

Computer Security and Privacy: The Third Wave of Property Law

by Leslie G. Berkowitz

©2004 The Berkowitz Firm, P.C. All Rights Reserved.

This column is prepared by the CBA Technology Law and Policy Forum Committee. The column provides information of interest to intellectual property attorneys and other attorneys who counsel technology companies, by focusing on developing law applicable to technology businesses.

Property law has evolved through three waves: land; chattels; and, now, information. This article explores a variety of the cyber security and privacy laws and the way in which they further the development of the information property wave.

Column Editors:

Nathaniel T. Trelease, WebCredenza, Inc., Denver—(720) 937-9930, ntrelease@webcredenza.com; Jim Brogan, Cooley Godward, LLP, Broomfield—(720) 566-4190, jbrogan@cooley.com

About The Author:

This article was written by Leslie G. Berkowitz, Denver, an attorney with The Berkowitz Firm, P.C., practicing in the area of technology law since 1981. He can be contacted at (303) 832-8520 or berkowitzles@berkowitzfirm.com.



When we talk about property, we are really talking about a right of a person to control a thing. The right to use, the right to exclude others from using, and the right to transfer something constitute the bundle of rights we call “property.” In other words, property is not the thing itself—it is the bundle of rights that give control of it.

This article explores how computer security and privacy issues help define the rights that convert information into property. It also discusses a framework and context for the privacy/security debate. This article does not intend to provide a comprehensive treatment of the law governing information privacy and security.¹ Instead, it intends to offer a conceptual framework for analyzing computer security and privacy laws and to demonstrate how such laws are part of a broader legal trend serving as the umbrella under which this information is protected.

Security and Privacy Allocation of Control

There are different aspects to security and privacy. The area where they overlap relates to control, which is basic to our concepts of liberty. John Stuart Mill associated property with liberty and suggested that security of property is essential for people to maximize their potential for liberty.² The right to protection of person and property is one of the oldest concepts of the common law.

Law-related security seeks to restrict others from interfering with the rights of control, including, among others, theft (the right to control chattels) and trespass (the right to control land). Privacy, likewise, relates to control, but is more abstract. Unlike security, which may have its roots in concepts of control over tangible objects or land, privacy has its roots in the concept of self. It was first articulated as a legal principle in an 1890 law review article³ and, then in 1894, enunciated by the U.S. Supreme Court.⁴ Principles akin to privacy actually were discussed even earlier when the Court stated:

... [N]o right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law.⁵

The right of an individual to choose what is revealed about him or her is essential to the concept of liberty.⁶

Concepts of Individual Control: Three Waves

The concepts of individual control have occurred in three waves. First, they arose with the end of feudalism, evolving into concepts of real property, from control strictly by the sovereign to being owned by a broader group of people. Future interests, forms of title, and other concepts of estates in land developed as people

struggled with how to extend to the masses the basic bundle of rights discussed above.

The second wave emerged with the development of the merchant class. It continued with the rise of the industrial revolution, where concepts of property spread to objects that had not always been considered to be under the control of individuals, such as furniture, tools, and even abstractions (promissory notes).

The third wave had its origin in the 1700s, when intellectual property concepts began to emerge and the cluster of four was developed to protect works of people's minds: (1) copyrights, (2) patents, (3) trademarks, and (4) trade secrets. Today, this third wave is coming fully into fruition, as property rights are attributed to information itself, even information not traditionally part of the four intellectual property areas.

Intellectual property derives its value from the time, labor, and capital that is required to develop it. Information derives value from the desire of people to control its use, availability, and transfer. Conceptually, the use of information in society shares many issues with other forms of property.

Companies and individuals seek to control who could have access to research reports, health-care data, driver's license information, and analysis of company stock, as well as how that information should be used. This is similar to the way they want to control who has access to their homes, drives their car, and supervises a company's plant and operates its equipment. Information may have a bigger effect on the profits of the company or the life of an individual than furniture or tools that they use. Thus, a calculator often is less important than the numbers that it adds.

Designating Information as Intellectual Property

The branch of intellectual property law that comes the closest to designating information as property is that of trade secrets, but even the law of trade secrets has not gone that far. Trade secrets law traditionally has governed the breach of a confidential relationship, rather than the creation of a property right.⁷ Misappropriating trade secrets could not, historically, be prosecuted as larceny, but this perspective has been breaking down, with some cases expressly defining trade secrets as property.⁸

As a trend of cases beginning in the 1980s demonstrates, information is increasingly being considered as property. Information is broken down into discrete units to be categorized and manipulated in much the same way that chattels have been in the past. Information about the buying habits of individuals may be stored, retrieved, or combined with other information by computers. Even visual images may be broken down into component parts and recorded as lines of "1s" and "0s" on computer hard drives.

In the modern age, when data are understood as forms of property, the subjects of security and privacy begin to overlap. Furthermore, to protect the right to control how that information is used and moved in society, legal principles are being developed to clarify these prerogatives. Both security and privacy affect the three basic property rights as they relate to information: (1) the right to use the information; (2) the right to prevent others from using it; and (3) the right to transfer it. Security and privacy may relate to issues other than information, but the overlap in the struggle over who controls which may

be best understood by looking at the diagram below.

