
John Morihara

Follow this and additional works at: https://repository.law.uic.edu/jitpl

Part of the Computer Law Commons, Health Law and Policy Commons, Internet Law Commons, Medical Jurisprudence Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

https://repository.law.uic.edu/jitpl/vol3/iss1/19

This Comments is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.
COMPUTERS, THE DISCLOSURE OF MEDICAL INFORMATION, AND THE FAIR CREDIT REPORTING ACT

I. INTRODUCTION

The right of the individual to privacy has been recognized in American jurisprudence since 1890. Today, with the widespread use of computers and their ability to store countless bits of information on every man, woman and child in America, this fragile privacy interest is threatened as never before. Although this threat is pervasive throughout many areas of society, this Note will focus upon the specific problem of the unnecessary disclosure and misuse of sensitive medical information. Suggestions on how an existing piece of legislation, the Fair Credit Reporting Act, could be amended to help control this problem will be proposed.

II. COMPUTERS AND PRIVACY GENERALLY

The use of computers and the interconnecting data networks that support them have rapidly expanded in the past few decades, and show every promise of continued expansion.

In part, the increased use of computers reflects growing technological capability. The state of the art has reached the point where it is actually "cheaper today to store information than to destroy it. To destroy generally requires that the data be run through the computer, consuming expensive time." In part, the increased use of computers reflects an increasing

2. A few of the controversial issues that face society today include the use of social security numbers as a universal identifier, direct access computers that allow for the possibility of monitoring, and interconnecting data networks.
demand by society for information and instant transactions. People have grown accustomed to credit cards which provide instant credit approval, and the ability to make travel reservations all over the world in a matter of minutes. When the government is involved, people expect social security, unemployment compensation, welfare, and a host of other services to be rendered quickly.

These systems need information to function, and vast, virtually uncontrolled networks of interchanging information systems have arisen to meet these needs. There are today about 2500 credit bureaus in the United States. The largest of these bureaus has files on about one hundred million people. Today when an individual applies for life insurance, buys on credit, opens a bank account, seeks hospitalization or insurance benefits, he will be slipped quietly into this vast web of information. Consider the signing of an application, for instance, the insurance form. This form "authorizes any organization to release all information, not just medical data, it may have about a person; it has no expiration date; and it indicates that a copy is as valid as the original."

Private companies routinely disclose confidential data about their employees upon request by a federal agency. Approximately 41% of the companies in one survey had no policy at all regarding the disclosure of such information.

A 1971 survey of fifty-four government agencies revealed that they had compiled 858 data files, ranging in size from ten records to 204,000,000 records. These files consisted of three major types of data banks: administrative, evaluative, and statistical. Of the data files, at least twenty-nine (such as the Debarred Bidders List and the FCC Blacklist) had been established for the apparent purpose of black-listing people. These are but a few examples of how the personal interest in privacy is under increasing pressure from the growing use of computers.

This assault on personal privacy falls into three general areas of

6. Linowes, supra note 4, at 1182.
7. Id.
9. Id. at 782.
10. Almost two-thirds (63%) of government data banks had no basis of express authority for their creation. Often the only reason for their creation was the agency's belief that it would facilitate their actions. Sixty percent of federal agencies allow other federal agencies some degree of access to their files. Twenty-five percent of federal agencies allow direct access by routine distribution of data or computer interface. Id. at 783.
concern: the actual invasion of privacy, misinformation, and pressures for greater conformity. The specific concern of this Note, disclosure and misuse of medical information, touches mainly upon two of these concerns, the invasion of privacy and misinformation.

The problems that evolve from the inclusion of misinformation in computer data banks are apparent. Keypunch or other operator error may result in the denial of applications for credit, jobs, housing, or insurance.

The threat of the invasion of personal privacy from computer usage is a little more amorphous and difficult to express. Although it has not been conclusively demonstrated that privacy is a basic human right protected in the federal Constitution, there is convincing evidence that privacy is not only a value of human beings, but also a basic human need.

One authority has identified four basic privacy needs: solitude, intimacy, anonymity, and reserve. It is the value of anonymity which is the most threatened by the computer revolution. One expert has explained that who you are is the “face” that others see, and the face you show others is based on the information about yourself that you choose to release. As computer files increasingly gather information about each individual, the information individuals wish to release about themselves slips further and further away from their control. Each individual gradually loses more and more control over which of their faces other people see.

