade secrets to computer files, relying exclusively on statutory protections, may correspondingly serve as a framework for refusing to extend privacy protection to the new frontier.[141]

One way to ensure privacy and a form of property interest in computer files is by contract.[142] Indeed, the advantages of contract are clear in the context of bulletin boards. A system operator may ask users to follow certain standards relating to privacy and courtesy; if the user does not like the standards the user may go somewhere else or start her own bulletin board.[143]

The possibility of protection through contract does not mean that we should fail to recognize property rights in computer information. Under trade secret law, or an expansion based upon that foundation which recognizes broader rights in computer files, a person could easily modify her rights, adding to or taking away from what the law provides as a baseline.[144] Additionally, relying upon contracts between the user and the company providing e-mail to the user instead of relying upon a broad understanding of property rights, provides less protection of Fourth Amendment rights, which are based on societal expectations of what is reasonable, not individual expectations.[145]

The limits put on Fourth Amendment rights by a contract scheme would have an effect on willingness to contract for a recognition of privacy. Lance Rose argues that the diversity of state privacy laws ensure that it is easier for a system operator,

---

[141] See *Soldal*, 113 S Ct at 544-45 (privacy protection only extends as far as society considers to be reasonable). The FBI is proposing legislation that would force computerized telephone and communication system companies and manufacturers to design into their systems the capability to eavesdrop on digital communications. The Bureau claims that the switch to digital communications will make wiretapping more difficult. However, the extensive wiretapping machinery would make wiretapping much easier than it is today. See John Eckhouse, *FBI Talks About Tapping Computers*, San Fran Chronicle D1 (Mar 12, 1993); Tim Weiner, *Hard Times for the FBI's Wiretapping*, Phil Inquirer A4 (Feb 7, 1993); *FBI's Digital Wiretap Bill Assailed in GSA Internal Documents*, Common Carrier Week (Jan 25, 1993).

[142] Rose and Wallace, *Syslaw* at 25-40 (cited in note 97).

[143] I borrow this idea from Professor David Friedman.

[144] David Bender, *Protecting Computer Trade Secrets*, Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, 224 PLI/Pat 713 (May 1, 1986) (Westlaw).

[145] See *Soldal*, 113 S Ct at 544-45. As an example, a person cannot contract into an expectation that the government will not search his person or effects without a warrant.

who may have his system seized if someone stores an illegal file on it, to monitor e-mail to ensure that it contains nothing bad. Even if the system operator could contract for privacy, given the diversity of state privacy laws in this area he will find it easier to simply refuse to promise any privacy for e-mail whatsoever.[146] A federal baseline recognizing privacy rights in computer information would provide more comfort for system operators.[147]

Thus, computer information faces a two-flanked attack. On one flank stands the hacker turned criminal; on the other stands the government and companies who provide e-mail services without respecting user privacy or property interests in the data. Each threatens the interests and privacy we expect in information stored on a computer. The importance of protecting information against both flanks is summarized in an anecdote Bruce Sterling recently reported: an AT&T employee, Charles Boykin, set up at his own expense a publicly-available computer which people could call using a modem. The system was so powerful that people began to call it "Killer". He considered the venture good advertisement for the new AT&T system. Killer eventually acquired 1500 users who communicated, uploaded and downloaded files and used the system for electronic mail.

> But by 1990, . . . AT&T Corporate Information Security was fed up with Killer. This machine offered no direct income to AT&T and was providing aid and comfort to a cloud of suspicious yokels from outside the company, some of them actively malicious toward AT&T, its property, and its corporate interests. Whatever goodwill and publicity had been won among Killer's 1,500 devoted users was considered no longer worth the security risk. On February 20, 1990, Jerry Dalton arrived in Dallas and simply unplugged the phone jacks, to the puzzled alarm of Killer's many Texan users. Killer went permanently off-line, with the loss of vast archives of pro-

