CSCI 7000-001 — Legal Aspects: a Primer

December 11, 2001

1 Motivation

There are at least three types of motivations to study law in the context of computer and network security:

- *common goals*: computer security is about protecting valuable assets, such as computing resources and information, from damage, theft, unauthorized use, modification, etc. These goals are consistent with the U.S. and many other legal systems.
- *high-level policies*: the protection of some assets often conflicts with the protection of other assets or rights. E.g., protecting the integrity of some system may require some violation of privacy. Laws define the ultimate policies.
- *limitations on security methods*: there exist laws that regulate use, communication and deployment of methods and techniques—namely cryptographic algorithms and tools—that form the foundations of computer and network security.

2 Common goal: protection of assets

Different kinds of assets:

- hardware: common property protection
- services: common property protection
- software, and some other forms of information: *intellectual property* law
- data (stored and transferred): *privacy protection* law

3 Types of intellectual property protections

The "universe" of intellectual works, ideas or expressions that are by no means protected is usually referred to as *public domain*.
Protection laws offer four classes of protection

- copyright
- patents
- trademarks
- trade secrets

4 Copyright

scope A copyright applies to a *fixed expression* of intellectual or artistic work. That is a tangible expression. Something that has been notated or somehow recorded.

protections copyright law protects *the right to make copies of the expression*. Expressed ideas or concepts are not protected. As stated in the Copyright Act:

> "In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work."

formal requirements practically none. Copyrights *may be registered* in the Copyright Office in the Library of Congress. The use of a copyright notice (somehow attached to the expression) is recommended, but not necessary.

duration the copyright protection is effective until 70 years after the last surviving author's death. In case there is no specific author, 95 years after publication or 120 years after creation, whichever is shorter.

A copyright notice should be marked with the © symbol, it should refer to the copyright owner, and the first year of publication.

5 Copyright ownership

A fundamental issue is the determination of copyright ownership. The following principles apply:

- *general rule*: the creator of the work owns all the copyright interests in the work

- *joint authorship*: a work qualifies as joint work if it is a combination of distinct contributions that are *conceived as a single whole*. In the case of joint work, all the contributing authors have the right to use the work as they please. However, if a single author makes a profit through the exploitation of the joint work, then the profits will have to be shared with the other joint authors

- *work made for hire*: the idea here is that the "author" is considered to be the entity which hired the actual creators of the work (such as a corporation for whom the author works as an employee). The work made for hire doctrine requires that the work be done "within the scope of" the employee's employment.

  The exact determination of whether a creator is considered an employee under the law is somewhat complex.

6 Essence of copyright protection

In practice, you should not make copies of a program. However, you may use that as a (formal) description to implement your own version of the same abstract functionality. Also, it is perfectly okay for someone to produce exactly the same expression, provided that it is expressed independently—that is, not by copying the protected expression.
There is also an important limitation to the protections offered by copyright laws. This is expressed by the doctrine of *fair use*. Fair use is determined according to four principles:

- *purpose and character of the use*: for example, whether such use is of commercial nature or is for nonprofit, educational purposes;

- *the nature of the copyrighted work*: published or unpublished work

- *the amount and substantiality of the portion used in relation to the copyrighted work as a whole*: quoting a sentence from a book is okay. Copying two chapters is not.

- *the effect of the use upon the potential market for or value of the copyrighted work*: it is okay to use a work if the particular use (not its context) would not affect in any way the market for the work.

7 Other important issues

Protection of *collections* of information is also extremely important. Examples are databases, phone books, collections of statistics, compilations of information of any kind.
Under U.S. law and doctrine, the following principles apply:

- the collection is protected by copyright laws only if the collection contains a minimum level of creativity in itself. In other words, in order to be protected, a database must be original in its selection, coordination, and arrangement. The mere alphabetic arrangement of data is not original enough for protection by copyright law unless there is some originality in the selection or coordination of the data.

- the protection, and therefore the rights of the copyright owner, do not extend to the underlying data. In other words, the protection over a database prevent an individual from extracting factual data from the database, as long as that does not involve copying the selection and arrangement of the database as a whole.