III. THE PRIVACY INTEREST IN THE LAW GENERALLY

A. Torts

The common law has slowly recognized an evolving right to privacy under the law of torts. In one form or another, the right of privacy has been recognized and accepted in all but a few jurisdictions. One noted authority has divided the complex field of tort law that protects privacy into four divisions. These four divisions, though varied, establish the right of the individual to be left alone. These four areas include appropriation, intrusion, public

11. See infra notes 23-24 and accompanying text.
13. Id. at 17.
16. Id.
17. Appropriation is the using of the name or likeness of another for the defendant's benefit without that person's consent. Id.
disclosure of private facts,\textsuperscript{19} and false light in the public eye.\textsuperscript{20} Although it would seem that the last two of these tort remedies would suffice to alleviate any problems with the disclosure of private medical information, these torts require that the information be exposed to publicity. Often although the medical information in question is circulated among private parties who have no legitimate interest, such circulation is too limited to constitute publicity.\textsuperscript{21} In addition, these torts are subject to certain defenses which might well mitigate their effectiveness in this case.\textsuperscript{22}

\textbf{B. The Constitutional Right of Privacy}

The right of privacy has also been recognized by the United States Supreme Court in a number of decisions. The Court has recognized an individual's right to control the image of himself which he presents to the world.\textsuperscript{23} As the Court said in \textit{Whalen v. Roe},\textsuperscript{24} "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."

The Court, in developing protections for the privacy interest, has relied upon four different Constitutional amendments. The first and fourth amendments have been the source of protection of the

---

\textsuperscript{18} The tort of intrusion comes in different forms. It may reflect simple intrusion into the physical solitude of another, eavesdropping via wiretapping or microphones, peering into the windows of a home, or persistent and unwanted telephone calls. The intrusion must be something which would be offensive or objectionable to a reasonable man, and the thing into which there is intrusion must be something which is, and is entitled to be, private. \textit{Id.} at 807-09.

\textsuperscript{19} Public disclosure of private facts occurs when highly objectionable publicity is given to private information about the plaintiff. This tort may arise even when the publicity is factually true, and no action would lie for defamation. The disclosure here must be a public one; information disclosed to an employer or even a small group does not constitute public exposure. The matter made public must be one which would be offensive and objectionable to a reasonable man of ordinary sensibility. The publicity must be given to facts which the community would ordinarily regard as highly objectionable or offensive. \textit{Id.} at 811.

\textsuperscript{20} False light in the public eye is based upon an attribution of some opinion or utterance made to the public. The attributed statement must be something that would be objectionable to the ordinary reasonable man. \textit{Id.} at 812-13.

\textsuperscript{21} \textit{Id.}

\textsuperscript{22} Some of the traditional defenses to these tort claims are the constitutional right to report on and discuss public figures and news, consent of the plaintiff, and reasonable investigations of credit and/or insurance claims. \textit{Id.} at 814.

\textsuperscript{23} L. Tribe, \textit{American Constitutional Law} 888 (1978).

\textsuperscript{24} 429 U.S. 589, 605 (1977). Although this case did not expressly address the issue of unwarranted disclosure of private data, it found New York's disclosure/safeguards sufficient.
individual's expectation of freedom from government intrusion.\textsuperscript{25} The Court has gone so far as to say that "the principal object of the Fourth Amendment is the protection of privacy rather than property."\textsuperscript{26} The Supreme Court has also used the ninth and the fourteenth amendments and the concept of the penumbra to create a zone of privacy in which the individual is guaranteed a certain degree of liberty to make his personal choices, free from the fear of government intervention.\textsuperscript{27} The Supreme Court, however, has not yet formulated a clearcut general doctrine to protect personal information or privacy. In fact, some cases seem to cut the other way.

In \textit{United States v. Miller},\textsuperscript{28} the Court upheld a request by government officials to gain access to bank copies of checks written by bank depositors. The Court found that neither a fourth amendment interest nor any legitimate expectation of privacy was involved on the part of the depositors.

