Journal of Civil Rights and Economic Development

Volume 11, Summer 1996, Issue 3 Article 8

Internet: A Safe Haven for Anonymous Information Thieves?

Peter J. Toren

INTERNET: A SAFE HAVEN FOR ANONYMOUS INFORMATION THIEVES?

PETER J. TOREN*

I am with the Computer Crime Unit of the Criminal Division of the United States Department of Justice. We view things somewhat differently than do some of the other panelists who have spoken this morning. You have probably all heard of the story about Willie Sutton.[1] Back in the 1920s or 1930s Sutton was asked, "Why do you rob banks?" His answer was very straightforward, "Because that's where the money is."[2] What we see now is that criminals are beginning to use the Internet and computers to commit their criminal acts, "because that's where the money is."

I will provide a brief illustration of some of the issues which demonstrate that information is an extremely valuable commodity and some of the problems which are associated with the advent of new technologies. These problems are exacerbated by criminal laws, which have not caught up to the new technology.[3]

The scenario involves officials of a large American corporation. They come to the FBI explaining that a former high level executive of the company has started his own consulting business, has hired away other engineers from their company, and has contracted with a number of foreign countries to build plants, all us-

* Peter J. Toren is a trial attorney with the Computer Crime and Intellectual Property Section, formerly the Computer Crime Unit, of the Criminal Division of the United States Department of Justice. As the Section's chief litigator, he is responsible for prosecutions and investigations involving: computer hacking, criminal copyright infringement, trafficking in counterfeit goods, and theft of trade secrets.

Mr. Toren has published an article in the Pepperdine University Law Review entitled *The Prosecution of Trade Secrets Thefts Under Federal Law*, 22 Pepp. L. Rev. 59 (1994). He is a frequent speaker at conferences on computer crime and other technology issues. The views expressed in this article are those of the author and do not necessarily reflect the views of the Justice Department.

[1] *See generally* WILLIAM F. SUTTON, WHERE THE MONEY WAS (1976).

[2] *But see* PAUL DICKSON & JOSEPH GOULDEN, MYTH-INFORMED: LEGENDS, CREDOS AND WRONGHEADED FACTS WE ALL BELIEVE (1993) (stating that this particular quote attributed to Sutton was in fact never used by him).

[3] *See generally* Stanley S. Arkin, *When Theft Of An Idea Can Be A Crime*, N.Y. L.J., Apr. 11, 1996, at 3 (discussing computer crimes and limitations of current laws in dealing with problem).

ing the company's proprietary information.[4] The FBI says that it sounds like a great case.

So what does the FBI do? They investigate. They find out that in the course of his employment, just before he left the company he downloaded thousands and thousands of documents belonging to the corporation. The process is really quite easy, because a single computer disk can hold upwards of 720 pages of information.[5] Using a few computer disks, the executive downloaded reams of information which was extremely valuable proprietary property of the corporation.

The FBI feels that the facts present a good case. They present the facts to the United States Attorney's Office and the United States Attorney's Office says, "Great, this sounds like a serious violation. What do we charge him with?" Everybody sits around and scratches their head a bit, and one person says, "Well we can charge them with wire fraud because the former executive deprived the company of their expectation of their honest services."[6] Another person comments that it is not clear that the executive used a wire in executing the criminal act. Further, the executive may not have used a telephone in his fraudulent endeavors. But what about mail fraud? The group responds negatively because there is no evidence that the executive used the public mails in the execution of the criminal act.[7]

Someone else suggests the Computer Fraud and Abuse Act of 1986,[8] which is currently the only federal criminal statute that is directly related to computer hacking. The statute, however, deals with unauthorized access and exceeding authorized access.[9] One attorney argues that the executive did access the company's computer in the commission of the act. The Computer Fraud and Abuse Act, however, provides that the access must have been

[4] *See* Kerry Fehr-Snyder, *Employers Stung By Stolen Trade Secrets*, PHOENIX GAZETTE, June 1, 1994, at A1.

[5] A 3.5 inch disk can store approximately 720 pages of double-spaced type.

[6] *See* 18 U.S.C. § 1343 (1994) (stating that anyone who commits fraud by wire, radio, or television is subject to fine and/or imprisonment).

[7] *See* 18 U.S.C. § 1341 (1994) (legislating that anyone who attempts to or does defraud "by placing any object in the Public or Private Mail" is subject to fine and/or imprisonment).

[8] *See* 18 U.S.C. § 1030 (a) (4) (1994) (stating that anyone who "knowingly" accesses computer without authorization and obtains protected information is subject to prosecution).

[9] *See id.* § 1030(a) (1) (1994) (providing that one who "knowingly access[es] computer[s] without authorization or exceeding authorized access" is subject to fine and/or imprisonment); *id.* § 1030(a) (2) (providing that "intentional" unauthorized access is punishable by fine and/or imprisonment).

without explicit authorization or that the actor exceeded his authorized access.[10] The statute might not work in this scenario because the executive had authorization to access the company's computer. He was a high level executive. He had access and he had authorization to access any of the company's information.

By now you can imagine that the United States Attorney's Office and the FBI are extremely concerned about this type of situation and its result. Someone suggests that the executive can be charged with the interstate transportation of stolen property.[11] There is evidence that he not only downloaded the information from the company's computers, but he also opened a number of consulting businesses overseas using the corporation's proprietary information. The executive transferred the corporation's proprietary information via the Internet, across computer lines to offices within other states and countries.

The property in question, however, was intangible property.[12] There was no physical thing transported across state lines, or across international boundaries. That presents a problem, because under title 18, section 2314 of United States Code, which prohibits the interstate transportation of stolen property, the property must be a good, ware, or merchandise.[13]

Someone asks if intangible property constitutes a good, ware, or merchandise. Professor Lessig talked a little bit about the unique quality and the unique characteristics of information and intangible property.[14] At the present time, it is not clear under federal

[10] 18 U.S.C. § 1030 (1)-(4) (1994).

