New York Law Journal

July 23, 2001 Monday

MISUSE AND MISAPPROPRIATION OF ELECTRONICALLY STORED INFORMATION

By Stanley S. Arkin

More and more, the transactions and interactions of our personal and business lives take place on-line. While the convenience and efficiencies to individuals and corporations are undeniable, we are only beginning to understand the implications and complications inherent in having such a great quantity and variety of information transmitted and stored electronically and potentially vulnerable to electronic interception or misuse.

A great deal of the personal data available about us on-line is directory-type information that is not generally considered private. Fee-based information clearing houses, however, do not restrict themselves to on-line phone books. These search programs delve far deeper into the personal affairs of their subjects, offering a wide variety of personal information to anyone paying as little as a few dollars. For example, a company called KnowX.com offers its customers detailed information on a search subject's assets, as well as information regarding the subject's credit, bankruptcy and marriage history. While much of this data is culled from public records and credit agencies, the ease and convenience with which it is now available to virtually anyone is, nevertheless, unsettling.

Proprietary information belonging to businesses, as well as privileged personal information such as medical records are, of course, also stored and transmitted by computer in quantities unimaginable even a decade ago, creating breaking and entering opportunities that burglars of old could not have entertained. Trade secrets, intellectual property and all manner of financial data (not to mention voluminous data on a company's customers) are vulnerable to theft and misappropriation as never before, placing the corporate world at greatly increased risk of loss. One study reported that 78 percent of U.S. companies suffered at least one network security breach in 1999.

As Internet communication matures and expands, it is worth pausing to ask what protection the law provides against the misappropriation of our personal and business-related confidential data. One safeguard has been the criminalization of certain hacking activities. In other instances, private actions under federal statutes some designed specifically to deal with electronic information and some not may provide an answer. In addition, common law privacy rights that have long been enforced by our courts may serve as legal deterrents to unseemly intrusion.

The primary federal statutory weapon against computer crime is the Computer Fraud and Abuse Act (CFAA), enacted in 1984. The current version provides that intentional unauthorized access to a government computer is a criminal act, regardless of whether any damage is caused or information stolen. Nongovernment computers also fall under the statute if they are protected computers. Protected computers include any computer used in interstate or foreign commerce and communication, which brings any computer hooked up to the Internet under the CFAA. Unauthorized access to nongovernment protected computers must result in damage in order to fall under the CFAA, but the intent required is only to access without authorization.

The media often bestow tremendous publicity on hackers like Kevin Mitnick who, over the course of a two-and-a-half-year cybercrime spree, broke into the systems of dozens of companies like Novell, Sun Microsystems and Motorola, stealing software while repeatedly evading federal authorities. Probably a greater threat to business, however, is the humble employee intent on mischief. A few recent federal prosecutions are illustrative of the vulnerability of electronic information to misappropriation by these inside hackers.

Recently, three men, including two former employees of Lucent Technologies, were indicted for conspiring to steal trade secrets from Lucent for transfer to a joint venture between a high-tech company they owned and a telecommunications company controlled by the Chinese government. The indictment charges that the defendants used e-mail and a password-protected Lucent Web site to steal and transfer valuable software, source code and design information to ComTriad Technologies, a start-up company founded by the defendants.

Although the profit motive probably impels most computer crime in the corporate world, as in any other business context, factors like spite, animosity and a perverse sense of challenge, unrelated to the content of the system being penetrated, may also drive the perpetrator. Last year, Internet Trading Technologies Inc. (ITTI), an on-line trading firm, was the victim of serious computer sabotage at the hands of a disgruntled employee. The employee, Abdelkader Smires, a programmer at ITTI, had quit after his demands for a raise were refused. Later that day, the company's computer came under attack from a computer traced to a nearby Kinko's, and crashed, resulting in lost income for the company and, perhaps more damaging, bad publicity and loss of reputation. Mr. Smires was charged under the CFAA and, after confessing, was sentenced to eight months in prison.

Striking about the ITTI case is the extent to which even the most sophisticated computer security system may be useless against a savvy insider with a grudge. The implications of a lone worker possessing the potential to inflict massive damage on his employer in a single afternoon from a nearby copy shop is staggering and frightening.

In addition to the CFAA, federal legislation not specifically designed to deal with computer crime is also potentially helpful in prosecuting computer crime. Internet communications, for example, likely implicate the federal wire fraud statute, an enormously elastic prosecutorial weapon usually held applicable to almost any sort of disingenuous conduct. The government has also used federal statutes proscribing wiretapping and the interstate transportation of stolen goods to prosecute cybercriminals. In the intellectual property arena, data bases constituting an original work by virtue of the compilation or arrangement of the facts contained therein enjoy federal copyright protection.

The task of combating computer crime has not been confined to the federal level. State lawmakers have also been active in drafting legislation to curtail electronic fraud, theft and wrongful intrusion. For example, Article 156 of the New York Penal Law provides for numerous offenses involving computers including unauthorized use of a computer, computer trespass, computer tampering (in the first through fourth degree), unlawful duplication of computer related material and criminal possession of computer-related material.