When the Supreme Court has intervened, it has been most adamant about the protection of a privacy interest if the violation of this interest would infringe upon some other constitutionally protected interest. For example, a state court order which required an organization to produce a membership list might impede the freedom to associate.\textsuperscript{29}

Even if the Supreme Court should decide to actively promote a personal right of privacy, barriers to effective application would still exist. In cases involving the private sector, the Court must find some showing of state action in order to become involved. There must be some "pervasive interdependence." Mere state regulation of business will not suffice.\textsuperscript{30}

Another difficulty with reliance on a judicial solution to this problem is that courts limit their decisions to the facts before them. It is unlikely that a judicial approach will lead to a comprehensive set of guidelines or, even more importantly, that such an approach can keep pace with the rapid rate of technological innovations in the computer and information processing field.


\textsuperscript{26} Warden v. Hayden, 387 U.S. 294, 304 (1967).


\textsuperscript{28} 425 U.S. 435 (1976).

\textsuperscript{29} NAACP v. Alabama \textit{ex rel.} Patterson, 357 U.S. 449, 461 (1958).

\textsuperscript{30} Murdock, \textit{supra} note 27, at 597 (citing L. Tribe, \textit{AMERICAN CONSTITUTIONAL LAW} 1171 (1978)).
The federal government has made some attempts to control the eroding right of privacy through statutes which regulate those agencies whose activities would threaten privacy. Five of these statutes are set forth below.

1. **Privacy Act of 1974**

   This important piece of legislation was intended to help control the dissemination of government data records by encouraging non-disclosure. It requires the written consent of the party who is the subject of the file before disclosure to third parties. It regulates and limits that data collected to data which is relevant and necessary to accomplish a legitimate agency purpose. It allows an individual access to his own records upon request and provides for procedures whereby an individual may challenge perceived inaccuracies in his records.

2. **Right to Financial Privacy Act of 1978**

   This statute was enacted in response to the outcome of *United States v. Miller* and effectively overruled the Supreme Court's decision in this case. The Act basically further protects an individual's financial records held by financial institutions from unauthorized government access.

3. **Family Educational Rights and Privacy Act of 1974**

   This Act provides that no federal funds will be available to any educational agency which has a policy of denying parents and students of majority age the right to inspect and review relevant educational records. It also restricts disclosure of educational records to school officials who perform organizational functions, to state or federal educational agencies, and to state or federal authorities pursuant to statutes in those jurisdictions.

---

32. Id. § 552a(b).
33. Id. § 552a(e).
34. Id. § 552a(d).
35. Id. § 552a(g)(1).
39. Id. § 1232g(b)(1).
4. *The Freedom of Information Act*[^40]

This Act is intended to preserve the individual's access to government information. Through this Act, an individual is allowed access to agency opinions, policy statements, manuals and instructions, that affect the public interests.

5. *The Fair Credit Reporting Act*[^41]

This Act restricts the information activities of private credit and investigatory agencies. This Act will be analyzed in depth in subsequent sections of this Note.[^42]

IV. THE SPECIFIC PROBLEM OF MEDICAL INFORMATION

One member of a state commission on privacy characterized the problem of misuse of computerized information as follows:

Undeniably, information technology is an integral part of modern society. As this technology has become more sophisticated and more accessible to a vast range of commercial use, the potential for use—and abuse—has increased geometrically.

Today, computers store (and release) rather comprehensive profiles: our spending habits, our credit histories, our medical histories and our employment records. In seconds, a high speed printer can disgorge more information about you than you are likely to be able to remember.[^43]

One recent article recognized the problem of the disclosure of medical information by data corporations, especially large information bureaus.

From birth on, medical records pile up. Notes on diagnoses, symptoms, medications, test results, previous illnesses and responses to treatment form the bulk of the record. But the file may also contain facts about your personal life and family history. As a recent government report on privacy put it, "Medical records contain more information, are more available to more users, are less well-controlled and are used for more non-medical purposes than ever before."[^44]

Another recent article dealing with the same problem stated:

Whether they are kept in a doctor's office, a hospital or company medical office, many parties could probably get their hands on your files in a flash without your knowledge. Among them are govern-

[^42]: See text accompanying infra notes 65-101.
ment agencies, the Medical Information Bureau (a huge data bank), the Secret Service and other law enforcement agencies, insurance companies and even credit investigation bureaus. 45

Of special interest here are the activities of behemoth information bureaus, such as the Medical Information Bureau (hereinafter referred to as the MIB), which use their vast resources and computer data banks to collect an overwhelming amount of information on individuals. The MIB collects files on over eleven million Americans and Canadians and allows access to its files by over seven hundred insurance companies. These companies write almost 95% of the insurance policies in this country. 46

Although these files contain medical records supplied by the insurers themselves, 47 the files also contain nonmedical information, such as sports participation and driving records. Such files also used to include records of sexual deviance and social maladjustment, but the Bureau began to purge these a few years ago. 48

Insurance and credit companies often gather much more information than they need.