[11] *See* 18 U.S.C. § 2314 (1994) (stating that anyone "transporting, transmitting or transferring in interstate or foreign commerce any goods, wares, merchandises securities or money exceeding $5,000, knowing same to have been stolen, converted or taken by fraud shall be fined and/or imprisoned"); *see also* Xan Raskin & Jeannie Schaldach-Paiva, Eleventh Survey of White Collar Crime, *Computer Crimes*, 33 AM. CRIM. L. REV. 541, 544-62 (1996) (discussing federal approaches to computer crimes); Camille C. Marion, Note, *Computer Viruses and the Law*, 93 DICK. L. REV. 625, 641-42 (1989) (discussing various state statutes addressing computer-related crimes).

[12] *See, e.g.*, United States v. Brown, 925 F.2d 1301, 1307-08 (10th Cir. 1991) (finding that computer programs and secure computer codes were intangible property, and as such, did not constitute goods, wares, or merchandise within the meaning of 18 U.S.C. §2314). *But see, e.g.*, United States v. Riggs, 739 F. Supp. 414, 418 (N.D. Ill. 1990) (holding that proprietary information contained in 911 computer text file was not based on deprivation of intangible right but rather property rights).

[13] 18 U.S.C. § 2314 (citing transportation, transmittal, or transfer of fraudulently obtained goods as offense punishable by fine and/or imprisonment).

[14] *See* Lawrence Lessig, Symposium, *Intellectual Property and Code*, 11 ST. JOHN'S J. LEGAL COMMENT. 635, 638 (1996) (explaining that intellectual property may be used without depriving owner of simultaneous use, but that same is not true of other property types).

law whether or not intangible property and information constitutes a good, ware, or merchandise.[15] The little guidance that exists is a case out of the Tenth Circuit[16] that says purely electronic signals transmitted across state lines are not considered goods, wares, or merchandise.[17]

So the United States Attorney's Office must decide which statute is the best to employ to prosecute the executive who has stolen proprietary information and has cost this American company perhaps millions and millions of dollars in lost sales to foreign companies. The end result is a situation in which the individual might not be able to be prosecuted under a criminal law.[18]

I think this example illustrates some of the problems we are faced with in the criminal area. The growth of the Internet and the effect of the computerization of the criminal area shows that proprietary economic information which is developed and stored in computers increases the risk of theft because thieves can access

[15] *See* Henock Gessesse & Karen Sauzaro, Eleventh Survey on White Collar Crime, *Intellectual Property*, 33 AM. CRIM. L. REV. 839, 843 (1996) (stating that Tenth Circuit, in *United States v. Brown*, determined items must be tangible, but one district court, in *United States v. Riggs*, found otherwise); *see also* Adam S. Ciongoli, et al., Ninth Survey of White Collar Crime, *Computer-Related Crimes*, 31 AM. CRIM. L. REV. 425, 431 (1994) (asserting that computer programs are not "goods" and "wares" when solely in intangible form and would most likely be governed by mail and wire fraud statutes).

[16] *Brown*, 925 F.2d at 1301.

[17] *See* United States v. Brown, 925 F.2d 1301, 1307 (10th Cir. 1991); *see also* Stanley S. Arkin & Michael F. Colosi, *The Criminalization of Theft of Technology and Trade Secrets*, 3 No. 5 BUS. CRIMES BULL. COMPLIANCE & LITIG. 4, 4 (1996) (discussing amount of theft of intellectual property owned by American corporations); Christopher Parkes, *Theft of Corporate Secrets Soars*, SAN DIEGO UNION TRIB., Mar. 22, 1996, at C2 (discussing American Society for Industrial Security study which measured amount of theft of corporate secrets).

[18] Since the date of the speech, Congress has enacted the Economic Espionage Act of 1996, 18 U.S.C. § 1831, which criminalizes the misappropriation of trade secrets. The intent of Congress in passing the Act was to cover a situation such as the one described in the speech:

> The principal problem appears to be that there is no federal statute directly addressing economic espionage or which otherwise protects proprietary information in a thorough, systematic manner. The statute that federal prosecutors principally rely upon to combat this type of crime, the Interstate Transportation of Stolen Property Act (18 U.S.C. § 2314), was passed in the 1930s in an effort to prevent the movement of stolen property across state lines by criminals attempting to evade the jurisdiction of state and local law enforcement officials. That statute relates to "goods, wares, or merchandise." Consequently, prosecutors have found it not particularly well suited to deal with situations involving "intellectual property," property which by its nature is not physically transported from place to place. Courts have been reluctant to extend the reach of this law to this new type of property. One court has held that "the element of physical 'goods, wares, or merchandise' in sections 2314 and 2315 is critical. The limitation which this places on the reach of the Interstate Transportation of Stolen Property Act is imposed by statute itself, and must be observed." United States v. Brown, 925 F.2d 1301 (10th Cir. 1991).

H.R. REP. No. 104-788 (1996).

such information remotely. In this case, the information thief did not have to go to the copying room and he did not have to get the documents out of some central file and physically have his secretary copy them. Rather, he was able to access the information using company passwords and he was able to transmit this stolen information across state lines.

Furthermore, it is very difficult to trace this sort of theft because of the anonymity of the Internet. Finally, the amount of information that is downloaded is limited only by the transmission speeds and exceeds the amount of data that can be stolen physically. The bottom line of what we are facing as part of the computer crime unit, is that criminal laws have not kept up with this monumental change in how information is stored and how information is transmitted across state lines and across trans-national boundaries.