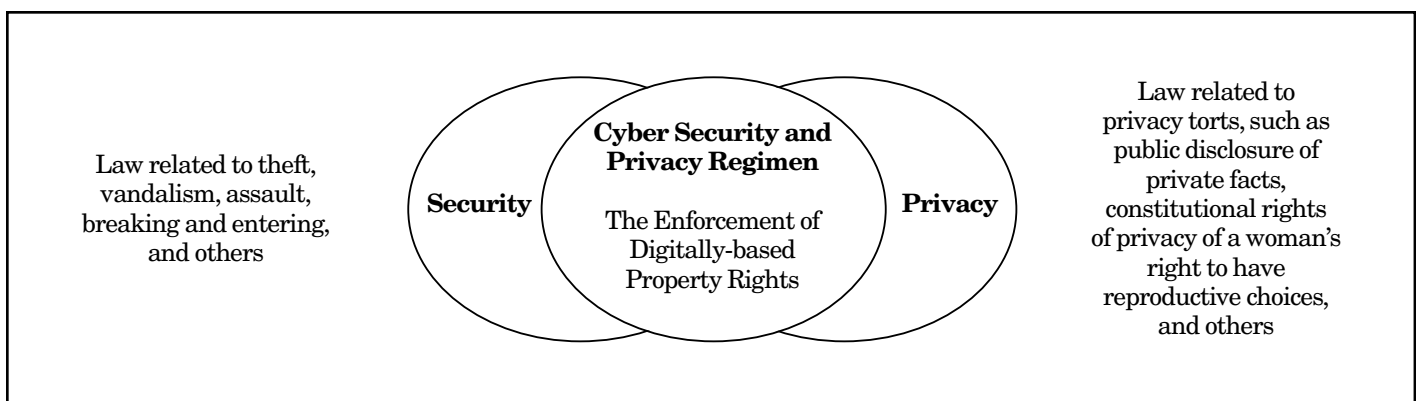
Security risks to access to information can occur from many sources. If the means of access is not controlled, the information that can be accessed is not controlled.

Common Internet Security Threats

Businesses transferring data online should be wary of the ever-increasing threat to their security. Would-be hackers have greater access to information than ever before. Some of the more common threats are as follows:

- *Communications Monitoring*: This occurs when an unauthorized party monitors and reads private information without penetrating the computer system. This problem is particularly urgent for those with dedicated lines such as DSL.
- *Theft of Information*: Sensitive information may be located through monitoring, then procured through interception or hacking.
- *Data Interception*: By using a process that generally begins with the application of a "sniffer" program, hackers often can intercept, remove, or modify online messages.
- *Repudiation*: Repudiation, the inability to authenticate a contract partner, occurs when a party to a transaction falsely denies the legitimacy of a transaction.
- *Masquerades*: Rogue servers may have the ability to impersonate legitimate servers to trick data owners into falsely revealing sensitive information.
- *Mapping of Information Flow*: Company information can be mapped under certain circumstances. By simply

Diagram: Security and Privacy Overlap



browsing the Web, users can become quite vulnerable. The following information can be obtained without the knowledge of the unwary user: technical information pertaining to the user's computer configuration; the name, physical location, and contact persons of the organizations with registered domain names; and browsing activity.

Most people are aware of the use of cookies⁹ to mark and identify users to enable tracking of their Web browsing habits. Other markers that can track use are not as well known. For example, the Microsoft Word File Menu has a selection for "properties," which includes information about the source of the document, its drafting history, and related information. Even revision-marking can reveal information about the thought process of a client and the attorney. Much of this code becomes embedded and can pose a security risk (threat to the loss of confidential information). Some of these threats clearly are controllable by the originator (attorney or client in this example), but others could rise to the level of prohibited behavior under the computer security and privacy statutes described in this article.

Even the use of cookies, as common as they are, has come under scrutiny under these statutes.¹⁰ Increasingly, attorneys must consider possible abuses of security and privacy statutes when advising clients regarding business models. Violation of the statutes can create substantial financial penalties, civil liability, and criminal sanctions. The remainder of this article discusses security and privacy statutes that are more easily understood if considered in a framework where information is treated as property.

The Computer Fraud And Abuse Act

The Computer Fraud and Abuse Act ("CFAA")¹¹ was enacted in 1984 in recognition of a growing problem with behavior that would be prohibited if not carried out with the use of electronic or computer means—activity that was not clearly within the scope of previous criminal statutes. The CFAA governs both internal and external threats, consisting primarily of seven distinct, prohibited activities or "deadly sins."

Definitions

Before exploring the behavior prohibited under the CFAA, it is important to understand some basic definitions, because, although widely used, their meaning varies. Understanding the statutory context is essential to applying the statute to specific business activities.

Computer: Pursuant to the CFAA, a "computer" includes any high-speed data processing device, even those of electrochemical design.¹² It comprises storage and communication facilities used in conjunction with such processing devices, but does not include automated typewriters or typesetting equipment, portable hand-held calculators, or other similar devices. It is unclear whether hand-held computers and personal data assistants ("PDAs") fall within the exception or within the main definition.

Hand-held computers and PDAs might be distinguished based on the fact that common calculators and typewriters lack storage, have limited input-output capabilities, and lack interconnectivity (they cannot upload or download). PDAs initially were similar to calculators and typewriters in these characteristics, but are rapid-



**COLORADO STATE
BANK AND TRUST**®
N.A.

Downtown 303 861-2111
Cherry Creek 303 318-6000

Cherry Hills 303 318-6070
Highlands Ranch 303 318-6040

TRUST SERVICES

Trust Administration
Estate Settlement Services
IRA and Qualified Plan Administration

Asset Custody Services
Individual Retirement Planning
Complete Banking Services for the Firm

- Professional Investment Management
- Compliance with the Colorado Prudent Investor Act
- Compliance with the Colorado Uniform Principal and Income Act

Specializing in the unique financial needs of Colorado's Legal Community

*Proudly supporting COLTAF as a Gold Honor Roll Bank
Actively supporting the Colorado and Denver Bar Associations*

ly shifting to having these elements in common with what now is more commonly viewed as a computer. It is unclear how the new wireless technologies will affect what is included in this definition.