[I]t has become readily apparent that some of the information requested on applications is simply not necessary for the purpose at hand. For example, life-style questions are irrelevant when you are seeking a homeowner’s policy, and educational background is immaterial to a medical history. Yet both continue to be sought by the respective providers. 49

Another and perhaps more serious problem occurs when this excessive amount of collected information is passed on to still other parties who use the medical files in ways that have no relation to the maintenance of quality health care. The medical files may be used in the employment field to deny a promotion or even a job. 50 This danger is especially real in situations where an employer has paid for group health insurance for its employees. The employee may sign an insurance claim or application authorizing the disclosure of medical records, not realizing that the insurance company will freely disclose the medical file to the employer.

Doctors are concerned that dissemination of medical information can actually threaten certain aspects of the medical treatment. Dr. Milton Sirota, the director of Psychiatric Counseling and Referral Associates in New York City complains that “the absence of con-

45. Odening, Protecting Medical Records, 126 FORBES 165 (Dec. 8, 1980).
46. Young, Your Health, Their Business, 13 NEW YORK 40 (Oct. 27, 1980).
47. Id. at 42.
48. Id. at 43-44.
49. See Feldman, supra note 43.
50. See Young, supra note 46, at 40.
fidentiality often makes it impossible to bring the kinds of material into the treatment process that should be there, and that can only destroy the effectiveness of psychotherapy."

Medical information can be used or misused by these secondary receivers in a variety of ways. It may be used as social gossip so that the patient undergoes the very distressing experience of finding out that his or her medical record has suddenly become the talk of the water cooler crowd. Such information may be misused by an employer. In an outrageous example, one employer used a psychotherapist's report from a family clinic to threaten an employee who had not even been allowed to see his own medical file. Such threats ultimately culminated in the employee's discharge.

Abuses such as the above are greatly exacerbated by the problem of misinformation, resulting either from misinterpretation or from data that is actually incorrect.

The relevance and significance of a particular piece of information depend upon the context in which the information is being used. Random interpretations of information for a purpose other than the one in which it was provided can lead to serious misinterpretation and erroneous conclusions.

The problem of abuse is especially serious when the information being dealt with is of a highly specialized, technical nature, as medical information so often is. Even if medical information is properly disclosed and should not be damaging to the individual's interests, "[y]ou can't always count on the recipient's being capable of interpreting the data. Many of the tentative, even speculative notations by doctors should not be in the hands of middlemen, such as personnel people who are unqualified to judge their significance."

Some employers or insurance personnel may be unduly swayed, for example, by family histories of cancer, mental disease, alcoholism, venereal disease, or drug addiction.

Moreover, problems of abuse may be magnified by disclosure of medical information that is simply incorrect. While the problems which may result from disclosure of incorrect information are readily imaginable, three additional considerations serve to heighten the problem. First, the medical records themselves may be in error. One survey of hospital records showed that over 20% of the complex hospital charts were in error. Second, once an error reaches the computer data banks, it is seldom corrected because so few people

51. Id. at 41.
52. The employee subsequently settled out of court. Id. at 40.
53. See Feldman, supra note 43.
54. See supra note 44, at 41.
55. Id. at 42.
actually know what is on any given file.\textsuperscript{56} Third, the data collected by information bureaus such as the MIB is unscreened by the collecting agency and is accepted directly from contributing insurance companies. MIB has no investigators of its own and no way to verify information it may receive.

Computers are playing an increasingly direct role in medicine. Computers already play a major role in record keeping, and the day is not too far off when they will aid in diagnosis and monitoring.\textsuperscript{57} Patient histories will soon be stored directly in computer banks.\textsuperscript{58} It is not difficult to imagine therefore what will happen to personal medical privacy if computers are hooked directly with data banks at the MIB. Clearly there is a need for private individuals to begin to defend their privacy interests.

