/Legal Requirements of Secure Systems/

by

Joseph M. Beckman

B.S., Kansas State University, 1982

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Computer Science

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1985

Approved by:

Myron A. Calhoun
Major Professor

INTRODUCTION

This paper examines the link between the laws regulating privacy and negligence and the actions of computer scientists. The storage of data in computer systems and the growing accessibility of this data coupled with a litigious society and specifically, concerns of privacy, warrant a close look at legal requirements to provide a measure of security in computer systems and applications.

By understanding the law in the area of privacy and the duty of care obligated in tort law of negligence, a computer scientist is in a better position to make a good decision about security policies and practices.

The first part of this paper reviews the laws in the areas of privacy and negligence. The second part applies those laws to some common computer science applications. The last part suggests some guidelines for individual computer scientists and the computer science profession as a whole to follow to obtain reasonably secure systems that meet the required standard of care of a professional.

The issue of copyrights, patents, and trade secrets will not be examined. The legal requirements discussed herein have to do with third parties who, initially, are not necessarily directly involved with computer systems.

DEFINITIONS

Some words used frequently in this paper are defined for clarification. Security refers to techniques, procedures, and safeguards that are used to protect computers, computer resources, and processes in the computer to ensure proper use of such [SALT75, TURN76]. The American Federation of Information Processes has eleven different definitions for security. A common concept in their analysis of security is that of protection. Security is concerned with the measures taken within the computer (internal) and those taken outside of the computer (external). Internal security measures are implemented as security kernels or they may be a separate filter; these measures may be implemented in either hardware or software or a combination of both. An attack is an attempt to violate security. Security may be breached, violated, or compromised, in which case it has failed.

Privacy is a term used concerning an individual's right to decide about information to be shared with others [WOOD80]. There is not a precisely bounded definition of privacy, so the courts may rule (and have done so) that different actions fall under privacy rights. These actions range from association rights to family rights to information rights. Consequently, it is generally better to assume that protection is needed than to go without.

Confidentiality is a property of data. If data is confidential, then it must somehow be protected from unauthorized access. Confidentiality may be relative to certain situations: in one instance data may be confidential and in need of protection, whereas in a different situation there is much

less need for protection of the same information. This may arise in circumstances where the data is collected and used by one agency and then given to another agency for one specific purpose. The use of confidential data must be confined to authorized purposes.

PRIVACY

Privacy rights are manifested in different ways in our society. Rights of privacy include the right to be free from unreasonable search and seizure, the right to free association and beliefs, and the right to make certain personal decisions.

Another right of privacy is information control. This right is concerned with the collection, dissemination, and use of information about personal attributes and actions. It becomes of increasing interest as data bases proliferate and store increasing amounts of personal data and as distributed systems and networks increase the accessibility and potential aggregation of data.

There is an obvious conflict between society's desire for personal information and a person's desire to maintain the confidentiality of that same information. Some of this information is needed for government to function. Government needs personal information for tax purposes, for the penal system, for agencies and other regulation purposes.

The amount of information the government should receive or the individual be forced to render depends on one's view of the government's role [SALT80]. A minimal role asserts that government's power over individuals is only to protect others, where a maximal role contends the government's duty is for the welfare and safety of citizens. Under the minimal role, the amount of information necessary would be small compared to that required to fulfill the maximal role.

Computer systems have enhanced the ability and possibility of persons

or organizations to violate privacy rights; whether they have already done so is a debatable question. The reasons they may hinder the protection of privacy have to do with the intrinsic differences between computerized and manual systems. Computers can store and process huge amounts of data. This data may come from many different geographical locations if a distributed data base or network is used.

The access of data may come without direct human supervision at the remote sites. Data may easily be correlated among the different network nodes, allowing an aggregation of data to be assembled. This is impossible or impractical in a manual system.

Since the data is normally stored in machine-readable (and human non-readable) form unless special care is taken to build an audit trail, it is almost never possible to determine if, and by whom, the data has been accessed or modified. The data may also be erased or altered by hardware or software malfunctions.

The Special Advisory Committee on Automated Personal Data Systems proposed a Code of Fair Information Practices, which is applicable to all information systems in both the private and the government sector. The following principles are embodied in the Code:

(a) No personal data base may have a secret existence.

(b) For any personal data base, an individual must be able to determine what information about him is stored and how that information is used.

(c) An individual must be able to correct or amend an erroneous record.

(d) An individual must be able to prevent the transfer of information obtained for one purpose for use in another, previously unannounced, purpose.

(e) Each organization must guarantee the integrity of the data stored and take actions to prevent the misuse of the data.

Currently, there exist certain federal statutes regulating privacy rights which use the Code as a framework. These laws apply to federal agencies, local government agencies, and certain private organizations. In general, though, the private sector is not bound by the Code of Fair Information Practices. Fair information practices in statutory law regulate four areas:

(a) Collection of data

(b) Subject access to data collected

(c) Control over internal use or external dissemination

(d) Notice to individuals of their rights or of the use of the information

Collection

The Privacy Act of 1974[1] enacts restrictions on the government's ability to collect information. It directs agencies to keep information about an individual only if it is "relevant and necessary" for the agency to accomplish its designated task. The "relevant and necessary" clause is broad and has not drastically curbed the collection of data for the government [WEWE81]. Legislation is more restrictive in the private sector. The Bank Secrecy Act[2] is an example of the detailed requirements imposed on financial institutions. For instance, the Act requires that banks keep a history of any financial transactions involving $100 or more.

The Fair Credit Reporting Act[3] limits the information that consumer credit reporting agencies can collect. It states that most information of a negative nature may not be reported if it took place more than 7 years ago (except bankruptcies, which are reportable for up to 14 years).

These laws limit the use of information once it is collected more than actual collection in the first place.

Access

The Freedom of Information Act (FOIA)[4] has been used extensively since its enactment to allow individuals to access records kept by the government on them. Many controversial areas are exempt from this disclosure requirement; personnel and medical files and certain law enforcement files, for

1. Privacy Act of 1974 5 U.S.C. 552a
2. Bank Secrecy Act of 1970 12 U.S.C. 1829b, 1953 31 U.S.C. 1051-1122
3. Fair Credit Reporting Act of 1969 15 U.S.C. 1681-1681t
4. Freedom of Information Act of 1966 5 U.S.C. 552

example.

The FCRA mandates that consumer reporting agencies disclose information kept on individuals who request such information. The agencies must also report sources and recent recipients of the stored information. The FCRA allows for an individual to contest information in his file. If the contested information is found to be inaccurate or is not verifiable, it must be stricken from the agency's files. If the contention is not resolved, the individual is allowed to write a "brief statement" about the contested information.