Protected Computer: The term "protected computer" began with a limited scope, focusing on government and financial computers. Since the enactment of the USA PATRIOT Act,¹³ the definition includes computers used in or affecting interstate or foreign commerce anywhere in the world.¹⁴ It is impossible to imagine any computer that does not come under this broad definition. Even a stand-alone computer used for personal use and not having a modem would seem to be included within the scope of the definition, because it could affect interstate or foreign commerce.

Financial Institution: The definition of "financial institution" itself is broad. It includes institutions insured by the Federal Deposit Insurance Corporation, National Credit Union Administration, Securities Investors Protection Corporation or Home Loan Bank, institutions of the Farm Credit System, a broker-dealer regulated under Section 15 of the Securities and Ex-

change Act of 1934,¹⁵ an organization operating under the Federal Reserve Act, or a branch or agency of a foreign bank.¹⁶

Exceeds Authorized Use: The phrase "exceeds authorized use" under the CFAA encompasses access that is permitted, but is used to do things not permitted by such access.¹⁷ This includes, for example, behavior of employees who are authorized to access their company's computer system for purposes of obtaining sales information, but not human resource records.

Loss: "Loss" means any reasonable costs to any victim, whether such costs are incurred in responding to the offending behavior or are incurred in assessing damage or restoring data. Furthermore, these costs may include lost profits or consequential damages incurred as a result of interruption of service.¹⁸

Seven Prohibited Activities

The CFAA prohibits seven distinct activities.¹⁹ These "sins" contain elements of "knowledge," "access," and "authorization."

1. The first sin is knowingly accessing, without authorization or in excess of authority, information that has been determined to be secret for national defense or foreign relations purposes, or data restricted by the Atomic Energy Act of 1954.²⁰ There has to be reason to believe that the information obtained could injure the United States or be used to the advantage of a foreign nation. A violation occurs when the information is willfully transferred or willfully retained, and the violator fails to deliver it to the appropriate officer or employee of the U.S. government.

By applying the prohibition even if the access is without authorization or exceeds the authority that is granted, the prohibition encompasses employees and others who have some authorized use, but who abuse that authority. For example, an employee of the Atomic Energy Commission who works in payroll has access to, but does not have authority to access, site specifications for a nuclear power plant. This first prohibition produces strict liability if someone knowingly accesses secret information that affects national security, whether or not he or she intended to cause harm. Another prohibited activity relates to simply retaining information, which was improperly accessed as described above, without delivering it to the person entitled to receive it.²¹

2. The second sin has three components, the third of which is broad enough to include almost any improper behavior. The first component is fairly specific, stating

that intentionally accessing a computer without authorization or exceeding authorization to obtain financial information from a financial institution or a card issuer is prohibited. The second component is broader than the first and relates to improperly obtaining information from any department or agency of the United States. The third component is the broadest and involves obtaining information without authorization, or exceeding authorization, from any protected computer if the conduct involved interstate or foreign communication.²²

3. The third sin relates to accessing government computers themselves, and not to specific information.²³ Most computers that are used by the federal government are used exclusively by and for the government, but many are used by the government and shared with others. For example, a government agency may share the use of a computer mainframe with a university for research purposes. Where a computer is solely for use by the government, it is illegal to intentionally and without authorization access such a non-public computer. However, where the computer is not for the exclusive use of the United States, it is still illegal to intentionally and without authorization access such a computer if the conduct affects governmental use.²⁴

For example, if the improper behavior prevents the government from conducting its work by occupying computer storage or processing capacity, the activity is prohibited, whether or not improper information was obtained. This might occur where someone uses a government computer to process his or her own data without ever accessing any government information. By using the government computer, the accessor saves considerable costs in equipment and facilities, but may have the effect of depriving the government of its use of the same equipment. Thus, such behavior is prohibited.

4. The fourth sin consists of accessing a computer without authorization for the purpose of perpetrating, or in furtherance of perpetrating, a fraud, if the perpetrator obtains anything of value.²⁵ This prohibition does not apply if the object of the fraud or thing of value obtained consists only of the computer itself, and the value of such use is less than \$5,000 in any one-year period. In other words, prohibited access for the purpose of minor uses of computer time is not included. This would carve out of the prohibition minor uses of a computer for personal Internet activity or use of per-

TRADEMARK

& COPYRIGHT SEARCHES

TRADEMARK-Supply word and/or design plus goods or services.

SEARCH FEES:

COMBINED SEARCH - \$315
(U.S., State, Expanded Common Law and Internet)
TRADEMARK OFFICE - \$135
STATE TRADEMARK - \$140
EXPANDED COMMON LAW - \$165
DESIGNS - \$210 per international class
COPYRIGHT - \$180
PATENT SEARCH - \$450 (minimum)

INTERNATIONAL SEARCHING

DOCUMENT PREPARATION
(for attorneys only - applications, Section 8 & 15, Assignments, renewals.)

RESEARCH- (SEC - 10K's, ICC, FCC, COURT RECORDS, CONGRESS.)

APPROVED- Our services meet standards set for us by a D.C. Court of Appeals Committee.

Over 100 years total staff experience - not connected with the Federal Government.

GOVERNMENT LIAISON SERVICES, INC.