8 Trademarks

scope a device (e.g., a word, phrase, symbol, product shape, or logo) that identifies a manufacturer or merchant. Service marks, which are used on services rather than goods, are also governed by Trademark law

protections U.S. trademark law protects the right of the owner to identify its goods and to distinguish those goods from those made or sold by another. In other words, it is intended to prevent an individual other than the owner of the mark to cause confusion as to the source or sponsorship of the goods or services involved.

Multiple parties may use the same mark only where the goods of the parties are not so similar as to cause confusion among consumers.

requirements A device (such as a word or a logo) can only be considered a trademark or a service mark if it is distinctive. A distinctive device is one that is capable of distinguishing the goods or services upon which it is used from the goods or services of others. A non-distinctive device is one that simply describes or names a characteristic or quality of the goods or services.

It is advisable to register a trademark, although it is not strictly necessary.

A mark which is registered with the federal government should be marked with the ® symbol. A Unregistered trademarks should be marked with the ™ symbol.

9 Trademarks and the Internet

The most important issue involving trademark infringement for computer systems is the dispute over domain names.
In most cases of domain name disputes, the party seeking to obtain the domain name typically relies on their trademark rights, with the domain name being identical to the company's well-established trademark. However, that fact alone is insufficient to prove a charge of trademark infringement. A number of criteria define the case of trademark infringement. In essence, infringement implies that the use of a mark has created a likelihood-of-confusion about the origin of the goods or services provided by the individual using the name.
An example is the case of roadrunner.com, a broadband ISP, challenged by Warner Brothers. The issue is that Warner Brothers. has no history and no intention of offering Internet access services to the public. In addition, Warner Brothers has allowed many other companies to operate businesses under the Road Runner name. As a result, it would be

difficult to prove that the operation of a web page for Internet access services under the roadrunner.com domain name would involve a likelihood of confusion with their Road Runner mark.

10 Patents

Patents provide a strong form of protection. The principle is that someone (a person or a corporation) may gain exclusive rights on *an idea* or *an invention*, regardless of the expression of that idea or invention.
The importance of granting monopolies for new inventions has been recognized in the United States since the adoption of the U.S. Constitution. In Article I, Section 8, the U.S. Constitution:

> Congress shall have power . . . To promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries.

Patents in the United States are governed by the Patent Act (35 U.S. Code), which established the United States Patent and Trademark Office (the USPTO). The most common type of patent is a utility patent. Utility patents have a duration of twenty years from the date of filing, but are not enforceable until the day of issuance. Design patents protect ornamental designs. Plant patents protect new varieties of asexually reproducing plants. To obtain protection under U.S. law, the applicant must submit a patent application to the USPTO, where it will be reviewed by an examiner to determine if the invention is patentable. U.S. law grants to patentees the right to exclude others from making, using, or selling the invention.

11 Requirements for patents

Because patents grant very powerful rights, the scope of patents is (or it should be) carefully limited. The following rules are requirements for a patent:

- *statutory*: "processes, machines, articles of manufacture, and compositions of matter are patentable." This definition is actually very broad, and covers software inventions. There are however a few exceptions (e.g., "data structures and programs per se" or natural phenomena such as electricity or magnetism).
- *novelty*: an invention cannot be patented if certain public disclosures of the invention have been made. This determination is complicated and often requires a detailed analysis of the facts and the law.

  The most important rule, however, is that an invention will not normally be patentable if:

- the invention was known to the public before it was "invented" by the individual seeking patent protection;
- the invention was described in a publication more than one year prior to the filing date; or
- the invention was used publicly, or offered for sale to the public more than one year prior to the filing date.

Although the United States grants the one year grace period described in the last two rules above, most other countries do not grant such a period. Therefore, it is almost always preferable to file a patent application before any public disclosure of the invention.

- *usefulness* the subject matter must be "useful." The term "useful" in this connection refers to the condition that the subject matter has a useful purpose and also includes operativeness, that is, a machine which will not operate to perform the intended purpose would not be called useful, and therefore would not be granted a patent. In most cases, the usefulness requirement is easily met in computer and electronic technologies.