The Family Educational Rights and Privacy Act (FERPA but also known as the Buckley Amendment)[5] allows access to and correction of an individual's records kept at federally funded and other educational institutions. This legislation has not been widely used.

Federal agencies and contractors who keep personal records for Federal agencies are covered under the Privacy Act's access and correction mandate. Like the FCRA, individuals are allowed access to their files. They may also propose corrections to information they believe to be erroneous.

Use

Most Fair Information Practices laws impose restraints on the disclosure or internal use of information that has been collected. The FOIA started this by prohibiting disclosure of government maintained information that was a clear violation of personal privacy.

---

5. Family Educational Rights and Privacy Act of 1974 20 U.S.C. 1232g

The Financial Privacy Act of 1978[6] revoked some of the Bank Secrecy Act's promotion of disclosure of sensitive data. The Bank Secrecy Act was a sweeping piece of legislation that allowed banks to disseminate information to the secretary of the Treasury and other Federal agencies. Now the agencies must state in writing that they believe the information to be transferred is "relevant to a legitimate law enforcement inquiry" and is within the jurisdiction of the agency that receives the information. The agency must also notify the person involved of the transfer.

The FCRA also places restrictions on the dissemination of data. It restricts disclosure of reports on consumers from consumer reporting agencies to specified instances. Any disputes added to the record must be given out along with the rest of the record. If the use of the report results in an adverse effect by the agency that received the information, then the agency is obligated to provide the consumer with the name and address of the company that provided the report.

The Privacy Act of 1974 prohibits agencies from disclosing information unless (1) the individual requests or consents to it in writing or (2) The information falls within one of eleven excepted categories. Most of the exceptions are for routine Federal agency use or for law enforcement reasons. FERPA likewise prohibits disclosure unless consent is given, or the information is used for specified educational business purposes.

Notice

Another safeguard for the public is the procedural requirement for notices. Notices make known the methods of information practices of

6. Right to Financial Privacy Act of 1978 12 U.S.C. 3401-3422

organizations. Notices can advise people of their rights and warn them of uses of gathered data that may have an adverse effect. It may also make known the very existence of databases containing personal information. However, a requirement that financial institutions notify all customers of their rights was repealed because the institutions argued that the cost would be too great for implementation [WEWE81].

The first piece of legislation with a notice requirement was the FCRA. The statute was vague on the actual details. The Privacy Act four years later more clearly specified the information necessary on a notice form. The actual format and language was left up to each individual agency. When the Financial Privacy Act of 1978 was enacted, precise notices were detailed by the government.

Many of these fair information practice laws are enforced through appropriate criminal and civil penalties, allowance for recovery of actual and punitive damages, and injunctive relief. Certain Federal agencies are given jurisdiction when appropriate. Government bureaucrats may be held personally responsible for the wrongful release of information nominally protected by the Privacy Act or FOIA. This has made them a bit cautious to release information. FERPA is enforced through the threat of a cut-off of federally funds.

It may be useful to examine a few court cases where the issue of the right to privacy in information control has arisen. The first case is Menarb vs. Saxbe.[7] Menarb was a 19 year old college student visiting some friends. While he was waiting for a ride, he fell asleep on a park bench.

7. Menarb vs. Saxbe, 498 F. 2d. 1017 (1974)

Residents of the neighborhood called the police about a 'prowler' after Menarb awoke and looked through a window in their house to determine the time. When he was picked up by the police, a wallet with ten dollars was found near the bench. He was arrested, booked, fingerprinted and held for two days. The wallet was not reported stolen, and no criminal complaint or charges were ever filed against Menarb.

The Los Angeles police gave Menarb's fingerprints to the FBI as a matter of course. Menarb's mother wrote the FBI about the file, but the FBI does not usually acknowledge the existence of any file in its data bases, nor do they generally alter or add to a file at a private citizen's request.

Menarb's mother took the matter to District Court and eventually to the Circuit Court of Appeals. The Circuit Court of Appeals decided that the FBI "had no authority to retain this record in its criminal files", along with the other arrest records stored there.

Because of the time, effort, and money it took Menarb's mother to effect this expungement, one may conclude that few people will take this route.

Anderson vs. Sills [8] raised the issue of the legality of collecting data on people who were not accused of criminal activities. Various riots (prompted by the war in Viet Nam) had already occurred in different parts of the US during the summer of 1967. In an attempt to prevent further riots in his state, the Attorney General of New Jersey issued a memorandum entitled "Civil Disorders--The Role of Local, County, and State

8. Anderson vs. Sills, 56 N.J. 210 (1970)

Government". In this document, he recommended that data bases containing information on riots, rallies, demonstrations, marches and so on be created and maintained by law enforcement officials. These data bases would contain information on the participants and on any sponsoring organization

Denise Anderson filed a suit alleging the compilation of information was unconstitutional. The case was appealed to the Supreme Court of New Jersey which reversed the Superior Court of Hudson County and ruled in favor of the defendants. The Court ruled that the danger to civil liberties must be proven, and that hypothetical instances of what could happen were not a sufficient reason to enjoin the collection of information. In the absence of a showing of bad faith or arbitrariness, the Court ruled that the executive branch of government was free to collect whatever information it believed to be beneficial in carrying out its duties. In effect, the court stated that the danger must be real and apparent before suit can be brought, and the possibility of a chilling effect is not enough to deny the executive branch the right to collect data.

Zurcher vs. Stanford Daily [9] involves not only information privacy, but also the right to be free from unreasonable search and seizure.

During an anti-war demonstration in early April 1971, demonstrators seized the administrative offices of the Stanford University Hospital. Police were called in to evict the demonstrators. During the eviction, all nine police officers were attacked and injured. They were able to identify only two of their assailants.

9. Zurcher vs. Stanford Daily, 98 S. Ct. 1970 USC (1978)

However, a photographer from the Stanford Daily was present and was seen taking pictures during the assault. A warrant was obtained to search the premises of the Stanford Dailys for film, negatives, or photoghaphs of the assault. Other than pictures printed on April 11, no photographs were found.

The Stanford Daily brought suit charging that the search had violated the constitutional right of freedom from unreasonable search and seizure. The case was eventually heard before the US Supreme Court and the Court ruled in favor of the defendants.

The Court held that the search was not unreasonable because there was reason to believe that the evidence desired was located on the premise to be searched and declared that whether the owner is accused of the crime is irrelevant to the legitimacy of the search. The Court found no constitutional reason to give the press higher immunity from search and seizure than private citizens. The Justices asserted that local magistrates could prevent the use of excessively broad, intrusive searches that would interfere with a newspaper.