200 North Glebe Rd., Suite 321
Arlington, VA 22203
Phone: (703) 524-8200
FAX: (703) 525-8451

Major credit cards accepted.

TOLL FREE: 1-800-642-6564

WWW.TRADEMARKINFO.COM

SINCE 1957

Brownstein | Hyatt | Farber

Brownstein Hyatt & Farber proudly introduces the newest additions to our firm.

2004 Shareholders

Mark T. Barnes

Shareholder
Litigation

Perry E. Bendicksen III

Shareholder
Municipal & Public Finance
Corporate & Securities

David P. Buchholtz

Shareholder
Municipal & Public Finance
Corporate & Securities

Meghan W. Martinez

Shareholder
Employment

Connie L. Peterson

Shareholder
Water & Public Lands
Environment & Natural Resources
Litigation

Christopher D. Reiss

Shareholder
Corporate & Securities

Jill K. Sweeney

Shareholder
Municipal & Public Finance
Corporate & Securities

New Additions in 2003

Rob L. Alvarado

Associate
Corporate & Securities

Judy A. Black

Senior Legislative Consultant
Public Policy

Eric R. Burris

Senior Counsel
Litigation

Eduardo A. Duffy

Associate
Corporate & Securities

Teresa J. Dyer

Legislative Specialist
Public Policy

Brent D. Johnson

Associate
Corporate & Securities

Michelle C. Kales

Associate
Environment & Natural Resources

Annie T. Kao

Associate
Litigation

Alfred E. Mottur

Senior Counsel
Public Policy

Mark M. Oveson

Associate
Real Estate

Douglas R. Sahmel

Legislative Assistant
Public Policy

Bryan M. Schwartz

Associate
Real Estate

Ryan J. Stuart

Associate
Litigation

Eric J. Zinn

Senior Counsel
Taxation

Celebrating **35**
A Partnership of Client and Counsel
years

www.bhf-law.com

sonal software on a company computer that results in relatively minor (less than \$5,000 in any one year) disruption of the company's computer.²⁶

5. The fifth sin prohibits three types of activities if they result in certain specific types of harm. The first prohibited activity of this sin includes knowingly transmitting a "program, information code, or command" that intentionally causes damage to a protected computer.²⁷ Second, the CFAA prohibits intentionally accessing a protected computer without authorization and recklessly causing damage.²⁸ Note here that if the access is intentional, the damage does not need to be intentional, but merely reckless. Third, intentionally accessing a protected computer without authorization and causing damage is prohibited.²⁹ Here, the prohibition is strict. Where the access is without authorization and intentional, if it causes damage, it is prohibited.

Violation of any of these prohibited activities is violation of the statute if it results in a variety of specific losses.³⁰ These specific losses are sufficient if, in the case of an attempted offense, they would have occurred if the offense had been completed. Such loss, during a one-year period, must be at least \$5,000 in value. This would seem especially difficult to apply in the event of an attempted offense, and it is extremely broad in application because it does not relate to any specific kind of damage.

The remaining damages that would result in a violation of this fifth sin are much more specific: (1) the modification or impairment of the medical examination, diagnosis, treatment, or care of one or more persons; (2) physical injury to any person; (3) any threat to the public health or safety; and (4) damage affecting the government in the administration of justice, national defense, or national security.³¹ These specific damages are not subject to the \$5,000 threshold that was established in the more general damage described above.

This fifth sin, 18 U.S.C. § 1030(a)(5)(B) (ii)-(v), is unclear in that "recklessly causing damage" is a subset of the broader provision, 18 U.S.C. § 1030(a)(5), not limited to "recklessly" causing damage.³² If the prohibition on recklessly causing damage were eliminated, the same conduct would seem to be included in the strict liability provision for simply causing damage. Also, this provision appears to be a catchall prohibition because most prohibited activity not covered elsewhere is picked up

here. For example, this provision prohibits transmission of viruses or other offensive code, as well as hacking. It also prohibits attacking computers for the purpose of damaging data, as well as inflicting physical harm, such as misdirecting the control of water at a dam.³³

6. The sixth sin is that of knowingly and intentionally trafficking in passwords "or similar information through which a computer may be accessed" without authorization if the trafficking affects interstate or foreign commerce or if such computer is used by or for the government of the United States.³⁴ By including the following language, "... or similar information through which a computer may be accessed . . ." the statute could include trafficking in decryption codes or cable television or wireless devices and other activity protected by similar authenticating techniques.

7. The seventh and final sin is that of extortion. It prohibits the transmission, with the intent to extort money or other things of value, of a threat to cause damage to a protected computer.³⁵ There are, for example, a number of documented instances involving threatening banks with disruption of their systems or seizure of their customers' information. The threat of such activity is prohibited, regardless of whether such threatened behavior actually occurs.

Offenses under the CFAA are not taken lightly. First-time offenses or attempted offenses are punishable by fine and/or imprisonment of up to ten years.³⁶ A second offense can lead to a fine and/or imprisonment of up to twenty years.³⁷

Historically, control of access was simply a matter of having a lock and key. Now that access to and distribution of media content and data are accomplished electronically and can be done remotely, they are harder to control. Access no longer requires a physical presence, but may need only the use of a number code. Cell phones are activated by identification codes, access to satellite cable content is acquired by descrambling encrypted signals, and automatic teller machines are accessed through the use of magnetic cards.

The CFAA seeks to protect the specific types of information described in this section of the article. From medical records to national security data, the CFAA clarifies who has the right to control such information. To allocate control, the CFAA also regulates the means of access to that information.