\textbf{V. PROPOSED LEGISLATION}

In 1980, the United States Senate attempted to pass legislation to address the problems of misuse of medical information.\textsuperscript{59} The law which was proposed, the Privacy of Medical Information Act,\textsuperscript{60} placed a two year limit on the effectiveness of signed general consent agreements. After two years, the agreement would have to be resigned to be valid. The Act also attempted to standardize procedures for those with legitimate concerns to get access to medical files. Stiff penalties were proposed to punish investigators who obtained files under false pretenses. Under the proposed Act, each medical file would include the names of all agencies or individuals who had consulted a file. The Act would also have allowed patients access to their files in their doctor's office or in a company's medical office.\textsuperscript{61}

Unfortunately, the Privacy of Medical Information Act was defeated in late 1980 due to the efforts of its two major opponents, law enforcement and intelligence authorities and the medical community. Law enforcement and intelligence authorities opposed the Act because they felt that it would only further complicate their job. Members of the medical community were opposed because they felt that it might ultimately result in even greater disclosure of medical information.\textsuperscript{62}

\begin{footnotes}
\item[56] \textit{See} Young, \textit{supra} note 46, at 40.
\item[57] \textit{L.A.} Times, Sept. 1, 1982, at col. 5.
\item[58] Hannay, \textit{An Information Society}, 46 \textit{Vit. Speeches Day} 461, 463 (1980).
\item[60] \textit{Id}.
\item[61] \textit{See} Feldman, \textit{supra} note 43; \textit{see also} Odening, \textit{supra} note 45, at 167.
\item[62] \textit{Id}.
\end{footnotes}
VI. THE FAIR CREDIT REPORTING ACT

This Note contends that existing legislation, the Fair Credit Reporting Act, could be amended to create a fairly effective tool which would help to control abuses in disclosure of medical information.

The Fair Credit Reporting Act, (hereinafter referred to as FCRA) was passed in response to legislative concern about the use and misuse of information gathered by credit and investigatory agencies. These concerns paralleled those regarding the improper disclosure of medical information.

FCRA is based on the general theory that by creating an avenue of communication between the consumer and the agencies which report on the consumer, a dialogue can be established which will result in a self-correcting flow of information.

The Act requires that the information agency disclose to the consumer the nature and substance of his file upon the consumer's request. The Act also provides that such information shall be available at reasonable times and establishes procedures for consumers to dispute any perceived inaccuracies in their files.

The behavior of investigatory agencies is further controlled by means of FCRA sections which specify additional regulations and penalties for noncompliance with the Act. One section in particular deals with fairness in collection and prohibits the use of certain ob-

---

64. The problems created by credit investigations were in many ways similar to the problem of medical information now before us. On the one hand Congress recognized a legitimate need by business and society for this credit information. On the other hand the problems of information abuse, careless dissemination, and inaccurate investigations, all aggravated by general consumer ignorance of the existence and contents of these reports, demanded some Congressional action. The FCRA was intended to meet both these needs; it provided consumers with information while holding investigative agencies to general standards of conduct.
65. The Fair Credit Reporting Act provides: “Every consumer reporting agency shall, upon request and proper identification of any consumer, clearly and accurately disclose to the consumer: (1) The nature and substance of all information (except medical information) in its files on the consumer at the time of request.” 15 U.S.C. § 1681g(a)(1) (Supp. IV 1980).
66. “A consumer reporting agency shall make the disclosures required under section 1681g of this title during normal business hours and on reasonable notice.” 15 U.S.C. § 1681h(a).
67. 15 U.S.C. § 1681i provides procedures for disputing inaccuracies in reports. Section 1681i(a) mandates reinvestigation for nonfrivolous complaints. Section 1681i(b) allows for a consumer to include his version of the dispute in his file. Section 1681i(c) requires that subsequent users of the report be notified of the dispute, and section 1681i(d) provides that if inaccuracies are deleted the consumer may request notification of past subscribers of his file for the proceeding two years.
The FCRA section dealing with the dissemination of information lists permissible uses of consumer reports and imposes burdens on the consumer reporting agency to know the uses to which its reports will be put. The Act also limits the circumstances under which an investigative consumer report may be furnished.