Two important points to gather from these Court cases are:

1) Information may be forcibly disclosed.

2) There is not a well-codified set of procedures to ensure personal information privacy. Laws regulating the improper collection of data, providing the ability to propose corrections or deletions, or requiring the notification of individuals are neither adequate nor comprehensive.

NEGLIGENCE

The price of not maintaining a secure system that is subsequently violated may be the loss of a professional negligence suit. Any time a defective product fails to work properly, its manufacturer may be liable for any injury that results. Generally, this liability may be mitigated if the manufacturer took precautions that an ordinary man would have taken in the design and manufacture of the product. If, instead, the manufacturer is a professional, and the injury was caused by his service (or lack of), a different standard of liability is applied. This section discusses professional negligence and certain court cases that apply to this concept.

Negligence has four components;

(a) a minimum obligation of duty

(b) failure to conform to a required standard of care

(c) a reasonably close connection between the service and an injury

(d) and the injury itself

Although all four elements comprise negligence, professional negligence is based on the heightened duty of care a professional must exercise in practice.

Many computer scientists consider themselves professionals because of the prestige of working in an occupation where one can be labeled a professional. Legally, professional status is more than just a label; there are criteria to fulfill before a person is considered to be a professional by the judicial system.

Professionals are characterized by their special competence which is not part of the usual equipment available for an ordinary man. They have acquired learning and an aptitude developed by special training and expertise. A professional's vocation serves the public.

Computer scientists fit this description. Universities offer advanced curricula and degrees in computer science. Some organizations administer and certify exams for expertise in areas of computer science. A computer scientist's skills are developed by special training and acquired learning and require them to make intellectual judgements. A computer scientist requires special competence that ordinary people do not have. Because their skills are beyond the scope of the ordinary man, clients must rely on the expertise of computer scientists.

Organizations such as the Association for Computing Machinery (ACM), Data Processing Management Association (DPMA) and the American Federation of Information Processing Society (AFIPS) may provide the necessary link to public service. Instead of promoting the commercial interests, they try to advance computer science as an art. These organizations closely resemble those of other professionals [BROO81].

In the judicial system, there is a minimum standard of care required of people who design, manufacture or market goods and services. If these people are the defendants in a negligence suit, the standard used is usually the "reasonable man" standard, which asks if a reasonable, prudent man would have acted in the same way as the defendant. If the answer is yes, the defendant will probably win the suit. But if the defendant is a professional being sued for professional negligence, a different standard will be used. The question asked of a professional's action is whether the

defendant exercised such care in his practice that other people in the profession would ordinarily have under like conditions. If this standard of care is violated without due cause, the professional may be held negligent.

Thus in the second component of negligence, failure to conform to a required standard of care, a professional's standard is generally accepted to be more stringent than that of the non-professional.

Because of the scope, complexity, mitigating circumstances and defenses involving the third component (the connection between service and injury), this paper will not attempt to examine details involving it.

The first component, a minimum obligation of duty, is important to computer scientists because of the potential scope and far-reaching effects of a computer application. Clearly, the duty is owed at least to the immediate client. But because an application may affect many different people (Electronic Funds Transfer, for instance) it is important to examine who else may have a claim to a professional's obligation of duty.

Until the MacPherson vs. Buick Motor Company[10] case, "privity of contract"[11] was the standard used to determine the extent of obligation for negligence. An injured party could only sue the person who sold the defective product. This case involved an automobile with a defective wheel. The wheel broke and the resulting accident caused injury to the plaintiff. The court held that a negligence suit could be brought against the manufac-

10. MacPherson vs. Buick Motor Co., 217 N.Y. 382, 111 N.E. 1050 (1916)
11. The term privity "implies special or particular knowledge showing active consent or concurrence" or a "connection or bond of union between parties as to some particular transaction" - from Corpus Juris Secundum, Vol. 72 (1951)

turer even though no privity existed between them and the defendant thus removing the immunity that had existed previously.

Since privity was no longer a requirement, the question was, "to whom was duty owed?". The answer to this question has been debated and refined through several court cases. The case of Glanzer vs. Shepard[12] allowed the plaintiff to recover for short weight of some beans purchased. Although the seller procured and paid for the weigher's certificate, the court held that the buyer was a "foreseen person" to whom the weigher was liable. Even though there was no privity between weigher and buyer, it was obvious that the certificate was going to be used for a buyer.

This concept was further clarified in the Supreme Court case of Ultramares vs. Touche[13]. Here, an accountant negligently prepared and certified some financial papers for an importer of rubber. The company went bankrupt within a year, and a factor who had extended credit to the company sued the accountant. Justice Cardozo held that the statement was for the "primary benefit" of the rubber company, and only incidentally for others who used the document. Hence, the accountant was not held liable for negligence.

The doctrine of "foreseen person" was extended to "foreseen class" in the 1977 case of White vs. Guarente[14]. An accountant was held liable in this case for professional negligence. The case involved a hedge fund (in essence, a small mutual fund). The general partners were withdrawing their

12. Glanzer vs. Shepard 233 N.Y. 236, 135 N.E. 275 (1922)
13. Ultrameres Corp. vs. Touche, 255 N.Y. 170, 174 N.E. 441, 448 (1931)
14. White vs. Guarente 43 N.Y. 2d 356, 401 N.Y. S.2d 474, 372 N.E. 2d 315 (1977)

money contrary to the partnership agreement. Arthur Anderson & Company was sued for not disclosing these withdrawals and for back-dating notices to satisfy the partnership agreement. The partners were a small group the court found "whose reliance on the financial statements is specifically foreseen". Hence, the accountant was held liable for negligence. This case broadened the standard from foreseen person to foreseen class.

The question of negligence has been raised in only a few computer cases. Most of these cases have involved an end-user who was not satisfied with a system purchased. The plaintiffs used the issue of negligence to avoid contractual disclaimers or limitations.

The one computer case that has successfully argued the point of negligence is The F & M Schaefer Corporation vs Electronic Data Systems (EDS)[15]. EDS was accused of negligent misrepresentation - Schaefer Corporation officials did not feel that a system designed by EDS was satisfactory. Judge Motley ruled that EDS may be liable for the negligent design of the system, and that the jury's job was to decide if the relationship between EDS and Schaefer was one of "professional to client" at the time of the alleged negligence. The case was settled before a definitive decision was reached by the courts. Judge Motley also ruled that the statute of limitations exception of "continuous treatment" was usable by Schaefer in this case.