Getting Past the Gate

Those who use electronic commerce must protect themselves from potential threats to their informational security. From physical breaches to programmed threats, electronic information is vulnerable to attack in a variety of ways. In general, electronic security goals should focus on preventing the following security breaches:

- *Interception:* Unauthorized interception of information during transmission
- *Extraction:* Unauthorized removal of information
- *Insertion:* Unauthorized alteration of information caused by the insertion of additional data
- *Destruction:* Unauthorized destruction of information
- *Denial of Access:* The inability to facilitate authorized access to information.

Laws dealing with "breaking and entering" are no longer adequate to control unauthorized access. The laws discussed in this article have been enacted to deal with modern twists to age-old problems: how to prevent someone from going into a locked room without being given a key and how to stop someone from "siphoning" oil between depots without admission to the access points. The issue of digital rights is not primarily about controlling unauthorized taking of content. It is about controlling unauthorized access. The pipeline, not the oil, is the focus of concern with these laws. Even if nothing ever happens to the content, it might be a violation to get past the gate.

Counterfeit Access Device Statute

One of the laws that governs this area is the federal Counterfeit Access Device statute ("CAD"), which attempts to regulate unauthorized access to proprietary digital or cable services.³⁸ The following concepts must be understood to apply the CAD: (1) the level of intent required to establish a prohibited act; (2) the specific kind of behavior prohibited; and (3) the specialized meaning given to terms that otherwise have common meaning.³⁹

For the most part, the level of intent used throughout the CAD is "knowing and with the intent to defraud."⁴⁰ Note that the concept of going beyond limiting access is not present in the CAD, as it was in the CFAA. There is no case on point, but the CAD would not seem to prohibit someone who has authorized access from using that

access in an unauthorized way. It does not appear to prohibit someone from using that access in ways that were not part of the agreement granting access. Those issues are left to traditional civil remedies pursuant to licenses or contracts.

Prohibited Behavior

Under the CAD, there are differences between the standards for counterfeit access devices and those for unauthorized access devices (see "Terminology," below). Counterfeit devices are subject to prohibitions on production, use, or trafficking in such devices. Merely possessing a counterfeit access device is prohibited if more than fifteen such devices are involved.⁴¹ Trafficking or using an unauthorized access device also is prohibited. However, unauthorized—rather than counterfeit—access devices or effecting transactions with someone else's access card require a further showing that the devices have been used to acquire things of value in excess of \$1,000. Also prohibited is use of a scanning receiver. Such a receiver is specifically designed to intercept or retrieve identification numbers used to control access to telecommunications.⁴²

Terminology

The term "access device" can seem misleading, because a device is usually thought of as something that can be touched and felt. However, the term, as used in this statute, focuses on modern means of access, which include such things as codes, account numbers, electronic serial numbers, and personal identification numbers.⁴³

Further definitions include the following: A "counterfeit access device" must be a genuine device of legal origin, but with altered identification code.⁴⁴ "Device-making equipment" might not be equipment at all. It might be software used to re-program a code.⁴⁵ An "unauthorized access device" includes those devices that are merely lost, revoked, or cancelled.⁴⁶

The distinction between "unauthorized" and "counterfeit" devices is murky. It is difficult to conceive of an access device that is not counterfeit when used by someone after being "cancelled." To cancel a card with a magnetic code requires changing the authorization on the computer that reads the card. The device would then be inoperable without altering the card, in which case the card would be a counterfeit access device.

Economic Espionage Act

Statutes such as CFAA and CAD, discussed above, cover similar behavior and, in some cases, overlap. The Economic Espionage Act of 1996 ("EEA") provides further protection.⁴⁷ The EEA expands the traditional scope of trade secret law beyond that which encompasses merely intellectual property concepts in prior common law or even those found in the Uniform Trade Secrets Act ("UTSA").⁴⁸ The requirements of value and secrecy have been expanded to include

all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, devices . . . whether tangible or intangible, and whether or how stored, compiled or memorialized.⁴⁹

The EEA has been criticized for going beyond the prohibition of: (1) taking or receiving trade secrets that are known to be protected because the party claiming the trade secret worked to maintain its secrecy; and (2) a taking that is merely unauthorized, without defining authorization. Although the EEA appears to focus on protecting trade secrets, it actually expands the traditional view of trade secrets to allocate control and use of other information. In other words, although a business's desks and chairs have been protected from being taken by others, its business information, such as business plans and mar-

keting strategy, had not been protected without a separate showing of secrecy and value. Since it was enacted, the EEA protects such information similarly to the way theft statutes protect equipment.

Colorado Security Statutes

Security is regulated at the federal level. However, there also is a wide variety of state legislation intended to control computer security. Two of these statutes are described below.

Colorado Computer Crime Act

The Colorado Computer Crime Act ("CCCA")⁵⁰ penalizes criminal activity perpetrated through the use of computers, as well as criminal activity that targets computers. It is illegal to knowingly use a computer for the purposes of fraud, obtaining money or services by fraud or false pretenses, or committing theft. It also is illegal to use, alter, or damage, knowingly and without authorization, any computer system, network, or data.

The unauthorized access to a computer and altering and deleting data from the computer, among other offenses, are grounds for disbarment of a Colorado Attorney General.⁵¹ The CCCA also would appear to provide some property rights (for example, the right to restrict access) in information to those who own the computer that stores and manipulates it.

Professional
Liability
Consultants, Inc.