---

[146] Lance Rose, *Cyberspace and the Legal Matrix: Laws or Confusion?* (available online at eff.org). This is not mere speculation. A bulletin board located in Illinois, AKCS, upon signup warns the potential user that he should expect no privacy whatsoever. The concerned system operator noted that he felt the seizures of bulletin boards in the *Riggs* case were in violation of the Constitution, but to play it safe he would monitor everything closely. Rose and Wallace advise that: "The most surefire method [to guard against system seizure due to illegal files being placed on your bulletin board] is to turn your BBS into the equivalent of a well-lit and heavily guarded prison camp. Look through every single message, private and public alike, and every file." Rose and Wallace, *Syslaw* at 125 (cited in note 97).

[147] Id.

> grams and huge quantities of electronic mail; it was never restored to service. AT&T showed no particular regard for the "property" of these 1,500 people. Whatever "property" the users had been storing on AT&T's computer simply vanished completely.[148]

As computers increasingly replace traditional media for storage of information, communication, and interaction generally, what is at stake in defining the status of a computer file is whether current notions of rights and powers travel with the data into the computer world. Whether current federal laws can adequately address new forms of computer crime if read to extend to the new forms of crime is unclear. However, preserving existing property rights in the face of a new medium for storing information which offers unique avenues to theft demands, at a minimum, the same level of property protection that applied to the former medium. Hence, the NSPA should be read to cover theft of information stored on a computer, regardless of the method by which that information was stolen.

IV. APPLIED: THE PROBLEM OF VALUATION

Once one has property rights in the information contained in a computer file, a host of new questions arise. The previous Section argued in favor of extending the NSPA to intangible information stored on a computer. This Section addresses the remaining question: assuming the NSPA applies to computer information, how should we place value on that information? The NSPA applies where property "of the value of $5,000 or more" is transported across state lines. Theft of computer files presents special problems.

Consider the following hypothetical problem. A week before the long-awaited release of GameCo's new virtual reality computer game, CyberHacker, X in Illinois, using his personal computer, dials into GameCo's network in California, uses an unauthorized password, and gains access to the source code for CyberHacker. X downloads the source code file, uses a compiler program to compile the code into a working application and plays the game.[149]

---

[148] Sterling, *Hacker Crackdown* at 125-26, 141-42 (cited in note 22).

[149] As explained above, "downloading" means instructing the computer called to send information over the phone lines to the caller. "Source code" is a text file containing a computer program readable to human beings. "Compiling" means turning the source code file into a program by translating it into binary language (the computer's language). "Application" is another word for "computer program."

Feeling particularly devious, he decides as a joke to upload the source code file to a popular bulletin board in Texas used by other hackers across the country. Upon releasing CyberHacker a week later, the company finds that its sales do not even come near their previously projected levels. In fact, GameCo sells only a few packages. It turns out that most of GameCo's potential customers are hackers who have already downloaded the source code file and compiled it on their own.[150]

Under this Comment's interpretation of *Dowling*, both X's downloading and uploading of the source code file meet the first two requirements of the NSPA: "goods, wares, [or] merchandise" were transported or transmitted across state lines and they were known to be "stolen, converted or taken by fraud." The remaining issue, then, is valuation. The NSPA only applies to a particular act of transporting property "of the value of $5,000 or more."[151] Is the property sent over the line worth $5,000?

The meaning of "value" in this context can take one of two directions. First, "value" can refer to the value of the property if it were otherwise in the hands of the victim. Second, "value" can refer to the value of the property in the hands of the thief, in other words evaluated in a "thieves' market."

The most commonly-employed method for valuation is the thieves' market formula. The Seventh Circuit applied this approach in a case of stolen eight-track recording tapes, reasoning that the profit margin from sale in the thieves' market was the most the thieves could have obtained.[152] The thieves' market approach has been applied in other cases of partially intangible and partially tangible property. The Eleventh Circuit held that in cases of partially intangible stolen property this approach is preferred.[153]

---

[150] This hypothetical set of facts is similar to an incident which occurred several years ago. An organization known as the NuPrometheus League copied and distributed a portion of Apple Computer's proprietary source code without compensation. Apparently, a distaste for Apple's litigious nature spawned the act. Although no one is sure if any harm came to Apple, the incident highlights the unique nature of computer crime. See Sterling, *Hacker Crackdown* at 232-33 (cited in note 22).