The "continuous treatment" exception is one that is used when there is a professional malpractice case since a client is expected to put faith and trust into a professional's work. If the professional acts in a negligent manner causing an injury to the client and the statute of limitations were

15. F & M Schaefer Corporation vs. Electronic Data Systems, Inc., Docket No. 76 Civ. 3982 (S.D.N.Y Nov. 15 1977)

to run out, the professional may still be sued if the client has had continuous treatment from that professional. This is because of the trust placed in the professional, allowing the client to continue to receive the professional's attention. This exception has been traditionally applied to a doctor-patient relationship.

In another case, Triangle Underwriters, Incorporated vs. Honeywell, Incorporated[16] the court ruled that the statute of limitations precluded the plaintiff from recovering. Judge Haight ruled that the continuous treatment exception was reserved for professional-client relationships. He also pointed out New York statutes that seem to limit the exception to the case it traditionally applied to, doctor-client suits.

He did not suggest that Honeywell was not a professional. Instead, he apparently believed that Triangle's employees were not ordinary people, but with a training and background on par with Honeywell's employees. He pointed out that Triangle's employees had no problem indicating that there was something wrong with the system delivered. Since the relationship was more professional-to-professional and not the usual professional-to-lay person, there was no higher duty owed to the client, simply the reasonable man standard of duty. The court ruling indicated that the tack taken was inappropriate, that a simple contract for the sale of goods was the proper basis for the Honeywell suit.

16. Triangle Underwriters, Inc. vs. Honeywell, Inc. 604 F. 2d 737 (2d Cir. 1979)

COMPUTER SCIENCE APPLICATIONS

At this point, the previous laws and rulings will be discussed in terms of the impact they will have on some common computer science applications. The first area examined is electronic mail. Electronic mail may be a facility that is used on a local network, it may utilize the Post Office's E-COM system or a private carrier's system, or it may be a facility provided in a long-haul network.

Electronic mail has the capability to carry personal information and is therefore subject to privacy restraints. Not only must this information be protected because it may be personal in nature, but a user could rely on the electronic mail service provided. If something should happen to the service normally provided, or if information were deleted, modified, or unduly delayed while using the service, this reliance increases the likelihood of a professional negligence suit against the designer, implementer or marketer.

Electronic mail may contain sensitive information. This information may be personal in nature, it may be a confidential file being sent somewhere, or it may contain certain corporate information that needs protection. The information sent may be personal correspondence between two (or a few more) people or it may contain personal information about a third party. Corporate design, manufacturing, and marketing techniques, practices, and suggestions may be sent through electronic mail. This information could be extremely valuable to a competitor in industry. Compromising an electronic mail system may very well compromise an organization's business affairs which it would rather keep secret.

Addresses of source and destination of electronic mail messages could also be valuable information in need of protection. An electronic mail system that is susceptible to this kind of traffic analysis would allow someone to form a series of inter-relationships among the users. The fact that a certain user is communicating with another particular user could be extremely useful to know. Knowing that it is the corporate President talking to person X tells an intruder something different than if it were the Assistant-Executive's secretary talking to X.

Law enforcement officials would be interested in forming relationships. They may want to know everyone who contacts The Organization of Left-Wingers, for instance. The ability to collect and maintain tables of relationships is not clearly covered in the privacy laws.

Remember, the Anderson _vs_. Sills case allowed law enforcement officials to collect similar information on demonstrators. But people may not know when or if collection is happening electronically. Also, electronic mail is not as public an event as a demonstration; whereas the purpose of a demonstration is to call public attention to the event and thus to some cause, the purpose of electronic mail is communication between two people.

Electronic mail has on occasion been 'seized'. The Criminal Investigation Division (CID) at the Army's DARCOM has been reported to have obtained a complete listing of an electronic mail service used internally. Several hundred workers had their computer records examined in an investigation with no apparent legal recourse available to them. The purpose of the investigation was never clearly defined (to the workers) and may have been just a "fishing expedition" [WARE84].

The legal status of electronic mail messages is not clear. The status of electronic mail service from private firms is even murkier than that of E-COM from the Post Office. The responsibilities of the carrier to the users are not defined or codified in statutory or judicial law yet.

Suppose a carrier wanted to back-up its electronic mail in case of a failure somewhere in the system. Is this allowed? It is inconceivable for the Post Office to open every letter and photo-stat the contents "in case it gets lost", but it is much easier and less obvious to do something analogous to computerized information. If back-ups are allowed, what status do they enjoy? Would it be the same as the original message? How long should private firms be allowed (or required) to keep back-ups?

The protection issue also raises questions. Is the company responsible for messages that get lost in their electronic mail system? If so, then the question of the value of the message or the loss of service is raised. Certainly, the value is not contingent solely on the loss of service, but the value of the lost or damaged data must also be considered. The Post Office allows customers to insure items. Perhaps users must insure items (messages) to recover for lost or damaged messages.

A reasonable electronic mail service would ensure that a message submitted is delivered intact only to the addressee within a certain amount of time. Therefore, a server has an obligation to ensure that a message does not get lost, delayed, damaged or deleted because of the design or a malfunction in the system. The server must also take care that a message is not accidentally released to an unauthorized third party. The amount of care necessary to fulfill this obligation would be the question in a negligence suit.

The judicial system has answered this question in a case involving a runaway barge[17]. The formula:

B < P X C

may be used. B stands for the burden of the defendant to protect some item. P is the probability of some adverse action affecting the item taking place, and C is the cost or value of the item to be protected. The amount of care taken must be proportional to the value and risk to a particular item. The server is liable for damages if an item is damaged or destroyed and the server failed to implement some safeguard that would have prevented the loss and the cost of which was less than the P X C value.

A system that is designed and marketed to handle sensitive corporate information would require a higher level of security than one advertised for handling non-sensitive memoranda. In deciding electronic mail services cases, the courts will probably look at how the system is represented. At the same time, simply stating that a system is designed only for non-sensitive information probably will not avoid a suit if it can be used for information of a more sensitive nature. Just because a product is abused does not negate the designers' responsibilities.

The Post Office has proposed three generations of electronic mail, "PAPER IN, PAPER OUT", "ELECTRONIC IN, PAPER OUT" and "ELECTRONIC IN, ELECTRONIC OUT". It has been interested in obtaining a monopoly on electronic mail [NELS81]. However, the current E-COM system calls for the Post Office to use common carriers between Post Offices offering electronic mail.

17. United States vs. Carroll Towing Co. 159 F.2d 169 (2d Cir., 1947)

Treating electronic mail as the analog equivalent of paper mail has several problems; consider the case of "ELECTRONIC IN, ELECTRONIC OUT". A mailman traditionally places the mail inside a mailbox where it is retrieved later at the customer's convenience. Hazards up to the mailbox must be overcome by the letter carrier. But how does one deliver an electronic message if all the lines to the destination computer are busy? Third generation electronic mail implies the need for external storage of undeliverable messages. These messages must be protected from unauthorized access and modification while stored.

