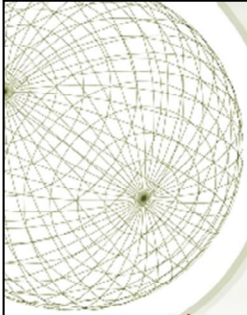


Fundamental Concepts of Data Security

Ethics



COMMONWEALTH OF AUSTRALIA

Copyright Regulation 1969

WARNING

This material has been copied and communicated to you by
or on behalf of Curtin University of Technology pursuant
to Part VB of the Copyright Act 1968 (the Act)

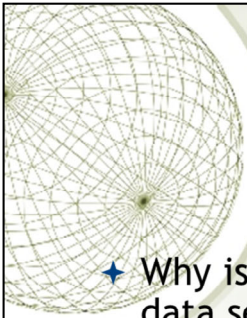
The material in this communication may be subject to
copyright under the Act. Any further copying or
communication of this material by you may be the
subject of copyright protection under the Act.

Do not remove this notice



Outline

- ✦ Ethics and laws
- ✦ Policy enforcement
- ✦ Ethics and professional organisations
- ✦ Preventing unethical behaviour
- ✦ Ethical issues



Ethics and Data Security

- ★ Why is ethics important from the point of view of data security?
 - ★ It is critical to understand the ethical responsibilities of your work as you will be dealing with privacy and secrecy issues in a large part of your work.
- ★ All security setups and incident investigations have a legal and ethical components.
- ★ How you deal with the ethical component of your work is crucial as it can increase the liability of both the organization that employs you and yourself.
- ★ Organizations should demand that the employees have a strong ethical behaviour.

4

As a future information security professional, you must understand the scope of an organization's legal and ethical responsibilities. The information security professional plays an important role in an organization's approach to managing liability for privacy and security risks. In the modern litigious societies of the world, sometimes laws are enforced in civil courts, where large damages can be awarded to plaintiffs who bring suits against organizations. Sometimes these damages are punitive—assessed as a deterrent. To minimize liability and reduce risks from electronic and physical threats, and to reduce all losses from legal action, information security practitioners must thoroughly understand the current legal environment, stay current with laws and regulations, and watch for new and emerging issues. By educating the management and employees of an organization on their legal and ethical obligations and the proper use of information technology and information security, security professionals can help keep an organization focused on its primary objectives.

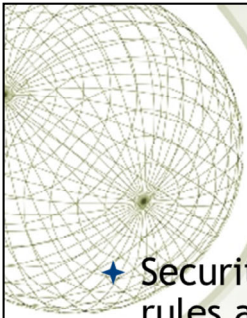
Law and Ethics in Information Security

In general, people elect to trade some aspects of personal freedom for social order. As Jean- Jacques Rousseau explains in *The Social Contract*, or *Principles of Political Right*, the rules the members of a society create to balance the individual rights to self-determination against the needs of the society as a whole are called laws. Laws are rules that mandate or

prohibit certain behavior; they are drawn from ethics, which define socially acceptable behaviors. The key difference between laws and ethics is that laws carry the authority of a governing body, and ethics do not. Ethics in turn are based on cultural mores: the fixed moral attitudes or customs of a particular group. Some ethical standards are universal. For example, murder, theft, assault, and arson are actions that deviate from ethical and legal codes throughout the world.

Organizational Liability and the Need for Counsel

What if an organization does not demand or even encourage strong ethical behavior from its employees? What if an organization does not behave ethically? Even if there is no breach of criminal law, there can still be liability. Liability is the legal obligation of an entity that extends beyond criminal or contract law; it includes the legal obligation to make restitution, or to compensate for wrongs committed. The bottom line is that if an employee, acting with or without the authorization of the employer, performs an illegal or unethical act that causes some degree of harm, the employer can be held financially liable for that action. An organization increases its liability if it refuses to take measures known as due care. Due care standards are met when an organization makes sure that every employee knows what is acceptable or unacceptable behavior, and knows the consequences of illegal or unethical actions. Due diligence requires that an organization make a valid effort to protect others and continually maintains this level of effort. Given the Internet's global reach, those who could be injured or wronged by an organization's employees could be anywhere in the world. Under the U.S. legal system, any court can assert its authority over an individual or organization if it can establish jurisdiction—that is, the court's right to hear a case if a wrong is committed in its territory or involves its citizenry. This is sometimes referred to as long arm jurisdiction—the long arm of the law extending across the country or around the world to draw an accused individual into its court systems. Trying a case in the injured party's home area is usually favorable to the injured party.