Specializing in Legal Malpractice Insurance

with

Broad Coverages, Service & Affordability

Contact Sue Eppley, CIC, President

at

15593 E. Princeton Ave.

Aurora, CO 80013

Phone: 303-627-9002 or 800-491-5715

Fax: 303-627-9605

e-mail: PLCinc@attbi.com

Serving the Legal Community Since 1995

Colorado Theft of Trade Secret Act

Another Colorado statute that protects information is the Colorado Theft of Trade Secret Act,⁵² which protects information beyond that which is protected by common-law trade secret concepts. The definition of "trade secret" under the statute is relatively broad and includes business and financial information. Furthermore, it specifically identifies "... listing of names, addresses, or telephone numbers, or other information relating to any business or profession . . .," which includes customer lists, one of the most common sources of litigation. In litigation, the question remains whether the customer list has been maintained in a confidential manner.⁵³

Federal Privacy Statutes

Several statutes were enacted to protect the online privacy of businesses and individuals. These primarily deal with electronic mail and access to digitized private information.

Electronic Communications Privacy Act

The Electronic Communications Privacy Act ("ECPA")⁵⁴ brought electronic communications, such as electronic mail ("e-mail"), under its purview. An electronic communication is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted . . . by wire, . . . [or] radio . . . system that affects interstate or foreign commerce."⁵⁵ The ECPA is divided into two parts: one governs access to communications during transmission; the other governs access to stored communications.

Interception During Transmission: The first section of the ECPA makes illegal any "eavesdropping" on e-mail. It refers to "tapping" into a communication as it occurs. It is illegal for the government, businesses, or individuals to intentionally intercept any electronic communication or to intentionally disclose the illegally obtained contents of electronic communications.⁵⁶

However, providers of electronic communication services may intercept, disclose, or use the communication in the normal course of providing services when it is necessary to do so to render services or to protect their own rights or property.⁵⁷ System providers also are immunized from liability under the ECPA if they are cooperating with court or Attorney General-authorized investigations.⁵⁸ Finally, there is no li-

ability for intercepting e-mail if either the sender or recipient consents⁵⁹ or if the communication is publicly accessible.⁶⁰

Access to and Disclosure of Stored Communications: The second section of the ECPA is aimed at outside hackers. It prohibits intentional access without authorization, or in excess of authorization, of an electronic communication facility, and thereby obtaining, altering, or preventing authorized access to an electronic communication while it is being stored.⁶¹ Online system operators are authorized to access their own systems and e-mail stored therein. However, it also is illegal to disclose the contents of stored electronic communications, and this provision applies equally to outsiders and system providers.

Disclosure of the communication may be made to certain recipients and for various purposes. These include: (1) to the addressee; (2) with the sender or recipient's consent; (3) to an intermediary forwarding facility; (4) for debugging and administration purposes; (5) to protect the system provider's rights in the system; or (6) to law enforcement agencies, if the communication was inadvertently obtained by the system operator and appeared to pertain to the commission of a crime.⁶²

Intercepted Versus Stored Communications: Some argue that an e-mail that has not yet been read by the addressee is in transmission. Once that e-mail is read, if the recipient chooses to save the e-mail, it goes into storage. This distinction is critical because communications in transmission and in storage are given significantly different protection under the ECPA.⁶³

The question of what is a transmission under the ECPA was answered in the case of *Steve Jackson Games, Inc. v. The U.S. Secret Service*.⁶⁴ The plaintiff was a role-playing game publisher that operated a bulletin board service ("BBS") and provided its users e-mail services. The Secret Service seized the plaintiff's computer BBS, in which more than 100 unread e-mails were stored. One of the plaintiff's claims against the Secret Service was that it violated the ECPA by intercepting unread e-mail.

The court found that the seizure of the computer system did not constitute an interception of electronic communications, interpreting interception as "contemporaneous acquisition."⁶⁵ The court did, however, find the Secret Service liable for violating the second part of ECPA by accessing stored e-mail. The Secret Service, therefore, was held liable for violation of the Privacy Protection Act ("PPA"), discussed below.⁶⁶

Remedies: The party injured by violation of the ECPA may seek civil damages. The injured party may invoke the exclusionary rule⁶⁷ to prevent evidence illegally obtained by the government from being admitted in a criminal proceeding.⁶⁸

Privacy Protection Act

The PPA⁶⁹ prohibits government searches and seizures of publishing media "work product materials" and documents. This statute was enacted in response to U.S. Supreme Court decisions in the 1970s, which compelled some news disseminators to cooperate with law enforcement officials in connection with their investigations of crimes.⁷⁰

A government officer may not, in connection with a criminal investigation, search or seize work product materials or documentary materials of someone who is a news disseminator or publisher.⁷¹ The PPA's definition of "work product materials" includes notes, outlines, written descriptions of mental impressions and opinions, and equipment used to prepare and publish information. Documentary materials are those on which information is recorded, such as transcripts, negatives, photographs, audio- and videotapes, and disks.⁷² This protection does not apply when the news disseminator is the one under criminal investigation. Moreover, it does not apply when national security or human life is in danger.

Subpoenas: The PPA protects only against government searches and seizures accomplished under a search warrant. However, the government may subpoena publishing materials. Subpoenas give the publisher an opportunity to cooperate with the investigation and to challenge the subpoena in court before having to submit the subpoenaed materials.⁷³

Online Publishers: The publishing material protected under the PPA is broadly defined.⁷⁴ It encompasses "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 form of public communication."⁷⁵ Many traditional news providers (such as national magazines, local newspapers, and journals) also disseminate some work through online news services. These entities are clearly protected. *Steve Jackson Games*⁷⁶ establishes that even a BBS with relatively few subscribers is a "publisher" under the PPA, as long as the BBS and its files are used, as they invariably are, for public communication.