Another problem is the privacy issue. Normally the public does not see the contents of mail as it is being delivered. But microwave and satellite links disperse an image of their message contents over a wide area. Many lines and links do not use encryption. All common carriers may not use the same encryption technique, or even the same level of cryptographic strength. If a message is sensitive, there must be some way to treat it in a special manner and ensure that a proper level of security is used for the message.

A third problem is the interstate or international flow of messages. The Federal government is in charge of regulating commerce and activities between the states; unfortunately, it has failed to legislate in this area. This flow is therefore not directly protected or overseen by federal law.

If an electronic mail message is deemed important and relevant to law enforcement officials, it is possible that they could obtain a search warrant for it, similar to the action described in Zurcher _vs_. Stanford Daily. The problem, of course, is that they may also seize many messages that are in no way related to the one sought. It is not feasible to state with

assurance what will happen to those other messages not mentioned in the search warrant. Nor is it evident that a carrier should open its network or back-ups for the officials. The carrier's management may have a duty to protest or attempt to block efforts to search and seize messages.

It is entirely possible that law enforcement officials may not need a search warrant if it is legally possible for them to seize electronic messages. A search warrant is not necessary if there is reason to believe that the evidence desired will not be around by the time the search warrant is obtained. Could police simply wait for a certain person to send a message and then seize the entire network? Would they be allowed to do this without a search warrant if back-up copies of all messages are kept? No law or case has addressed these questions yet.

Even basic issues such as ownership are in question. At what point (if ever), does a message no longer belong to the sender, but changes to the custody of the carrier, and then change ownership to the recipient? There is no comprehensive legal framework to answer the above questions. Regrettably for the electronic mail server and the professional who designs the system, these questions are not likely to be answered in the near future.

One possible business use of a computer is a database. A database is made up of records, which may describe people, as in the Census Bureau's database. When personal information is stored in a database, no series of queries should be able to isolate the information on any one individual.

The problem of preventing this isolation is called the inference problem. It is distinct from other classes of security problem, in that it can involve authorized people conducting authorized actions (queries).

Suppose the following were a database in a computer system.

NAME	SEX	SCHOOL	INCOME
Osgood	M	KSU	30000
Owens	F	KU	27000
Ostrum	F	KSU	53000
Orban	M	ESU	21000
Ozbrind	M	OTU	22500
O'Day	M	WSU	23750
Olson	F	PSU	34250
Orrman	M	CCCC	26500
Otto	M	JCCC	32250
Oppy	F	KSU	43300

The field values (except those under "NAME") can be used in queries. It should not be possible, for example, for someone to associate an income to a particular person, the income being "private" or personal data.

Some simple queries may ask for the number of records that are in a specified (query) set, or the sum of a numerical field in a query set. COUNT and SUM will be the designation for these queries. The query set may be selected by giving a characteristic formula which has data values and logical operators (& for AND, | for OR and ~ for NOT). The sample query COUNT (M | CCCC) asks for the number of records that have an "M" for sex or that have "CCCC" for school. In this case, the query would return the number six. The sample query SUM (CCCC | JCCC : INCOME) would return the value 58750.

Suppose that some user knew that Ostrum is a female and graduated from KSU. If the user issued the queries COUNT (F & KSU) and SUM (F & KSU : INCOME) the user would know from the results (1, 53000) that Ostrum is the only female from KSU in the database, and the user would have obtained her income, compromising her privacy.

There are several ways to protect the private information from being disclosed. The database could return a result only if the query set size is within a certain range, the database could distort the value returned, or the database could be partitioned somehow so that a query acts on partitions and not on individual records.

Setting a query set size provides superficial protection. It has been shown that a user can construct a "tracker" that will foil limits on query set size. A tracker is a characteristic formula that will provide an overlap of query results that can be manipulated to isolate an individual.

Suppose the database management system only returns results if the query set size is between three and seven. A user could query the system

for SUM (F : INCOME) and SUM (F & ~ KU : INCOME), subtract the results (157550 - 130550) and obtain Owen's income of 27000. Both query set sizes are within the allowable range (4, 3). Even if the query set size is restricted so that only queries accessing nearly one-half the database are answerable, trackers may still be found to compromise the privacy of individuals.

Distorting the value returned limits the statistical validity of the queries. This technique may be subverted by averaging enough results from the same query, or adding dummy records to the database and then observing the change.

Partitioning the database allows a user to query a group of records, but not an individual record. The problem with partitioning is that improperly formed partitions can reduce the statistical value of the database, it may be subverted by dummy records and the authorized insertion and deletion of records may be costly when the database must be re-partitioned.

Keeping track of overlapping query sets may work to stop trackers, but this technique involves storing a large amount of data for each user conducting queries, it may limit legitimate queries and would not work if two or more people were in collusion to compromise the database.

A few methods that may work to protect the privacy of the database are random-sample queries -- the query applies to a randomly picked sample from the normal query set, data-swapping -- values of fields are exchanged so that information on a particular individual is probably incorrect, and distorting the final result -- when the distortion is dependent on the query. All these methods are under study and refinement [DENN80b, BECK80, DOBK79].

Protection mechanisms must be employed when a database has personal or sensitive corporate information. This is certainly true for governmental agencies falling under the auspices of the Privacy Act. The Foreign Corrupt Practices Act (FCPA) of 1977[18] mandates that corporations reporting to the Securities Exchange Commission (SEC) must have internal controls sufficient to "maintain accountability of assets" and ensure that "access to assets is permitted only in accordance with management's general or specific authorization". A company may be violating this law even if there were no corrupt practices taking place. Furthermore, members of management may be held personally responsible for losses from inadequate controls by the shareholders. These losses may occur as privacy rights violation suits if the private information is disclosed to or inferred by unauthorized third-parties.

Not only is the company that owns the database responsible for the security of the system, but a computer scientist who designs or implements the system can also be liable for the protection and security of the system under the professional negligence laws. Nor would it be enough to claim that the system was used improperly or that the warranty disclaims responsibility for unauthorized disclosures; these defenses have been disallowed in some negligence cases. A computer scientist must design a database system such that - even if it is misused - it cannot, except under extreme circumstances, be compromised and release confidential information to unauthorized persons.