Ethics and Data Security

- ✦ Security setup, as mentioned before, specifies the rules and procedures which ultimately determine the behaviour of employees.
- ✦ A computer security professional maintains security by developing and helping with the implementation of security policies.
- ✦ The security policies are enforceable when the following requirements are met:
 - 1) the policy has been communicated to all staff
 - 2) the policy is easily comprehended by all staff
 - 3) compliance with the policy is agreed with by the staff
 - 4) the enforcement is uniform and consistent

5

Within an organization, information security professionals help maintain security via the **establishment and enforcement of policies**. These policies—guidelines that describe acceptable and unacceptable employee behaviors in the workplace—function as organizational laws, complete with penalties, judicial practices, and sanctions to require compliance. Because these policies function as laws, they must be crafted and implemented with the same care to ensure that they are complete, appropriate, and fairly applied to everyone in the workplace. The difference between a policy and a law, however, is that ignorance of a policy is an acceptable defense. Thus, for a policy to become enforceable, it must meet the following five criteria

•**Dissemination (distribution)**—The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.

•**Review (reading)**—The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading, and reading-impaired employees. Common techniques include recordings of the policy in English and alternate languages.

•**Comprehension (understanding)**—The organization must be able to demonstrate that the employee understood the requirements and content of the policy. Common techniques include quizzes and other assessments.

•**Compliance (agreement)**—The organization must be able to demonstrate that the employee agreed to comply with the policy through act or affirmation.

Common techniques include logon banners, which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.

•**Uniform enforcement**—The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.



Ethics and Professional Organizations

- ✦ There is no universal binding ethics code for computer security professionals.
- ✦ Different international professional organizations (ACM, IEEE, SANS, ISACA) provide their own guidelines on ethical behaviour.
- ✦ The Australian Computer Society (ACS) has its own recommendations on ethics.

6

Codes of Ethics and Professional Organizations

A number of professional organizations have established codes of conduct or codes of ethics that members are expected to follow. Codes of ethics can have a positive effect on people's judgment regarding computer use. Unfortunately, many employers do not encourage their employees to join these professional organizations. But employees who have earned some level of certification or professional accreditation can be deterred from ethical lapses by the threat of loss of accreditation or certification due to a violation of a code of conduct. Loss of certification or accreditation can dramatically reduce marketability and earning power.

It is the responsibility of security professionals to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society. It is likewise the organization's responsibility to develop, disseminate, and enforce its policies.

Major IT Professional Organizations

Many of the major IT professional organizations maintain their own codes of ethics. The Association of Computing Machinery (ACM) (www.acm.org) is a respected professional society that was established in 1947 as "the world's first educational and scientific computing society." It is one of the few organizations that strongly promotes education and provides

discounts for student members. The ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional. The code contains specific references to protecting the confidentiality of information, causing no harm (with specific references to viruses), protecting the privacy of others, and respecting the intellectual property and copyrights of others. The ACM also publishes a wide variety of professional computing publications, including the highly regarded Communications of the ACM.

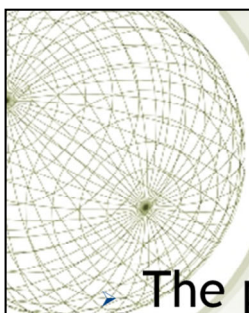
The International Information Systems Security Certification Consortium, Inc. (ISC)2 (www.isc2.org) is a nonprofit organization that focuses on the development and implementation of information security certifications and credentials. The (ISC)2 manages a body of knowledge on information security and administers and evaluates examinations for information security certifications. The code of ethics put forth by (ISC)2 is primarily designed for information security professionals who have earned an (ISC)2 certification, and has four mandatory canons: "Protect society, the commonwealth, and the infrastructure; act honorably, honestly, justly, responsibly, and legally; provide diligent and competent service to principals; and advance and protect the profession." This code enables (ISC)2 to promote reliance on the ethicality and trustworthiness of the information security professional as the guardian of information and systems.

The System Administration, Networking, and Security Institute (SANS) (www.sans.org), which was founded in 1989, is a professional research and education cooperative organization with a current membership of more than 156,000 security professionals, auditors, system administrators, and network administrators. SANS offers a set of certifications called the Global Information Assurance Certification, or GIAC. All GIAC-certified professionals are required to acknowledge that certification and the privileges that come from it carry a corresponding obligation to uphold the GIAC Code of Ethics. Those certificate holders that do not conform to this code face punishment, and may lose GIAC certification.

The Information Systems Audit and Control Association (ISACA) (www.isaca.org) is a professional association that focuses on auditing, control, and security. The membership comprises both technical and managerial professionals. ISACA provides IT control practices and standards, and although it does not focus exclusively on information security, it does include many information security components within its areas of concentration. ISACA also has a code of ethics for its professionals, and it requires many of the same high standards for ethical performance as the other organizations and certifications.

The Information Systems Security Association (ISSA) (www.issa.org) is a nonprofit society of information security professionals. As a professional association, its primary mission is to bring together qualified information security practitioners for information exchange and educational development. ISSA provides a number of

scheduled conferences, meetings, publications, and information resources to promote information security awareness and education. ISSA also promotes a code of ethics, similar in content to those of (ISC)2, ISACA, and the ACM, whose focus is “promoting management practices that will ensure the confidentiality, integrity, and availability of organizational information resources.”