The Act as presently written, however, is inadequate to deal with the problem of the abuse of medical information for three reasons. First, the FCRA section which requires disclosure of the agency's files, specifically exempts disclosure of medical information from these requirements. Second, the FCRA requires that an agency disclose the "nature and substance" of their files. If this requirement is narrowly interpreted, it would apparently allow for a mere summary of the file and not the full and complete disclosure that medical information might require. Third, courts have generally restricted the FCRA's applicability to investigations of insurance eligibility and have held that the FCRA does not apply to investigations of insurance claims.

A. The Medical Exception

Perhaps the most serious obstacle to applying the FCRA as written to cases of improper disclosure of medical information is the Act's clear omission of medical information from that information which needs to be disclosed by a reporting agency. Section 1681(a) of the FCRA dealing with disclosures to consumers provides:

(a) Every consumer reporting agency shall upon request and proper identification of any consumer, clearly and accurately disclose to the consumer:

(1) The nature and substance of all information (except medical information) in its files on the consumer at the time of the request. (emphasis added)

Medical information is defined in section 1681(a) as "information or records obtained, with the consent of the individual to whom it relates, from licensed physicians or medical practitioners, hospitals, clinics or other medical or medically related facilities." As presently written, therefore, the Act clearly exempts medical information from disclosure.

This explicit exception of disclosure of medical information

---

69. Id. § 1681b (permissible purposes of consumer reports).
70. Id. § 1681e (compliance procedures).
71. See Murdock, supra note 27.
under the FCRA has been held to bar local governments from enacting stricter legislation which would require disclosure of such information. In Retail Credit Co. v. Dade County, Florida,\textsuperscript{73} a local ordinance was held invalid insofar as it required disclosure of medical information. The court in Retail Credit pointed out that not all information concerning a consumer's health constitutes medical information. Information supplied by nonmedical personnel, such as a consumer's neighbors, does not constitute medical information subject to the protection from disclosure under the Fair Credit Reporting Act exemption for medical information.\textsuperscript{74} Under this rationale, that portion of the local ordinance which required the disclosure of health facts from nonmedical sources did not violate the Fair Credit Reporting Act.

The Fair Credit Reporting Act does not protect the privacy of medical information submitted by doctors and hospitals to insurance investigating agencies. Congress may have wished to prevent disclosure of such information because of a fear that "raw medical information should only be tendered with the counsel of a physician or other trained personnel."\textsuperscript{75}

Although the possibility of a patient's misreading or misinterpreting his own medical data is a valid consideration, this danger is outweighed by benefits the patient would receive. The time has come, therefore, to remove the medical information exception from the Fair Credit Reporting Act. This Note therefore proposes that section 1681(a)(1) of the Fair Credit Reporting Act be amended to read: The nature and substance of all information (including medical information) in its files on the consumer at the time of the request.

**B. THE INSURANCE CLAIM**

Section 1681a(d) provides that "the term 'consumer report' means any written, oral, or other communication . . . serving as a factor in establishing the Consumer's eligibility for (1) credit or insurance to be used primarily for personal, family or household purposes."\textsuperscript{76} This Note proposes that this section of the Fair Credit
Reporting Act should be amended to include "insurance claims" as section (3). The remainder of the Act would be renumbered accordingly. Such an amendment would eliminate the controversy surrounding the application of the FCRA to insurance claims. Conflicting cases have created some confusion as to whether or not the Fair Credit Reporting Act applies to insurance claims. The confusion is especially relevant to the problem of the abuse of medical information because insurance companies often obtain access to the medical files by means of waivers signed by insurance claimants.

The most recent case which involved the question of the applicability of the FCRA to insurance claims is Cochran v. Metropolitan Life Insurance Co.\textsuperscript{77} Cochran involved an insurance claimant, Marion Cochran, who had submitted a disability claim along with supporting medical documentation. Cochran was notified by his insurance company that he would be required to submit rigorous proof of his disability to qualify for continued policy benefits after receiving 24 months of benefits. Cochran failed to supply the proof, and the insurer ordered an investigative agency to prepare an insurance claim report. This report consisted of interviews with Cochran's neighbors. Cochran's complaint alleged that these interviews without prior notice to him violated the Fair Credit Reporting Act. After an analysis of the plain meaning of the statute, the precedents involved, and the legislative history, the court concluded that insurance claims were not protected by the FCRA. "Our reading of the prescriptive ambit of the Fair Credit Reporting Act includes only those information reports prepared to determine eligibility for insurance coverage or underwriting and not those compiled to evaluate claims for benefits."\textsuperscript{78}