Publisher's Remedies: The aggrieved publisher may recover civil damages from the government for violation of the PPA. The publisher in *Steve Jackson Games* was awarded more than \$50,000 in damages.⁷⁷ However, the publisher may not invoke the exclusionary rule to suppress the wrongfully seized materials from being admitted in court as evidence.⁷⁸

The PPA grants greater property rights in certain kinds of information (that is, "work product materials") to reporters than is afforded to others with regard to other kinds of information.⁷⁹ It does this by restricting, beyond that which would normally be required, the government's right to seize such material.

General Review

The primary statutes described above focus on the nature of information that is to be protected. They define the property and who has the various property rights to use, exclude others from using, and transfer that property. Security statutes, such as the CFAA and CAD, proscribe behavior that would jeopardize privacy property and intellectual property.

As noted above, the first wave of property law concepts brought laws of estates in land, future interests, tenancies, trespass, breaking and entering, and others that explored how people relate with regard to real estate. The second wave brought laws related to bills of sale, commercial law, conveyance, theft, vandalism, and others that explored how people relate with regard to chattels. The current, third wave of property law concepts brings laws restricting computer access, standards for copying of content, rules for handling personal information, and means for controlling computer viruses, as well as other laws that explore how people relate with regard to information.⁸⁰

This third wave is demonstrated well by the EEA, which first expanded the concepts of confidential relationships that move property in the form of secret things of value to property that may be of questionable value (such as customer lists or financial information) and, finally, to information that might not even be secret. This law has provided an increase in remedies as well.⁸¹

The EEA, perhaps more than any other statute, shows the growing relationship

between privacy and security and between confidential relationship and property protection. A similar analysis could be used in connection with the application of the CFAA to computer networks. Concepts of authority or scope of authority imply right to control and, therefore, the right to permit others to use information.

A number of specific cases have examined these questions. A growing body of law is developing concerning the information provided by a person's Web browsing.⁸² Some of the cases that have determined the rights relate to "cookies."⁸³ The same discussion occurs in the cases that try to determine which aspects of an employee's knowledge is a protected trade secret of the employer and which are the knowledge and life experience of the employee who is free to take to another job.⁸⁴

A simple set of questions that should be useful in analyzing any security or privacy issue follows:

- Who should have control of the information in question?
- Who should have control of the access points to reach information?
- What type of control should the "owner" of the access or information have

INTRODUCING

www.colorado-appealsblog.com

Keeping you informed

on the latest decisions and other news

from the

Colorado State Appellate Courts



Blain Myhre,

Chair of the Appellate Practice Group

IRWL

ISAACSON ROSENBAUM

WOODS & LEVY, P.C.

law-client-community®



JOHN A. CRISWELL

ARBITRATION AND MEDIATION SERVICES

IN

LABOR AND EMPLOYMENT DISPUTES

- Senior Judge, Colorado Court of Appeals
- 25 years' experience in prosecuting and defending employment claims
- Hearing Officer for Denver Civil Service and Colorado Judicial Department
- American Arbitration Association's Employment Arbitrators Panel

1045 Lincoln Street, Suite 201

Denver, Colorado 80203

Tel: 303-864-1664

Fax: 303-837-1622

E-mail: CRISWELL1956@AOL.COM

and to what extent should that person exert it?

- What kinds of access and information should be in the public domain?
- Under what circumstances should control be transferred or relinquished?

Rather than focusing the discussion on “spying” and “Big Brother,” it may be more useful to center the discussion on who should have the right to control the use, preservation, and exclusiveness of specific kinds of information and who should have the right to transfer those rights to others. Consistent rules could develop and gain consensus if more effort was spent discussing whether information should float within society or be controlled by specific people or companies—and with whom the control should reside. Security and privacy are not only about safety and confidentiality. They also are about property rights.

Conclusion

When approached by a client to plan a transaction requiring designating control of the use and transfer of information, many practitioners have come to expand their consideration of contract law to principles related to licensing. Governments, individuals, and businesses are increasingly working to control information, even information that is not subject to intellectual property law, which has a long history of controlling works of the mind. Now, practitioners should add consideration of security and privacy principles to their repertoire of techniques for advising their clients regarding issues related to controlling information. In the context of the third wave of control—as property rights are attributed to information itself—it is important to keep an open mind and consider this alternative to traditional practice.

NOTES

1. More than 200 new security laws have been enacted since the events of September 11, 2001. Keynote Address of Valerie McNevin, then Security-Privacy Officer for the state of Colorado, to the ITEC Conference (Fall 2002). Also, in a study of health-care privacy laws conducted by the author (2000), it was estimated that approximately 250 such laws exist that are just related to health care. Therefore, many statutes relating to security and privacy, such as The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub.L. No. 107-56, 115 Stat.

272 (codified in scattered sections of the U.S. Code: 5, 8, 10, 12, 15, 16, 18, 21, 22, 28, 31, 42, 47, 49, and 50), are beyond the scope of this article.

2. Definition can be found under “Property Law,” *Encyclopedia Britannica* (CD-ROM) (2003).

3. Warren and Brandeis, “The Right to Privacy,” 4 *Harv. L.Rev.* 193 (1890).

4. *Interstate Commerce Comm’n v. Brimson*, 154 U.S. 447, 489 (1894).

5. *Union Pac. Ry. Co. v. Botsford*, 141 U.S. 250, 251 (1891).