ACS Code of Ethics

- The primacy of the public interest
- The enhancement of quality of life
- Honesty
- Competence
- Professional development
- Professionalism

<https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Ethics.pdf>

7

The ACS Code of Professional Conduct as from

https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Professional-Conduct_v2.1.pdf

1. The Primacy of the Public Interest

You will place the interests of the public above those of personal, business or sectional interests.

2. The Enhancement of Quality of Life

You will strive to enhance the quality of life of those affected by your work.

3. Honesty

You will be honest in your representation of skills, knowledge, services and products.

4. Competence

You will work competently and diligently for your stakeholders.

5. Professional Development

You will enhance your own professional development, and that of your staff.

6. Professionalism

You will enhance the integrity of the ACS and the respect of its members for

Interest takes precedence over the other values.

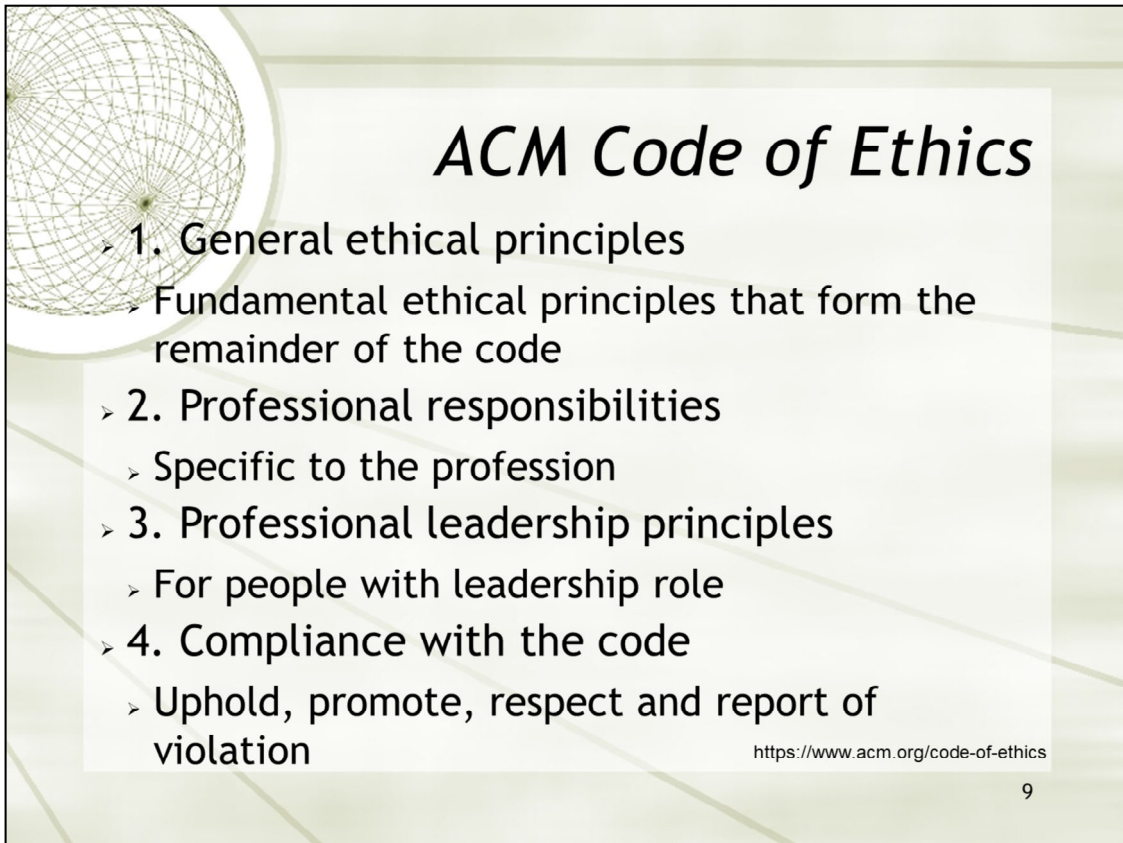


Computer Ethics Institute

★ Ten commandments:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

<https://www.computerethicsinstitute.org/ten-commandments-of-computer-ethics.pdf>

A presentation slide titled "ACM Code of Ethics". On the left, there is a decorative graphic of a wireframe sphere. The title is in a large, bold, black serif font. Below the title is a bulleted list with four main items, each preceded by a right-pointing arrow. The first item is "1. General ethical principles", followed by a sub-bullet "Fundamental ethical principles that form the remainder of the code". The second item is "2. Professional responsibilities", followed by a sub-bullet "Specific to the profession". The third item is "3. Professional leadership principles", followed by a sub-bullet "For people with leadership role". The fourth item is "4. Compliance with the code", followed by a sub-bullet "Uphold, promote, respect and report of violation". At the bottom right of the slide, there is a small URL "https://www.acm.org/code-of-ethics" and a page number "9".