[151] Although the government can aggregate different shipments in some cases, see *United States v Berkwitt*, 619 F2d 649, 656 (7th Cir 1980), I treat these two acts separately for purpose of analysis.

[152] *Berkwitt*, 619 F2d at 657-58.

[153] *United States v Gottesman*, 724 F2d 1517, 1521 (11th Cir 1984). See also *United States v Sarro*, 742 F2d 1286, 1296 (11th Cir 1984) (thief's belief as to potential earnings is sufficient).

An analysis of whether this is the proper approach is beyond the scope of this Comment. As a general matter, where the cost of catching and punishing an offender is $0 and all offenders are caught, punishment should be set at damage done (the cost to the

It is important to realize that this applies only to a special case: where the value in the thieves' market can be determined. When such a market value cannot be determined, courts employ other methods. Generally, expert testimony,[154] the amount of time and money invested in the scheme, and the amount spent to develop the goods stolen,[155] are necessary to determine value. Notably, the Fifth Circuit has held that without a market upon which to base the value, other factors will not suffice.[156]

Computer file theft presents unique problems in this area, as the hypothetical case described above illustrates. To begin with, in the particular hypothetical I have chosen, the file stolen was not the object file, but rather the source code. While there may be a discernable market for the compiled end product, there is no such market for the source code. However, the source code may actually be more valuable to the customers than the object code. Many if not most of the recipients would be able to compile the source code themselves. Presumably, many of the recipients of the file could have altered the code for their own particular use.

---

victim). This deters all inefficient crimes. But since catching and prosecuting criminals is costly, prosecuting crimes is efficient only to the extent that the net cost from the offense occurring is greater than the cost of preventing it. The cost of preventing an offense may be negative in that with each prosecution other crimes will be deterred. As fewer offenses occur, society must spend less to catch and punish offenders. See David Friedman, *Should the Characteristics of Victims and Criminals Count? Payne v Tennessee and Two Views of Efficient Punishment* 34 BC L Rev 731, 733-37 (1993). Hence, both value to victim and value to thief will be relevant. Assume for purpose of analysis that there are no negative costs from deterrence of additional inefficient crimes, and assume further that there are no enforcement costs. If the total cost of prosecuting a criminal under the Act is $4,999, then prosecuting him makes sense only if the total social loss prevented by that prosecution is $5,000 or greater. Therefore both value to the victim and value to the thief will be relevant: a decision to commit social resources to prosecute a crime depends, at least partially, on social loss. Social loss is, in a very simple sense, value of the property stolen to the victim minus value of that property to the thief. Value to the thief tells us at what level to set the punishment in order to deter him, but it does not tell us what the social loss from the crime is (since the value to the victim may be $5,001 or $20,000). Value to the victim, likewise, does not measure social loss (since the value to the thief may be $10 or $4,900). Hence, since the jurisdictional limit appears to be concerned with preventing waste of society's resources, see *United States v Shaffer*, 266 F2d 435 (2d Cir 1959), aff'd, 362 US 511 (1960), we know at a minimum that both values will be relevant.

[154] See, for example *Greenwald*, 479 F2d at 321; *Lester*, 282 F2d at 754; *Seagraves*, 265 F2d at 880.

[155] See Michael A. Epstein, *National Stolen Property Act*, in Model Intellectual Property, ch 3, II.A. (1991); *Seagraves*, 265 F2d at 880; *United States v Drebin*, 557 F2d 1316, 1318 (9th Cir 1977).

[156] *Abbott v United States*, 239 F2d 310, 313 (5th Cir 1956) ("Mere cost of production, cost of replacement, value to the owner, . . . is not market value. For that value—market—depends on a market, whether formal or informal, in which willing buyers bargain with willing sellers.").