6. *Goldman v. U.S.*, 316 U.S. 129, 137 (1942).

7. Samuelson, “Information as Property: Do *Ruckelshaus* and *Carpenter* Signal a Changing Direction in Intellectual Property Law?” 38 *Cath. U.L.Rev.* 365, 374 (1989).

8. See, e.g., *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986 (1984); *Carpenter v. U.S.*, 484 U.S. 19 (1987). See also note 7, *supra*.

9. *Chance v. Avenue A, Inc.*, 165 F.Supp.2d 1153 (2001). A “cookie” is a small file that is sometimes transmitted to a user’s computer when the user requests access to a website. These files identify the user and can store additional information.

10. *Chance, supra*, note 9.

11. 18 U.S.C. § 1030.

12. 18 U.S.C. § 1030(e)(1).

13. See note 1, *supra*, for a citation to the USA PATRIOT Act.

14. 18 U.S.C. § 1030(e)(2)(B).

15. 15 U.S.C. §§ 78 *et seq.*

16. 18 U.S.C. § 1030(e)(4).

17. 18 U.S.C. § 1030(e)(6).

18. 18 U.S.C. § 1030(e)(11).

19. 18 U.S.C. § 1030(a).

20. 42 U.S.C. § 2014(y).

21. 18 U.S.C. § 1030(a)(1).

22. 18 U.S.C. § 1030(a)(2).

23. 18 U.S.C. § 1030(a)(3).

24. *Id.*

25. 18 U.S.C. § 1030(a)(4).

26. *Id.*

27. 18 U.S.C. § 1030(a)(5)(A)(i).

28. 18 U.S.C. § 1030(a)(5)(A)(ii).

29. 18 U.S.C. § 1030(a)(5)(A)(iii).

30. 18 U.S.C. § 1030(c).

31. 18 U.S.C. § 1030(a)(5)(B)(ii)-(v).

32. 18 U.S.C. § 1030(a)(5).

33. 18 U.S.C. § 1030(a)(5)(A).

34. 18 U.S.C. § 1030(a)(6).

35. 18 U.S.C. § 1030(a)(7).

36. 18 U.S.C. § 1030(c)(1)(A).

37. 18 U.S.C. § 1030(c)(1)(B).

38. 18 U.S.C. § 1029.

39. 18 U.S.C. § 1029(e).

40. 18 U.S.C. § 1029(a).

41. 18 U.S.C. § 1029(a)(3).

42. 18 U.S.C. § 1029(a)(8).

43. 18 U.S.C. § 1029(e)(1).

44. 18 U.S.C. § 1029(e)(2).

45. 18 U.S.C. § 1029(e)(6).

46. 18 U.S.C. § 1029(e)(3).

47. EEA, Pub.L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831-1839).

48. UTSA §§ 1-12, 14 U.L.A. 433-67 (1990).

49. 18 U.S.C. § 1839(3).

50. CRS §§ 18-5-5-101 *et seq.*

51. See, e.g., *People v. Brown*, 726 P.2d 638 (1986).

52. CRS § 18-4-408.

53. CRS § 18-4-408(2)(d).

54. ECPA, Pub.L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2522 and 2701-2711).

55. 18 U.S.C. § 2510(12).

56. 18 U.S.C. § 2511(2)(a)(i).

57. 18 U.S.C. § 2511(2)(a)(ii)(B).

58. 18 U.S.C. § 2511(2)(c).

59. *Id.*

60. 18 U.S.C. § 2511(2)(g)(i).

61. 18 U.S.C. § 2701.

62. 18 U.S.C. § 2511(3).

63. See, e.g., *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (2002).

64. *Steve Jackson Games, Inc.*, 816 F.Supp. 432 (W.D.Tex. 1993).

65. *Id.* at 442.

66. PPA, Pub.L. No. 96-4401, 94 Stat. 1879 (1980) (codified as amended at 42 U.S.C. § 2000aa-2000aa-12).

67. 18 U.S.C. § 2518.

68. 18 U.S.C. § 2520.

69. See PPA, *supra*, note 66.

70. See, e.g., *Branzburg v. Hayes*, 408 U.S. 665 (1972) (First Amendment does not create privilege protecting press from subpoenas seeking identity of confidential sources); *Zurcher v. Stanford Daily News*, 436 U.S. 547 (1978) (First Amendment does not preclude use of search warrants to obtain evidence from newspaper reporter who has witnessed a suspected crime).

71. 42 U.S.C. § 2000aa(a).

72. 42 U.S.C. § 2000aa-7(a).

73. 42 U.S.C. § 2000aa5-7.

74. 42 U.S.C. § 2000aa-7(b).

75. *Id.*

76. *Steve Jackson Games, supra*, note 64.

77. *Id.* at 441.

78. 42 U.S.C. § 2000aa(c).

79. 42 U.S.C. § 2000aa(a).

80. A compendium of many of the types of property constituting the third wave can be found in Branscomb, *Who Owns Information? From Privacy to Public Access* (New York, NY: HarperCollins, 1994), which chronicles the types of information that have acquired the same status as property.

81. See Berkowitz, “The Economic Espionage Act of 1996: An Experiment in Unintended Consequences?” 26 *The Colorado Lawyer* 47 (Dec. 1997).

82. E.g., *In re Doubleclick Inc. Privacy Litigation*, 154 F.Supp.2d 497 (2001).

83. See *Chance* and a description of “cookies” in note 9, *supra*.

84. *Julius Hyman & Co. v. Velsicol Corp.*, 233 P.2d 977 (Colo. 1951).