ACM Code of Ethics

- 1. General ethical principles
 - Fundamental ethical principles that form the remainder of the code
- 2. Professional responsibilities
 - Specific to the profession
- 3. Professional leadership principles
 - For people with leadership role
- 4. Compliance with the code
 - Uphold, promote, respect and report of violation

<https://www.acm.org/code-of-ethics>

9

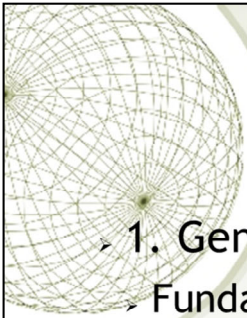
The ACM code of ethics as from

<https://www.acm.org/code-of-ethics>

<https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-booklet.pdf>

Consists of four sections

- Section 1 outlines general ethical principles that form the basics of the code
- Section 2 is about general professional responsibilities
- Section 3 provides guidance for individuals in a leadership position
- Section 4 is about compliance



IEEE Code of Ethics

- 1. General ethical principles
 - Fundamental ethical principles that form the remainder of the code
- 2. Professional responsibilities
 - Specific to the profession
- 3. Professional leadership principles
 - For people with leadership role
- 4. Compliance with the code
 - Uphold, promote, respect and report of violation

<https://www.ieee.org/about/corporate/governance/p7-8.html>

10

The IEEE code of ethics as from

<https://www.ieee.org/about/corporate/governance/p7-8.html>

1. to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, and to disclose promptly factors that might endanger the public or the environment;

2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;

3. to be honest and realistic in stating claims or estimates based on available data;

4. to reject bribery in all its forms;

5. to improve the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies, including intelligent systems;

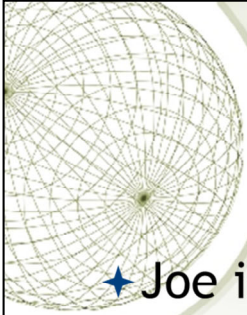
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;

7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;

8. to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression;

9. to avoid injuring others, their property, reputation, or employment by false or malicious action;

10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics



ACS Case Study

★ Joe is working on a project for his computer science course. The instructor has allotted a fixed amount of computer time for this project. Joe has run out of time, but has not yet finished the project. The instructor cannot be reached. Last year Joe worked as a student programmer for the campus computer centre and is quite familiar with procedures to

ACS Case Study No. 9 for discussion in class

ACS Code of Professional Conduct values and relevant clauses of the Code of Professional Conduct

1.2.1 Public Interest

a) identify those potentially impacted by your work and explicitly consider their interests;

1.2.4 Competence

f) accept responsibility for your work;

1.2.6 Professionalism

f) refrain from any conduct or action in your professional role which may tarnish the image of the profession or detract from the good name of the ACS;



Ethics and Ethical Behaviour

- ✦ Ethics and ethical behaviour vary depending on the country or culture that one has interaction with.
- ✦ This is a significant problem especially when attempting to handle groups across area with different ethical expectations and enforcement mechanisms.
- ✦ Education and training are key in reducing unethical behaviour.
- ✦ Causes of unethical behaviour:
 - 1) Ignorance
 - 2) Accident
 - 3) Intent

12

Ethical Differences Across Cultures

Cultural differences can make it difficult to determine what is and is not ethical—especially when it comes to the use of computers. Studies on ethics and computer use reveal that people of different nationalities have different perspectives; difficulties arise when one nationality's ethical behavior violates the ethics of another national group. For example, to Western cultures, many of the ways in which Asian cultures use computer technology is software piracy. This ethical conflict arises out of Asian traditions of collective ownership, which clash with the protection of intellectual property. Approximately 90 percent of all software is created in the United States. Some countries are more relaxed with intellectual property copy restrictions than others.

Ethics and Education

Attitudes toward the ethics of computer use are affected by many factors other than nationality. Differences are found among individuals within the same country, within the same social class, and within the same company. Key studies reveal that the overriding factor in leveling the ethical perceptions within a small population is education. Employees must be trained and kept aware of a number of topics related to information security, not the least of which are the expected behaviors of an ethical employee. This is especially important in information security, as many employees may not have the formal technical training to understand that

their behavior is unethical or even illegal. Proper ethical and legal training is vital to creating an informed, well prepared, and low-risk system user.

Deterring Unethical and Illegal Behavior

There are three general causes of unethical and illegal behavior:

- Ignorance**—Ignorance of the law is no excuse; however, ignorance of policy and procedures is. The first method of deterrence is education. This is accomplished by means of designing, publishing, and disseminating organization policies and relevant laws, and also obtaining agreement to comply with these policies and laws from all members of the organization. Reminders, training, and awareness programs keep the policy information in front of the individual and thus better support retention and compliance.

- Accident**—Individuals with authorization and privileges to manage information within the organization are most likely to cause harm or damage by accident. Careful planning and control helps prevent accidental modification to systems and data.

- Intent**—Criminal or unethical intent goes to the state of mind of the person performing the act; it is often necessary to establish criminal intent to successfully prosecute offenders. Protecting a system against those with intent to cause harm or damage is best accomplished by means of technical controls, and vigorous litigation or prosecution if these controls fail.