- *nonobviousness* If an invention is not exactly the same as prior products or processes (which are referred to as the "prior art"), then it is considered novel. However, in order for an invention to be patentable, it must not only be novel, but it must also be a nonobvious improvement over the prior art.

  This determination is made by deciding whether the invention sought to be patented would have been obvious "to one of ordinary skill in the art." In other words, the invention is compared to the prior art and a determination is made whether the differences in the new invention would have been obvious to a person having ordinary skill in the type of technology used in the invention.

  As you can imagine, the determination of whether a particular change or improvement is "obvious" is by no means. . . obvious!

12 Trade secrets

A trade secrets is any form of "know-how."
In other words, it is "any formula, pattern, device or compilation of information used in one's business, which gives the owner an opportunity to obtain an advantage over competitors who do not know or use it."
Examples:

- the formula for Coca-Cola

- ideas that offer a business a competitive advantage. For example, an idea for a new type of product or a new website

- knowledge that a new product or service is under development, and knowledge of its functional or technical attributes. For example, how a new software program works
- valuable business information such as marketing plans, cost and price information and customer lists. For example, a company's plans to launch a new product line
- "negative know-how". For example, research revealing that a new type of drug is ineffective
- any information that has some value and is not generally known by your competitors. For example, a list of customers ranked by how profitable their business is

13 Trade secret requirements

In contrast to copyright, trademark, and patents, a trade secret must be explicitly protected. In other words, the owner of a trade secret must affirmatively act in a way that proves its desire to keep the information secret.
In the most common case, a company holding some information will have its employee sign a *nondisclosure agreement*.

14 Trade secret protections

Trade secret law provides protection against improper dissemination and improper acquisition of secret information. In other words, the owner of a trade secret may obtain the following forms of legal protections

- confidentiality from people who are automatically bound by a duty of confidentiality, including any employee who routinely comes into contact with the employer's trade secrets as part of the employee's job
- protection against people who acquire a trade secret through improper means such as theft, industrial espionage or bribery
- protection against people who knowingly obtain trade secrets from people who have no right to disclose them
- protection against people who learn about a trade secret by accident or mistake, but had reason to know that the information was a protected trade secret
- confidentiality from people who sign nondisclosure agreements (also known as "confidentiality agreements") promising not to disclose trade secrets without authorization from the owner.

Notice that trade secret laws *do not protect against analysis or reverse engineering*.

15 Nondisclosure agreements

A nondisclosure agreement (a.k.a. NDA or confidentiality agreement) is a contract in which the parties promise to protect the confidentiality of secret information that is disclosed during employment or another type of business transaction.
There are five important elements in a nondisclosure agreement:

- definition of confidential information
- exclusions from confidential information
- obligations of receiving party
- time periods, and
- miscellaneous provisions.

16 Policies

Perhaps the most important policy issue is the tension between the needs of law enforcement, and the protection of privacy.
The issue that is most relevant to computer and network security is that of *key escrow*.

17 Key escrow: goals

The idea is to prevent criminals from hiding information that can be used against them in court. Specifically,

- *FBI* wants to have read access to all the information that *Alice* stores or transmits to *Bob*,
- for each *Alice* and *Bob*
- at any point in time
- without letting *Alice* or *Bob* know that

18 Key escrow: issues

Alice has two ways to allow *FBI* to achieve its goals:

- use a weak cryptosystem, so that *FBI* (and anyone else with the same computing power) can *break* it as needed
- share keys with *FBI*

The first approach is clearly flawed in some fundamental way. The second approach has practical problems:

- *FBI* must manage a very large set of keys in a secure manner
- *Alice* must trust *FBI*

Notice that these problems are essentially independent of any technology used for the key escrow system.

19 Privacy: ECPA '86

The Electronic Communications Privacy Act (ECPA) sets out the provisions for *access, use, disclosure, interception and privacy protections of electronic communications*. The law was enacted in 1986 and covers various forms of wire and electronic communications.
According to the U.S. Code, electronic communications "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce."
ECPA prohibits unlawful access and certain disclosures of communication contents.
Additionally, the law prevents government entities from requiring disclosure of electronic communications from a provider without proper procedure.