The conclusion in Cochran is contrary to the rulings and trends of many other courts. For example, in Beresh v. Retail Credit Co.,\textsuperscript{79} the plaintiff sustained an injury waterskiing. In order to determine if the plaintiff should receive disability payments, the insurance company had investigative reports prepared to see if the plaintiff was really disabled. The court concluded that investigative reports of this nature were consumer reports under the FCRA because they were prepared in connection with a business transaction between the insurer and the insured.\textsuperscript{80}

\begin{flushleft}
\textsuperscript{77} 472 F. Supp. 827 (N.D. Ga. 1979). This medical investigation would not have been protected under the rationale of Retail Credit.
\textsuperscript{78} Id. at 832.
\textsuperscript{80} Id. at 262.
\end{flushleft}
The source of the confusion between these cases seems to derive from two sections of the FCRA which do not clearly define the term “consumer report.” Section 1681a(d) carefully defines consumer reports and concludes that a consumer report is used for “(3) other purposes authorized under section 1681b of this title.”

But § 1681b lists the permissible purposes of a consumer report and concludes that “a consumer reporting agency may furnish a consumer report ... [t]o a person which it has reason to believe ... otherwise has a legitimate business need ...” This definition of a “consumer report” is broad enough to encompass almost any report used in business transaction arising from a dispute over which section of the FCRA has priority. The Beresh court apparently gave greater weight to section 1681b(E) in rendering its interpretation. The Cochran court, however, decided that such an interpretation would render the restrictive language of section 1681a meaningless and thus refused to define the term “consumer report” as broadly as the court in Beresh. The Cochran court then concluded that reports for insurance claims must have been intentionally excluded and, therefore, were not subject to the FCRA.

To settle the confusion this Note proposes that section 1681(d) of the FCRA be amended to clearly include insurance claim investigations.

Even if the FCRA is not amended, a practitioner might argue the following. Section 1681a(d) provides in pertinent part “consumer report means ... any information ... which is used or expected to be used or collected in whole or in part for the purpose of ... establishing the consumer's eligibility for [1] credit or insurance” (emphasis added). It could therefore be argued that the information in data banks such as the MIB was collected with the expectation that it would be used to establish consumer eligibility for insurance, and that, therefore, reports which use that informa-


82. Permissible purposes of consumer reports are set forth in 15 U.S.C. § 1681b. A consumer reporting agency may furnish a consumer report under the following circumstances and no other:

(1) In response to the order of a court having jurisdiction to issue such an order.

(2) In accordance with the written instructions of the consumer to whom it relates.

(3) To a person which it has reason to believe—...

(E) otherwise has a legitimate business need for the information in connection with a business transaction involving the consumer.

(emphasis added).

tion fall under the FCRA. In one case, Sizemore v. Bambi Leasing, a personal credit report which had been collected and maintained for personal credit, insurance, and employment purposes was used in a subsequent report. The court's holding that this new report was not a consumer report is contrary to the majority trend. The Federal Trade Commission, the federal agency responsible for enforcing the Act, issued an opinion supporting the above argument. "[W]hen the information contained in the report was originally collected in whole or in part for consumer purposes, it is a consumer report and may not be subsequently furnished in a business credit or business insurance report." The FTC interpretation has also been followed in two recent cases which supported the collected argument.

In Rasor v. Retail Credit Co. a businesswoman's application for business-related insurance, was denied on the basis of data from an earlier application for health insurance. The court held that where the original "consumer report" was used for medical purposes, its "character" would not be changed merely by subsequent use as a business report.

In Rice v. Montgomery Ward, Montgomery Ward attempted to use credit reports as a discovery tool to aid in preparation of a case for litigation. The court concluded that the reports obtained by Montgomery Ward would probably constitute a consumer report "because the information in it was either collected or expected to be used for one of the purposes set out in § 1681a(d)."

Thus it appears that even without amending the FCRA, the Act could be applied to provide consumers with protection against abuse of medical information. Still, because of its wider scope, an amendment would still be the preferred method to prevent the misuse of medical information. The "collected" argument would only apply to files which had already been collected under certain expectations of use; it would probably not apply in cases where a credit agency is specifically requested to investigate an insurance claim.

C. THE DISCLOSURE REQUIREMENT

The most controversial element of the section of the FCRA requiring disclosure concerns the phrase "nature and substance."