Preventing Unethical Behaviour

- ★ The computer security professionals have a responsibility to prevent unethical or illegal behaviour.
- ★ Deterrence can be enhanced if there is a concerted effort to highlight through training the type of behaviour that is unacceptable and the consequences of such behaviour, specifically one needs to ensure that:
 - 1) the penalty is appropriate to discourage repeat offending
 - 2) the likelihood that the offence is detected is high
 - 3) the enforcement of the penalties is carried out according to the security policy

13

Whatever the cause of illegal, immoral, or unethical behavior, one thing is certain: it is the responsibility of information security personnel to do everything in their power to deter these acts and to use policy, education and training, and technology to protect information and systems. Many security professionals understand the technology aspect of protection but underestimate the value of policy. However, laws and policies and their associated penalties only deter if three conditions are present:

- Fear of penalty**—Potential offenders must fear the penalty. Threats of informal reprimand or verbal warnings may not have the same impact as the threat of imprisonment or forfeiture of pay.
- Probability of being caught**—Potential offenders must believe there is a strong possibility of being caught. Penalties will not deter illegal or unethical behavior unless there is reasonable fear of being caught.
- Probability of penalty being administered**—Potential offenders must believe that the penalty will in fact be administered.



Ethical Issues

- 1) Security rights
- 2) Hackers
- 3) Domains
- 4) Illegal Downloading of Material

14

The term “security” is something of a catch-all term. In its broadest use, the term connotes nothing more specific than “freedom from danger,” but “danger” itself is a broad term appropriately used to characterize any serious threat to a morally significant interest. On this usage, then, any law that protects life, liberty, or property is fairly characterized as attempting to ensure a person’s “security.”

We are of course concerned only with legal and ethical issues as they arise in connection with computer security, “computer security” being construed to mean “freedom from unauthorized computer intrusions.” Accordingly, this section is concerned with legal protections against unauthorized computer intrusions, the justification for such protection, and the challenge posed to such justifications by hackers.

Security from unauthorized computer intrusions has become a priority for lawmakers. Most, if not all, developed nations have laws prohibiting unauthorized computer intrusions.

Security Rights

At first glance, laws prohibiting unauthorized computer intrusions seem easy to justify on ethical grounds. Although the more malicious intrusions involve serious ethical transgressions because of the harm they are

intended to cause, all seem morally objectionable for two reasons. First, they appear to constitute an electronic form of trespass onto the physical property of another person. To obtain unauthorized entry into some other person's network or computer seems, from an ethical perspective, straightforwardly analogous to uninvited entry onto the real property of another person. Even if it turns out that there are no natural moral rights to intellectual property, it seems clear that persons have property rights in their computers and networks (which are, after all, material objects and not intellectual objects). Such trespass is widely regarded as morally wrong, regardless of whether it results in damage or harm, because it violates the property right of the owner to control the uses to which his or her property is put and hence to exclude other people from its use. Similarly, hacking into someone else's computer or network is wrong, regardless of whether it results in damage, because it violates the owner's property right to exclude others from using his or her computer or network equipment.

Second, such computer intrusions seem to violate the legitimate privacy rights of the victims. If it is true that persons have a property right in their physical hardware, then it is reasonable to think that they have privacy rights in the documents and files they store on that hardware. If I know that I may legitimately exclude you from appropriating my computer, then I have a reasonable expectation that I may exclude you from the files and documents that I store on my hard drive. On this second line of reasoning, hacking into someone else's hardware is wrong because it violates the legitimate privacy expectations of the owners. This is true regardless of whether owners actually store sensitive information on those machines: breaking into my home involves a violation of my privacy even if the perpetrator acquires no private information about me.

It is worth noting here that considerations having to do with the legitimacy of intellectual property rights do not play a general role in justifying laws prohibiting unauthorized computer intrusions. The reason for this is that unauthorized intrusions need not involve infringement on those interests protected by intellectual property law; there is nothing in the nature of such an intrusion that entails, say, the infringement of interests that are protected by a patent or by trademark law. In contrast, unauthorized computer intrusions seem, by definition, to impinge on someone's property rights in their computer hardware and hence on reasonable privacy expectations.

Hackers

There are a growing number of well-publicized incidents in which hackers obtain unauthorized entry into a firm's or state agency's servers. Some of these incidents involve comparatively innocuous exploration of a network's structure; in such cases, hackers look around and leave without altering the system. Others involve the commission of computer pranks; one such famous incident involved an insulting message left by hackers on the New York Times Web site (see, e.g., Nutall, 1998). Yet others involve the commission of cyberterrorism that threatens

national security, as when a hacker breaks into a government network that stores classified material, or individual wellbeing, as when a hacker breaks into a corporate server and takes credit card and bank account numbers.

Many hackers reject the claim that all unauthorized computer intrusions can legitimately be prohibited to protect moral interests in property and privacy, arguing that some hacking activity can be justified in terms of its social benefits, at least when it results in no damage or harm to innocent persons. These computer intrusions, they point out, contribute to increasing our technological knowledge in a number of ways. First, by gaining insight into the operations of existing networks, hackers develop a base of knowledge that can be used to improve those networks. Second, the very break-ins themselves call attention to security flaws that could be exploited by malicious hackers or, worse, terrorists. Thus, electronic trespass is distinguished, according to proponents, from other forms of trespass in that it inevitably conduces to public benefit.