Also, it may have provided them with the means to clandestinely develop their own virtual reality games. Expert testimony would be needed to determine the value of the source code file.

A different problem arises in X's decision to upload the file to a bulletin board. While X only posted the file once, each time someone downloaded the file, GameCo suffered an additional loss.[157] Assuming X had sold the file to individual buyers, X would have earned money on each sale. But one need not look to the value the company places on the source code to address this problem. Since copying the file qualifies as taking of property, each act of copying is reasonably seen as a separate transfer of property. It is reasonable, therefore, to calculate the value of the good based on the number of copies downloaded.

Further complicating this analysis is X's decision to distribute the code for free. X never, in a conventional sense, received any monetary value for distributing the source code. But this statement is incomplete, for X did receive some value in placing the file onto the bulletin board. Theoretically, X made a decision that in distributing the file for free he would end up in a better position than if he had sold the file to someone else or sold it to end users outright. Thus X did receive a benefit; the only question is how to translate that benefit into monetary terms.

Applying hypothetical amounts of money to these conclusions, the determination might be made as follows. First assume the compiled application with accompanying documentation retails for $110. Assume expert testimony establishes that buyers of the stolen good would be willing to pay $100 for a copy of the source code without documentation—the expert assumes that those who would buy it are able to compile it easily, can acquire third-party documentation relatively cheaply, and see independent value in having the source code because they know how to alter it. Also, assume that it can be established that a total 51 people downloaded the file, and that is the total number of people who would be willing to buy the stolen file. Assume further that X could have easily found a willing buyer for his only copy of the code who would be willing to distribute the code on his own (assume X adheres to a hacker's code of ethics and will not retain a copy for himself).

---

[157] GameCo suffers at least two losses every time someone acquires an unauthorized copy of the source code. First, GameCo loses a potential sale of the product. Second, a new potential competitor of GameCo is able to compete unfairly with GameCo by avoiding a great deal of the cost of developing the product.

Since we do not know how much value X derived from uploading the file to the bulletin board, but can reasonably assume that it is more than the value of selling the source code file to one individual who could distribute for $100 each the file to 51 people (with $0 in transaction costs),[158] the value to X must have been at least $5,099. Under these facts, a jury might conclude that the value of the stolen property in a thieves' market meets the statutory threshold.

In these cases, there can be no simple answer to the question of value. Expert testimony will be necessary. The above analysis serves only as an example solution to one problem and a list of questions to ask in similar cases. Computer file crime forces the recognition that new forms of property require new approaches in questions of valuation.

CONCLUSION

The NSPA attempts to solve the shortcomings of state theft laws as applied to property which easily migrates across state lines. Courts have applied the NSPA to property that is, for all practical purposes, entirely intangible. The Supreme Court, in *Dowling*, held that copyright infringement alone is not sufficiently like stealing to meet the statutory requirement that the property be "stolen, converted or taken by fraud." However, to read *Dowling* as a case which applies to all intangible property would be to render application of the NSPA anomalous: a thief can easily avoid federal prosecution by merely copying the intangible property onto his own tangible medium. The theft of computer files provides an excellent example of a case in which such an anomaly could frequently arise. Because it is plausible to reasonably distinguish mere copyright infringement from using illicit means to acquire a computer file, the NSPA should be read to apply to computer file theft. When read this way, new problems of valuation arise. However, existing case law provides the means to overcome these problems.

Unauthorized acquisition of a computer file is different from stealing a car. But this should not necessarily require the enactment of an entirely new statute for every type of computer crime. One alternative, and a good starting point, in an era when com-

---

[158] I make this assumption only to simplify the analysis. The assumption is unrealistic. X probably would have incurred significant costs in locating a buyer for the package who would be willing to distribute it at a profit.

puters will repace paper as a medium of storage, is the simple recognition that these cases involve a new form of property, and a new form of theft.