/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].