The federal and state criminal justice systems, however, can only do so much to stem the tide of cybercrime. For a variety of reasons, including limited resources, the vast majority of federal agency referrals for the prosecution of computer crime are not, in fact, prosecuted. These referrals, of course, are only a tiny fraction of the number of hacking incidents. One study estimated that less than two percent of computer security breaches ever reach the initial attention of law enforcement, perhaps because the targets do not want to risk the negative publicity of a security breach.

Private Actions by Statute and Common Law. The criminal law statutory scheme, however, is supplemented by numerous private actions that may serve as a defense against, or at least a remedy for, computer mischief, particularly in the privacy context. The common law tort of intrusion on the seclusion of another makes liable a person who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, provided the intrusion would be highly offensive to a reasonable person. Having applied the tort successfully to wiretaps, the courts should have no trouble extending its reach to cover, under certain circumstances, wrongful access to information systems or electronic communications.

Privacy law also imposes liability for the public disclosure of private facts about another if the disclosure is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public. This tort, which would seem to provide for protection against the electronic disclosure of certain information or the disclosure of information electronically stored or communicated, was included in a 1996 action brought in Texas state court by Beverly Dennis against Metromail Inc., a direct-marketing firm. The facts reveal the potentially serious consequences of the commoditization of seemingly innocuous information about consumers.

Ms. Dennis had filled out a Metromail preference survey in exchange for the promise of discounts and giveaways. Among the information Ms. Dennis provided was her name, address, gender and age, as well as information about her health and buying habits. Months later, Ms. Dennis received a sexually graphic letter from a convicted rapist serving a sentence at a prison that had contracted to perform electronic data processing tasks for Metromail under an inmate work program. The inmate sprinkled his letter with personal information about Ms. Dennis gleaned from the survey. He also proposed a visit to her house upon his release and, of course, he had her address. The case was settled before trial.

Also useful in prosecuting a private action against a nongovernmental body for the wrongful dissemination of private information are various Federal statutes. The Electronic Communication Privacy Act (ECPA), for one, enacted in 1986, protects against unauthorized access, interception or disclosure of private electronic communications by private parties (as well as by the government). The ECPA applies to communications both while in transit, and while stored,

and includes a provision prohibiting a public telecommunications company from disclosing the contents of communications or an electronic message.

A private right of action is also available under the CFAA, which provides that any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A number of additional statutes including the Fair Credit Reporting Act (FCRA) and the Video Privacy Protection Act (VPPA) address concerns regarding particular types of information disclosures. The FCRA places restrictions on the purposes for which a credit agency may release information about a consumer, and requires the user of a credit report to supply the consumer with the name and address of the credit-reporting agency. The VPPA, passed in reaction to the media's access to the names of videos rented by U.S. Supreme Court nominee Robert Bork, prohibits the disclosure of the title description or subject matter of a film rented by a particular customer absent written consent. While helpful, these laws apply only to a limited category of information in particular industries.

Constitutional and Statutory Protection Against Government Abuse. Not only may the criminal justice system not always suffice to protect individuals and corporations against computer crime, but the government itself may sometimes overstep its bounds in its intrusion upon the privacy of the electronic information of an individual or business. The courts have been struggling for decades with the question of the applicability of traditional constitutional protections against wrongful search and seizure to new technologies.

The application of Fourth Amendment protections to information communicated or stored electronically was explored by a United States military court in **United States v. Maxwell,** in which the incoming and outgoing e-mails of the accused were obtained from America On-line by prosecutors. A lower military court had held that although the accused, who was charged with using his personal computer to communicate indecent language and child pornography, had a subjective expectation of privacy for his e-mail messages, the manner in which the transmissions were sent over AOL negated the objective reasonableness of the expectation. The appellate court disagreed, finding that although the appellant may have forfeited his right to privacy to any e-mail transmissions that were downloaded from the computer by another subscriber or removed by a private individual from the on-line service, the e-mail messages stored in the AOL computer were entitled to Fourth Amendment protections. Similarly, the court found messages sent to appellant protected to the extent that he alone could retrieve them through his assigned password.

Additional protection against governmental infringement of privacy rights in electronic information and communications are provided for by legislation. As described above, the Electronic Communications Privacy Act applies to the government as well as to private parties. In **Steve Jackson Games Inc. v. United States Secret Service,** the court found that the Secret Service violated the ECPA after agents seized plaintiff's computers containing software, unread e-mail and other materials that were outside the scope of the Secret Service's warrant. The agents, who were searching for a document stolen by computer hackers, suspected that it had been uploaded to an on-line bulletin board operated by the plaintiff. Although they obtained a warrant to search certain materials from the bulletin board, their seizure of the additional stored information, the court concluded, constituted a violation of the statute.

The court also found the government in violation of the Privacy Protection Act (PPA), which guards the First Amendment rights of publishers by prohibiting the government from searching or seizing any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast or other similar forms of public communication. Among the work product materials found to have been wrongfully seized in **Steve Jackson** were materials to be published on-line. It remains to be seen how broadly the courts will interpret forms of public communication as they relate to on-line materials. Will, for example, anyone with a Web site fall under the PPA's protection with respect to related material? As we come to rely increasingly on information transmitted and stored by computers, these, and a host of other questions, will have to be sorted out.

As the centralization and accessibility of our personal information increases, as, indeed, our personal and business existences become more and more data based, our Congress and state legislatures need to carefully focus on crafting rules and sanctions capable of dealing with this manifest threat to commonly conceived notions of privacy.