18. Foreign Corrupt Practices Act of 1977 PL 95-213-95th Congress

INDUSTRY CONCERNS

The guidelines for computer scientists to follow should be established by industry and government organizations. Industry has an obvious reason to be concerned with the standards and certain government organizations such as the Department of Defense (DoD) Computer Security Center (CSC) have a great deal of knowledge on the subject. These criteria would be used as a minimum standard which computer scientists would legally have to meet. Unfortunately, no one has completed a top-to-bottom, comprehensive study to suggest security practices and policies to be used. It would help significantly if security could be measured and quantified; it is difficult to apply a standard of security if one can not measure security.

The best-documented security metric (in a limited domain) is from the DoD CSC which has identified four divisions in which to classify systems that are being considered for processing and storing classified or sensitive information. Each division is a measure of trust that can be placed in a system and represents a major difference in the amount of trust or protection provided.

The divisions are named A, B, C, and D. The B and C divisions are further subdivided into classes of B1, B2, and B3, and C1 and C2, respectively. The divisions are hierarchically arranged with division A providing more trust or safeguards than division D. Likewise, within the B and C divisions, the higher the class number, the more security provided.

Each division and class has a set of requirements that must be met before a system may obtain that particular rating. These requirements are in four major areas:

(1) Security Policy - the system must enforce an explicit and well-defined security policy.

(2) Accountability - the system must be able to attribute certain actions to individuals.

(3) Assurance - an evaluation of the system must provide confidence that the system does what it is supposed to do and nothing else.

(4) Documentation - certain system documentation is required.

The requirements frequently mention the TCB (Trusted Computer Base). The TCB can be a security kernel, front-end device, or an entire operating system. It contains everything necessary to enforce the security policy. The requirements specify how the TCB should behave.

Division D (minimal protection) is assigned to systems that are evaluated by the Computer Security Center but fail to meet the requirements for any higher division.

Division C (discretionary protection) provides the ability to limit access to information using discretionary (need-to-know) policies and to audit certain user actions. C level systems are expected to be used in a single-level mode. Users are to specify control and access of shared objects. The C2 class provides finer granularity of access control than does C1, and also provides more complete audit information.

Division B (mandatory protection) classification is given to systems that implement mandatory protection schemes. To do so, the system must have sensitivity labels on the major objects it manipulates. A sensitivity label is a marking of an external level (Top Secret, Secret, Confidential,

and Unclassified) that represents the minimum clearance level accepted of an individual who wishes to access the object. These labels must be protected from tampering. Developers must provide the formal security model that the TCB implements and present evidence that demonstrates that the three concepts (complete, tamperproof and verifiable) of a reference monitor have been implemented.

Systems in the B1 subclass must maintain labels for major objects. The B2 subclass addresses covert (storage and timing) channels and extends the enforcement mechanisms in B1 to cover all objects in the system. The B2 rating increases the requirements for configuration management, documentation, and authentication mechanisms. The documentation includes a DTLS (Descriptive Top Level Specification) of the TCB. The DTLS completely and accurately describes TCB behavior. The notion of a trusted path is introduced. A trusted path is a communication path to the TCB that is opened by the user and provides the user confidence that he is talking to the TCB during login and authentication proceedings.

Designers and implementers employ software engineering techniques to minimize the complexity of the TCB for a B3 rating. They must exclude code not essential for security policy enforcement. System recovery techniques and support of a security administrator are required. The DTLS must be demonstrated to be consistent with the security model.

Division A (verified protection) requires no new architecture or security policy. The increase of trust placed in systems with this rating derives from the analysis from formal design specifications and verification techniques. More rigid configuration management controls are required, as well as procedures to ensure trusted distribution of the TCB

to sites.

This rating system was originally designed to provide a metric for evaluating systems, as guidance to manufacturers, and as a basis for specifying security requirements for acquiring systems. It is important to note that the requirements do not form a complete description of preferred security practices. Rather, the domain considered has been limited to the behavior, design, and implementation of the TCB. Encryption, enforcement, and external security needs have all been excluded from consideration in this rating system. Thus the CSC has defined the limits in which they are evaluating security.

The DoD metric is limited in what it measures; other areas of security ought to have a metric also. Metrics should be proposed and accepted and then propagated through-out the computer science community. One obvious way to do this is through professional organizations such as the ACM, DPMA or AFIPS; although it has been suggested [WARE84] that the General Services Administration (GSA) be tasked with this duty. Certainly some organization should document standards and propose metrics that cover security areas outside what the CSC has already done.

Among the guidelines may be suggestions for the mandatory certification and evaluation of computer scientists. This would help identify those persons lacking some skill or knowledge that all computer scientists should have acquired. It may also serve to separate the true professional from the mere technician. Special interest examinations and organizations also must be developed to further delineate special areas of expertise. This would be similar to the medical profession which has a fairly universal organization (the American Medical Association) as well as other special

interest organizations (such as the American College of Obstetricians and Gynecologists).

It is important to realize that meeting a governmental or industrial standard does not exclude one from liability in a negligence suit. These standards are taken to be minimum standards only. Although a failure to meet a standard may be taken as evidence of negligence per se, merely meeting the standard is not enough.

In Berkebile vs. Brantly Helicopter Corporation[19], a pilot who took off in a helicopter with a nearly empty fuel tank crashed and died. His widow brought suit charging that the one second time span allowed (for putting the helicopter into auto-rotation mode) by the helicopter's designers was not enough time. The helicopter company argued that the one second time span was an FAA standard. The FAA standard indicated that the one second was the minimum time to be allowed and the court ruled that meeting the government standard was not adequate if a reasonable man would have done more.

This may be especially true when examing the Data Encryption Standard (DES). The DES was designed by IBM aided by the National Bureau of Standards and the National Security Agency. Use of encryption is fast becoming a standard in the financial world. If an organization believes that using the DES will stop all lawsuits from the encryption protection needs because it is using a technique the government sanctions, it is wrong. Given that arguments have been made about the integrity of DES and the proposal that encryption standards be revised every five to seven years, a reasonable man

19. Berkebile vs. Brantly Helicopter Corp. 462 Pa. 83, 337 A.2d 893 (1975)

may use a different technique, or may put two DES chips in parallel to double the size of the key and prevent attacks from penetrating that layer of security.

ACTIONS

There are many things that computer scientists and industry as a whole can do to limit legal liability for systems and products. The individual can apply certain principles during work on a project while industry pushes for broad guidelines that will help establish standards for the computer scientists to follow. The first thing computer scientists should do when working on a product beyond the initial requirements phase is to ensure safety through good design. A risk analysis study is essential to guarantee an adequate measure of security for assets already in place. When initially designing a system, a process similar to risk analysis should be completed. Both of these processes are described below.

The purpose of risk analysis is to identify assets in need of protection, ways in which the assets may be destroyed or damaged, and ways to counteract threats against the assets. First the process of risk analysis is described, and then some added considerations are examined. There are three main areas to the process of risk analysis.