Certain hacking activities have also been defended as a form of free expression in two ways. First, the permissibility of benign break-ins appears to be a consequence of the claim that “information wants to be free.” If it is true, as an ethical matter, that all information should be free, then security measures designed to keep hackers out of networks are morally objectionable on the ground that they inhibit the free flow of information. Second, some writers have argued that benign break-ins can be defended as a form of protest or political activism (“hacktivism”). On this line of reasoning, such incidents express legitimate outrage over the increasing commercialization of the Web. Politically motivated hacking, according to these writers, should be permitted as long as it results in neither harm nor profit.

Domain Names.

Every computer on a network has its own Internet protocol (IP) address consisting in a unique sequence of numbers and dots (e.g., 213.57.66.938) that defines its location on the Web. When a user accesses a particular Web site, the contents of that site are sent from the host server’s IP address to the IP address of the user’s computer. In effect, then, IP addresses make it possible for networked computers to find each other, enabling users to access the contents of Web sites hosted at other locations on the network.

In most cases, users need not know a complicated IP address to access a Web site. Most Web sites have a natural language domain name (e.g., <http://www.sporting-goods.com>) assigned to their IP addresses that permits easier and more intuitive access to their contents. The user simply types in the natural language domain name, and the ISP either looks for the corresponding IP address or submits a request to a “root server” that serves as a digital directory

associating IP addresses and domain names. Once the ISP has determined the corresponding IP address, the desired site is accessed.

Domain names can be valuable commodities. An intuitive domain name saves consumers time and energy; it is much easier to find a site with an intuitive domain name than with a long IP address that is difficult to find and remember. The resulting convenience to users can naturally translate into economic benefits; the easier it is to access a commercial Web site, the more likely users are to visit and buy from that site.

In consequence, there have been conflicts over the use and ownership of domain names. Early in the development of the Web, some people registered domain names featuring the trademarked names of large firms in the hope that the firms would buy those names whenever they decided to go online. Although a few such “cyber-squatters” made a quick profit for their trouble, courts now treat the practice of speculating on domain names incorporating trademarks as actionable trademark infringement (see, e.g., *Panavision v. Toeppe*, 1998).

More commonly, a slightly modified version of a popular Web site’s domain name is used to capture some of its traffic. One commercial pornographic Web site in the United States, for example, uses the domain name “www.whitehouse.com.” Users who type “www.whitehouse.com” instead of “www.whitehouse.gov” into their browsers—a common mistake—will access sexually explicit material instead of the U.S. president’s official Web site. By such means, a person can dramatically increase traffic to his or her site.

Although such practices appear deceptive, they can facilitate legitimate purposes of free expression. A user who mistakenly types “www.gwbush.com” instead of “www.georgebush.com” will access a site criticizing George Bush’s views and policies instead of his personal Web site. While the commercial use of a domain name similar to a trademarked name can dilute the value of the trademark and is hence unethical, the politically motivated use of a domain name to express legitimate criticism is arguably unobjectionable—as long as users are not likely to be confused about the origin of the site.

Illicit Copying Over the Internet

No case better exemplifies the clash between the intellectual property rights of copyright holders and the increasingly libertarian spirit of online users than the proliferation of MP3 file sharing over the Web. The development of the MP3 format was the first significant step in realizing the Internet’s latent potential for online dissemination of music files. Earlier technologies offered little incentive to share music files; the files were too large to be uploaded and downloaded quickly, and their sound quality was generally inconsistent. MP3 technology, however, permits the compression of nearly perfect digital reproductions of sound

recordings into small files that are efficiently transmitted from one user to another.

Napster augmented MP3's capabilities by introducing true peer-to-peer (P2P) file sharing. Whereas users of earlier file-sharing technologies had to download previously uploaded files from a central Web site or file transfer protocol (FTP) site, Napster users could simply take music files directly from the computers of other users. Although a central server was needed to keep a searchable list of all the available MP3 files, its purpose was limited to helping Napster users find each other. Because users could share music files online without anyone needing to take the time to upload music files to some central server, Napster made it easier than ever before for large groups of users to share their sound recordings. Napster's P2P networking capabilities also inhibited the efforts of recording companies to stop reproduction and distribution of their copyrighted materials. When music files had to be transmitted through a central server, recording companies could demand that the server's owner destroy copyrighted files or litigate an expensive civil suit. Because Napster eliminated the need for centralized storage of such files, however, there was no one entity that could be pressured by copyright holders. Not surprisingly, the music industry viewed Napster as a grave threat to the value of its copyrights. The conflict came to a head when a group of music companies sued Napster for "indirect" violations of U.S. copyright law. Because Napster's role was limited to enabling users of Napster's MusicShare software to gain access to the hard drives of other users, the company could not be held liable for direct infringements. Instead, the plaintiffs sought to hold Napster liable for contributory infringement (i.e., knowingly assisting others in directly infringing a copyright) and vicarious infringement (i.e., benefiting financially from infringements when it has the ability to supervise and terminate users). Although the litigation did not settle the legal issues, it resulted in a preliminary injunction forcing Napster off the Web temporarily. A U.S. federal court issued an injunction prohibiting Napster from assisting users in sharing copyrighted materials without the express permission of the owners (*A&M Records v. Napster*, 2000). The court based its injunction on a prediction (as opposed to a final judgment) that Napster would lose at trial because (a) users were deriving an unfair economic benefit from using Napster by saving the cost of the relevant recordings and (b) Napster use was decreasing CD sales among users (*Napster*, 2000 at 1017). Napster recently returned to the Web offering music downloads for sale after negotiating contract agreements with five major record labels and hundreds of independent labels (see <http://www.napster.com/about us.html>).