20 E-Privacy: interesting links

- http://www.fbi.gov/hq/lab/carnivore/carnivore.htm
- http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf

21 Regulations over cryptographic software in the U.S.

- *import*: there are no import restrictions on cryptography
- *export*: the US generally maintains somewhat strict controls

Cryptography export used to be controlled by the International Traffic in Arms Regulation (ITAR). At the end of 1996, cryptography export was transferred to the Export Administration Regulations of the Department of Commerce. The export policy was relaxed to favor export of data-recovery cryptography. This initiative was announced in a statement by the Vice President of 1 October 1996, and further elaborated in a November 15, 1996 executive order and memorandum, and in the Commerce Department draft Export Administration Regulations of December 30, 1996. The Department of Justice is now

included in crypto export decisions. (Incidentally, the Commerce Department has "borrowed" three export control and crypto specialists from the FBI and NSA to help process license applications.)
Making available cryptography on the Internet or a BBS is considered export, unless appropriate measures are taken to prevent foreigners from accessing the cryptography.
The export rules distinguish between five categories of "encryption items" (EI).

- certain mass-market encryption software may be released from EI controls after a one-time review.
- "Data recovery" crypto (meaning that government can access keys or plaintext with a lawful warrant) will be eligible for an export license to non-embargoed countries. The procedures for data-recovery licenses were simplified in September 1998, when also "recoverable products" were released for export (a recoverable product means that an operator can access plaintext without the user noticing).
- after a one-time review, (up to) 56-bit cryptography can be granted a six-month export license, provided the exporting business commits itself to incorporating a data recovery feature in its products within the next two years. This provision was changed in December 1998, when all 56-bit crypto was released for export after a one-time review, with no requirement of data recovery.
- all other encryption items may be eligible for encryption licensing arrangements; items not authorized under a licensing arrangement will be considered on a case-by-case basis.
- encryption "technology" may be licensed for export on a case-by-case basis.

After the President's Export Council Subcommittee on Encryption advised in "Liberalization 2000" to ease the export controls, the government announced further relaxation of export controls
The new regulations were finally published on 12 January 2000 (the press release is less specific but much more readable). The major components of the updated policy are the following.

- any crypto of any key length can be exported under a license exception, after a technical review, to non-government end users in any country except the seven terrorist countries.[1] Exports to governments can be approved under a license.
- retail crypto (i.e., crypto which does not require substantial support and is sold in tangible form through retail outlets, or which has been specifically designed for individual consumer use) of any key length can, after a technical review, be exported to any recipient in non-terrorist countries.

[1]The "terrorist countries" are: Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.

- unrestricted crypto source code (like most "open source" software) and publicly available commercial source code (like "community source" code) can be exported to any end-user under a license exception without a technical review. The Bureau of Export Administration (BXA) must be given a copy or the URL of the source code. All other source code can be exported under license exception after a technical review to any non-government end-user. One may not, however, knowingly export source code to a terrorist country, although source code may be posted on the Web for downloading without the poster having to check whether it is downloaded from a terrorist country.

- any crypto can be (re)exported to foreign subsidiaries of US firms without a technical review. Foreign nationals working in the US no longer require an export license to work for US firms on encryption.

- the regulations implement the December 1998 Wassenaar changes (notably, export of 56-bits and 64-bits (for mass-market products) crypto to non-terrorist countries).

- post-export reporting is required for exporting certain products above 64 bits to non-US entities.

Since 19 October 2000, a further liberalization of export controls is effective, triggered by changes in the EU export regulations (see the Federal Register Vol. 65, No. 203, pp. 62600-10, available at BXA). The liberalization was announced on 17 July 2000. A license exception is introduced for export of any crypto product to any end user (so, the distinction between government and non-government end users is dropped) in the 15 EU countries, Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland, and Switzerland. Also, US exporters can ship products immediately after filing a commodity classification request, without waiting for the technical-review results or the previously used 30-day delay period.