First, all data processing assets should be listed and a set of values given to them. These assets include tangible assets such as computers, disk drives, printers and other hardware, as well as intangible assets such as software. Software can include both the programs and processes to which the system has access as well as data and information stored in the system. Intangible assets can also include the privacy of confidential data kept on the system, the providing of services to users, and the integrity of stored objects.

The values associated with each asset are a projection of the worth of the asset to the organization. Each asset may have several values which could represent varying degrees of disruption. No item should be excluded from this step because the purported value of the item is too small.

Personal responsibility should be assigned for each asset. If possible, a single person should be given the responsibility to ensure the correct handling of the item, should help detail how the asset may be accessed and by whom, and should propose a means of logging transactions regarding the asset. Access should be based on need-to-know or the least-privilege-necessary principle. It should be difficult for users to misuse their capability to initiate a transaction with the asset and they should be prohibited access to assets to which they do not have access privilege.

The second major step in risk analysis is to enumerate all the potential threats and vulnerabilities of the system. Threats include all the natural, accidental and intentional events that may adversely affect the system. Included in this step should be an evaluation of frequency and possible impact of each threat. Usually, the high frequency threats will have a less severe impact than the low frequency events. For instance, the power may fail several times a year, but one does not expect an earthquake every few months.

Threats should be ranked according to risk. Risk is the interaction of probability and expected loss. The formula:

$$Ri = P \times L$$

may be used. Ri is the risk factor for event i, P is the probability for event i occurring, and L is the projected loss if i does in fact occur.

At this point, it is useful to compare the cost of the countermeasures to the cost of the threat to the asset. Documenting this comparison may be useful later if the question of whether the manufacturer's burden was greater or less than the cost of the risk times the impact on the asset.

After listing and ranking the threats, management should examine potential countermeasures -- actions they can implement to foil the threats and decrease risk to the system assets. Management may want to first designate a minimum level of security necessary to achieve an adequate security policy for their needs. Countermeasures to each threat and the interaction of those countermeasures together should be examined in some detail. Since resources may be limited, it is important to consider organizational goals and capabilities. Those countermeasures that best reduce the risk while not violating some organizational goal should be accepted for implementation.

A distributed system will have a more complicated risk analysis than a centralized one because of the intrinsic nature and greater flexibility of access from a distributed system. A threat, for example, may not originate at the same node that is attacked, but from some other node in the net. The added layers of protocol complexity allow for a greater chance of error and thus lower the amount of trust one can place in the system. Also, in addition to the other hardware, the entire communication net must be analyzed for threats and countermeasures.

A means of implementing the chosen security measures should be designed and responsibility for each step should be detailed along with a plan of testing and evaluating countermeasures. The entire risk-assessment procedure should be reinitiated at appropriate time intervals as evolving

threats, advances in security measures possible, and fluctuating values in assets make this re-evaluation necessary. Re-initiating this process will promote security measures that are timely and state-of-the-art.

Another process similar to risk analysis should be conducted during the initial design and be continued on through the implementation phase. A risk analysis helps management decide whether the controls and safeguards in place are adequate to protect assets against certain threats; this second process helps management and designers determine what safeguards should initially be built into the product. The documentation from this process may be used in court to answer questions about the design and alternative designs of a product.

The first step to this process is to describe the environment for which the product is designed. This includes a description of the uses and users of the product. The uses should already be documented through a previous design phase. A description of the users would include an evaluation on their sophistication and prior knowledge of like systems. An application package may be a word processor designed for the novice, or it may be a sophisticated software tool for the experienced user. Users may be from a static, rigidly controlled pool such as a military organization, or they may be from a more dynamic, open group, such as from a university.

A method needs to be employed to determine the value of sensitive data and operations. Also during this phase a comparison with like products should be undertaken. Using state-of-the-art technology and safeguards is not an absolute defense to all lawsuits, but it may be helpful in alleviating liability in some cases.

The next phase is to enumerate the hazards the system is likely to encounter. Hazards should include such obvious threats as unauthorized users trying to logon and users attempting unauthorized actions. Activities that are not so obvious should also be included -- even ways the system can be misused. Although the natural reaction to potential harm from misuse or abuse of a product may be to supply a simple warning, this is not always acceptable to the judiciary. Foreseen misuse must be planned for and steps must be taken to limit the damages from abuse of the product, or the designer may lose a negligence or Strict Liability suit.

The last step to take for this process is to compare the trade-offs or vulnerabilities that occurred in the design of the product. Differences between the system-to-be and other similar commercial systems should be detailed, and the impact of the differences on the security performance should be projected. Alternative designs, ones not found in other products or the proposed one, should likewise be examined. The effect of these differences (between other products and different designs) should be examined in some detail. If these differences would produce other hazards and risks to the system, those new threats should be noted. The usefulness of the product may also be adversely affected by design differences; designers should note a change that reduces risk but eliminates the utility of a product were a design change be implemented.

If the cost of the system would be changed by the alternatives, estimates and the method of calculating the increase should be documented. Special instructions and warnings may be planned, even though warnings do not totally mitigate responsibility for the system's safe design.

SUMMARY

Although most of the laws legislating privacy apply to government agencies, the desire "to be let alone" and the power of computers will eventually lead to increased restrictions on computer systems. Designers can start following the Code of Fair Information Practices' guidelines. Failure to adequate protect sensitive information may lead to lawsuits based on negligence.

Shareholders may sue corporate management if internal controls are not sufficient to protect corporate resources and citizens may sue if information that is personal about themselves is released to unauthorized third parties. Because computer scientists are probably professionals, they must exercise greater care in their practice to ensure safety and integrity when working on computer systems. Computer scientists will be liable for the effects of their work to those people who are specifically foreseen, although possibly excluding those people who are merely foreseeable.

Two computer science applications have been examined in some detail; electronic mail which may transmit sensitive information and which may possibly be seized by law enforcement officials, and databases which may contain personal information that may be inferred from a series of queries using trackers.

A metric for measuring security has been discussed along with the need for a more comprehensive way of determining the total security level of a system. Guidelines for security should be promulgated by industry and government, and then used by individual computer scientists as a "floor" of

safety to design into systems.

WEST83 Westermeier, J., T. "Legal Implications of Computer Security" Advances in Computer Security Management, Vol. 2 Wofsey, M.M. Editor 1983 John Wiley & Sons, Ltd.