Because the litigation never resulted in a final judgment on the issue of file sharing, music-sharing technologies and Web sites have continued to proliferate,¹⁸ apparently cutting into industry profits by reducing CD sales ("Downloads Blamed," 2002). In a controversial response, the Recording Industry Association of America recently started suing individuals, instead of music-sharing Web sites, for making music files available on these sites ("Recording Industry Begins Suing," 2003; "RIAA Strikes Back," 2003). These lawsuits have targeted not only adult users, but

also the parents and grandparents of children users (RIAA Leaning on Kids' Parents, 2003). Although such tactics have been passionately criticized, they seem to have succeeded, according to recent reports, in reducing illegal file sharing—at least temporarily (Borland, 2003).



Ethical Issues

- 5) Private vs public information
- 6) Commercial collection of personal information
- 7) Misuse of corporate resources
- 8) Software piracy

15

Public and Private Information

The general claim that personal information ought to be protected by law does not, by itself, tell us much about how to determine what information about a person deserves legal privacy protection. For example, the altogether plausible consequentialist claim that protection of information is justified by a personal need to control the structure of various social relationships says little as to what information about a person ought to be protected by the law. For this reason, general justifications of privacy rights, such as those discussed in the last section, represent only a starting point in determining what content privacy law ought to have.

It is reasonable to think that whether a person ought to have a protected privacy right in a piece of information depends in part on the character of that information. Some facts about a person are generally accepted as private facts in which a person has a legitimate expectation of privacy. Because, for example, I am entitled to draw my drapes to prevent people from viewing what is going on in my home, the facts about what is going on in my home are private—at least when the drapes are drawn and my behavior is lawful. Thus, I have a legitimate expectation of privacy in aspects of my behavior that I may rightfully prevent people from viewing; these aspects of my behavior define private facts.

Some facts, however, should be regarded as private in virtue of their intimate character. It is almost universally accepted that certain physical functions, such as those involving the sexual and excretory organs, express private facts because of their felt intimate character. Information regarding a person's physical and emotional health is also widely regarded as private information that he or she should be entitled to control; indeed, so intimately vital are these facts that medical professionals are charged with a legal duty of confidentiality.

Although many privacy issues concern private facts, others are concerned with information of a significantly different character. Some information contained in public records concerns matters that most individuals would regard as sensitive. For example, many people are reluctant to make their debt history readily available to anyone who happens to be curious about it—and this is especially so if that history includes a bankruptcy. Likewise, many people who have paid their debt for criminal offenses are reluctant to make their criminal records easily available out of a concern that such information would be used to discriminate against them.

The issue of whether a person has a moral right to control a particular piece of information that ought to be protected by the law thus depends on a variety of considerations. It will depend not only on broad theoretical arguments regarding the general justification of information privacy, but also on the character of the particular piece of information and how that information might be used by other persons. Such determinations present difficult issues of policy and ethics.

Corporate Use of Personal Information

Many commercial firms collect information from visitors to their Web sites, which is stored in small data files called “cookies” and deposited on the visitors' own computers. These files typically contain information—such as passwords, on-site searches, dates of previous visits, and site preferences—that can be used by the firm to customize the user's experience when revisiting its site. For example, a bookselling Web site might store a list of previous searches on the user's computer so it can be accessed by the site on subsequent visits to generate a list of books to recommend to the user. This enables the site to provide what it considers to be better service by tailoring the user's Web environment to his or her preferences as expressed in previous visits to the site.

Although the use of cookies thus has a plausible business rationale, it raises ethical issues. Typically, cookies are transmitted from the user's hard drive to the site and retransmitted (possibly with modifications) from the site to the user's hard drive in a way that does not interrupt the user's browsing experience. This means that, in many cases, the user's hard drive—that is, his or her physical (as opposed to intellectual) property—is being modified without his or her consent. Although the legitimacy of intellectual property rights may be controversial, the legitimacy of personal property rights in physical objects is not (at least not in mainstream theorizing). The idea that someone else can, in essence, modify the user's

physical property without his or her consent raises, to begin with, ethical issues concerning the user's property rights over the contents of his or her computer.