WEWE81 Wewer, William "Protection of "Privacy"; Federal Laws Regulating Fair Information Practices", DP & the Law 1981

WEIN78 Weinstein, Alvin S., Twerski, Aaron D., Piehler, Henry R., Donaher, William A. "Products Liability & the Reasonably Safe Product -- A Guideline for Management, Design and Marketing" John Wiley & Sons, 1978

WOOD80 Wood, C., Fernandez, E.B., and Summers, R.C. "Data Base Security: Requirements, Policies, And Models" IBM Systems Journal, Vol. 19, No. 2, 1980

WOOD82 Wood, Charles C. "Future Applications of Cryptography" Computers & Security Vol. 1, No. 1 1982

Bibliography

BECK80 Beck, Leland L. "A Security Mechanism for Statistical Databases" ACM Transactions on Database Systems, Vol. 5, No. 3, September 1980

BOUN81 Bound, Lt. Cmdr William A.J. "Office Automation Systems: Problem Area of the '80's?" Security Industry & Product News Nov. 1981 Vol. 10, Nbr. 11

BROW83 Browne, Peter S. and Bigman, Robert Y. "Federal Legislation and Impact on Security Management" Advances in Computer Security Management, Vol. 2, Wofsey, M.M. Editor 1983 John Wiley & Sons, Ltd

BONY83 Bonyun, David A. "The Use of Architectural Principles in the Design of Certifiably Secure Systems" Computers & Security Vol. 2, No. 2 1983

BROO81 Brooks, Daniel T. "Liability for Porfessional Negligence (Malpractice)" DP & the Law 1981

CAMP79 Campbell, R.P. and Sands, G.A. "A Modular approach to Computer Security Risk Assessment" AFIPS Conference Proceedings, Vol. 48 1979

CONW72 Conway, R.W., Maxwell, W.L. and Morgan, H.L. "On the Implementation of security Measures in Information Systems" Communications of the ACM Vol. 15, No. 4 April 1972

DENN79 Denning, Dorothy e. and Denning, Peter J. "Data Security" Computing Surveys, Vol. 11, No. 3, September 1979

DENN79b Denning, Dorothy E., Denning, Peter J. and Schwartz, Mayer D. "The Tracker: A Threat to Statistical Database Security" ACM Transactions on Database Systems, Vol. 4, No. 1, March 1979

DENN80 Denning, Dorothy E. and Schlorer, Jan "A Fast procedure for Finding a Tracker in a Statistical Database" ACM Transactions on Database Systems, Vol. 5, No. 1, March 1980

DENN80b Denning, Dorothy E. "Secure Statistical Databases with Random Sample Queries" ACM Transactions on Database Systems, Vol. 5, No. 3, September 1980

DoDC83 Department of Defense, Computer Security Center "Department of Defense Trusted Computer System Evaluation Criteria" CSC-STD-001-83 15 August 1983

DOBK79 Dobkin, David, Jones, Anita K. and Lipton, Richard J. "Secure Databases: Protection Against User Influence" ACM Transactions

on Database Systems, Vol. 4, No. 1, March 1979

FREE84 Freedman, Warren "Products Liability for Corporate Counsels, Controllers, and Product Safety Executives" Van Nostrand Reinhold Company 1984

GRAY83 Grayson, William C. "Vulnerabilities of Data Telecommunications Systems" Advances in Computer Security Management, Vol. 2 Wofsey, M.M. Editor 1983 John Wiley & Sons, Ltd.

KITT83 Kittelberger, Kenneth L. "Scope of Computer Security Problems" Advances in Computer Security Management, Vol. 2 Wofsey, M.M. Editor 1983 John Wiley & Sons, Ltd.

KOLA77 Kolata, Gina Bari "Computer Encryption and the National Security Agency", Science, Vol. 197, No. 4302, 29 July 11977

ORCE75 Orceyre, M.J. "Data Security" Journal of Chemical Information and Computer Sciencies, Vol. 15, No. 1, 1975

SALT75 Saltzer, J.D. and Schroeder, M.D. "The Protection of Information in Computer Systems" Proceedings of the IEEE Vol. 63, No. 9, March 1975

SALT80 Salton, Gerald "A Progress Report on Information Privacy and Data Security" Journal of the American Society for Information Science March 1980

SALT83 Saltmarsh, Timothy, J. and Browne, Peter S. "Data Processing - Risk Assessment" Advances in Computer Security Management, Vol. 2 Wofsey, M.M. Editor 1983 John Wiley & Sons, Ltd.

SCHW84 Schweitzer, James A. "Personal Workstation Automation Security Vulnerabilities" Computers & Security Feb. 1984 Vol. 3, Nbr. 1

TURN76 Turn, R. and Ware, W.H. "Privacy and Security Issues in Information Systems" IEEE Transactions on Computers, Vol. C-25, No. 12, December 1976

VOYD83 Voydock, Victor L., and Kent, Stephen T. "Security Mechanisms in High-Level Network Protocols" Computing Surveys, Vol. 15, No. 2 June 1983

WADE83 Wade, James R. "Physical and Personnel Security Considerations for Data Processing Systems" Advances in Computer Security Management, Vol. 2 Wofsey, M.M. Editor 1983 John Wiley & Sons, Ltd.

WARE84 Ware, Willis H. "Information Systems Security and Privacy" Communications of the ACM, Vol. 27, No. 4, April 1984

Legal Requirements of Secure Systems

by

Joseph M. Beckman

B.S., Kansas State University, 1982

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Computer Science

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1985

ABSTRACT

This paper examines the role certain legal requirements play in the design of and subsequent liability for systems produced by computer scientists. First, the requirement for information privacy is examined. Many statutory and judicial laws outline the need for ensuring privacy in certain systems. A Code of Fair Information Practices has been established and has been partially implemented in statutory law. These laws apply mainly to government agencies and certain consumer reporting agencies in the private sector. Information may also be forcibly disclosed against the wishes of the nominal owner.

Negligence is the basis for law suits when a person has been injured through the carelessness of another who owed the injured a greater amount of care. The amount of care is greater in the case of computer scientists through virtue of their occupational status of being professionals. Who is entitled to this greater standard of care is an important point, as a computer system can affect a wide population. The matter has been addressed by the judiciary through a number of cases.

Electronic mail and databases are examined in detail to highlight areas where legal requirements would effect the design and where questions of potential liability arise. Both areas may involve personal or sensitive information that must be protected from loss or disclosure to unauthorized third parties.

A metric for an evaluation of security, provided by the Defense Department's Computer Security Center, is examined. Because this metric is not inclusive of all areas of security, industry or government should work towards providing means to evaluate security in a comprehensive manner. The subsequent guidelines may be used then by individual computer scientists while working on systems. If followed, these guidelines would not absolve professionals of liability for negligence, but provide a minimum standard below which the professional is liable for negligence per se.