Moreover, some theorists worry that the use of cookies to keep information on the consumer raises privacy issues. As Spinello (2000, p. 111) puts the matter, "cookie technology is analogous to having someone follow you through the mall with a video camera." In both cases, the technology keeps information on where you have gone, what you have looked at, and what you have purchased. To the extent that one has a legitimate expectation that one's movements in a public mall not be recorded, it can reasonably be argued that one also has a legitimate expectation that one's movements in cyberspace not be recorded.

Although it is possible for users to set up their browsers to refuse cookies or to alert them whenever a site attempts to store a cookie, this can cause inconvenience to the user. Refusing all cookies restricts the user's options in cyberspace because some Web sites cannot be viewed without accepting cookies. Setting a browser to ask before accepting cookies can result in frequent interruptions that radically change the quality of the browsing experience. Many users who restrict cookies find that the disutility associated with such frequent interruptions outweighs, at least in the short run, their privacy concerns and restore their browsers to the default setting that allows for unrestricted cookies.

There is thus a sense in which users who decline to configure their browsers to refuse cookies can be presumed to consent to cookies, but such consent is of questionable ethical significance. If the initial choice between A and B is not an ethically acceptable one, then the fact that a person voluntarily chooses A does not logically imply consent to A. For example, the fact that I voluntarily choose giving a robber my money if my only other choice is being shot does not entail that I have, in any ethically significant way, consented to give the robber my money. Consent is ethically significant only to the extent that it is rendered in an antecedent choice situation that is ethically acceptable. Thus, if the choice between accepting cookies and not being able to browse a Web site efficiently is not an ethically acceptable choice to impose unilaterally on a user, then the user's choice to accept cookies does not entail ethically meaningful consent. For this reason, the issue of whether accepting cookies amounts to meaningful consent depends on the issue of whether the choice to accept cookies or accept an inferior browsing experience can permissibly be imposed on users.

More troubling to privacy advocates than the data kept by any one firm, however, is the possibility that it could be combined with the information of other firms to create a comprehensive file about a user. To continue Spinello's analogy, this is analogous to having your movements in every store and mall recorded by a video camera and then keeping all those recordings in one central location that can be accessed by other persons. The more information about an individual that is centrally located and available for use by other persons and firms, the more likely it is to strike individuals as involving a breach of their privacy.

Notably, there are economic forces pushing in that direction. Businesses realize that consumer information is a valuable commodity and have evinced a growing willingness to sell it. Information about a consumer's buying and browsing habits can be used to tailor advertisements and mailings to his or her particular tastes and preferences, arguably serving both the consumer and the firm. It is not surprising, then, that trading in information itself is becoming an increasingly profitable venture—not only for firms specializing in information commerce, but also for ordinary firms specializing in other areas, and hence increases the likelihood that businesses will compile comprehensive files of personal information on individuals.

Software License Infringement

The topic of software license infringement, or piracy, is routinely covered by the popular press. Among study participants, attitudes toward piracy were generally similar; however, participants from the United States and the Netherlands showed statistically significant differences in attitudes from the overall group. Participants from the United States were significantly less tolerant of piracy, while those from the Netherlands were significantly more permissive. Although other studies have reported that the Pacific Rim countries of Singapore and Hong Kong are hotbeds of software piracy, this study found tolerance for copyright infringement in those countries to be moderate, as were attitudes in England, Wales, Australia, and Sweden. This could mean that the individuals surveyed understood what software license infringement was, but felt either that their use was not piracy, or that their society permitted this piracy in some way. Peer pressure, the lack of legal disincentives, the lack of punitive measures, and number of other reasons could explain why users in these alleged piracy centers disregarded intellectual property laws despite their professed attitudes toward them. Even though participants from the Netherlands displayed a more permissive attitude toward piracy, that country only ranked third in piracy rates of the nations surveyed in this study.

Illicit Use

The study respondents unilaterally condemned viruses, hacking, and other forms of system abuse. There were, however, different degrees of tolerance for such activities among the groups. Students from Singapore and Hong Kong proved to be significantly more tolerant than those from the United States, Wales, England, and Australia. Students from Sweden and the Netherlands were also significantly more tolerant than those from Wales and Australia, but significantly less tolerant than those from Hong Kong. The low overall degree of tolerance for illicit system use may be a function of the easy correspondence between the common crimes of breaking and entering, trespassing, theft, and destruction of property and their computer-related counterparts.

Misuse of Corporate Resources

The scenarios used to examine the levels of tolerance for misuse of corporate

resources each presented a different degree of noncompany use of corporate assets without specifying the company's policy on personal use of company resources. In general, individuals displayed a rather lenient view of personal use of company equipment. Only students from Singapore and Hong Kong view personal use of company equipment as unethical. There were several substantial differences in this category, with students from the Netherlands revealing the most lenient views. With the exceptions of those from Singapore and Hong Kong, it is apparent that many people, regardless of cultural background, believe that unless an organization explicitly forbids personal use of its computing resources, such use is acceptable. It is interesting to note that only participants among the two Asian samples, Singapore and Hong Kong, reported generally intolerant attitudes toward personal use of organizational computing resources. The reasons behind this are unknown.