85. Federal Trade Commission, Division of Consumer Credit and Special Programs, Bureau of Consumer Protections, Compliance with the Fair Credit Reporting Act 3 (2d ed. 1973).
86. 87 Wash. 2d 516, 554 P.2d 1041 (1967).
88. Id. at 671.
One commentator has taken the view that such a requirement is inadequate and is actually a weakness of the statute because it results in less than a complete disclosure. If this view is correct, further amendments would be required to prevent medical files that are disclosed to patients from becoming merely glossed-over summaries with little informational value to the patient. There are strong arguments, however, against this view.

Although there are no cases which speak directly to the question of what constitutes the disclosure of the nature and substance of a file, two major cases shed some light on how courts may choose to approach this question. In *Millstone v. O'Hanlon Reports, Inc.*, the plaintiff's application for insurance had been denied as a result of an agency report. The plaintiff then sought access to the credit agency file. The disclosure which the plaintiff received was a brief oral recitation from a single sheet of paper which noted, in part, allegations of "hippie" type behavior. The plaintiff could get virtually no further disclosure from the credit agency. The court held that such limited disclosure was insufficient to meet the standard of "nature and substance" required by the FCRA. The court, displeased with the disclosure by the O'Hanlon Reporting Corp., stated "To say that O'Hanlon was parsimonious in its disclosures in this case would be an exercise in understatement."

The second important case in this area is *Retail Credit Co. v. Dade County, Florida*. In this case Dade County adopted disclosure standards which were stricter than federal standards. Dade County required an actual copy of the consumer report to be delivered to a consumer upon request rather than a report of the "nature and substance" of the file. The court held that such a strict requirement was not "inconsistent" with the FCRA. "Disclosure of a copy of the report to the consumer appears to be consistent with the Congressional intent to protect consumers from inaccurate or incomplete information without upsetting the balance by unduly burdening the credit reporting agencies particularly since the copying costs are to be borne by the consumer himself."
The legislative history demonstrates that both the Senate and the House intended that the "nature and substance" provision would be loosely construed in order to allow complete disclosure of virtually the entire file. "The House offered the amendment to delete the words 'The nature and substance of' in section 609(1). The intent was to permit the consumer to examine all the information in his file except for sources of investigative information, while not giving the consumer the right to physically handle his file. The Senate conferees did not agree to this amendment contending that the existing language already accomplished this result. The conferees of both Houses intend that this important provision be so interpreted."98

The FTC explained that Congress used the phrase "nature and substance" because it recognized that there would be cases where the information would be encoded, and thus meaningless to the consumer if delivered verbatim.99 This interpretation harmonizes well with section 1681h(c) of the FCRA which requires that the "consumer reporting agency shall provide trained personnel to explain to the consumer any information" disclosed to him.100 This demonstrates that substantial disclosure must be made by the consumer reporting agency upon request by the consumer.

VIII. POTENTIAL APPLICATION

If the Federal Credit Reporting Act were amended as proposed, how would the new Act work? The best starting place would be section 1681a, the definition section. Section 1681a(d) defines a consumer report as any communication of information, produced by a consumer reporting agency, which deals with the consumer's credit capacity, character, or personal characteristics to be used as a factor in establishing the consumer's eligibility for credit, insurance or employment.101 A consumer reporting agency means any person102 who, for money or on a cooperative nonprofit basis, regularly engages in the practice of assembling or evaluating information about consumers for the purpose of providing consumer reports to third parties, and who uses interstate commerce to prepare or furnish its consumers report.103 Large data companies like the MIB clearly fall

---

100. 15 U.S.C. § 1681h(c).
102. 15 U.S.C. § 1681a(b) defines person as "any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity."
103. "The term consumer reporting agency means any person which, for monetary
within the category of consumer reporting agencies. The MIB, which is located just outside of New York collects information on millions of Americans across the nation and stores this information for future use by most of the insurance companies in the United States. Under the proposed amendments, it would not matter whether the information was actually used to determine insurance eligibility or to adjust insurance claims because both would come within the scope of FCRA's definition of consumer reports.

Having found that the statute with the proposed amendments would apply to medical data bureaus which collect their data through insurance investigations, this Note will now examine the ramifications the amended statute will have for the general public. Under section 1681d(a) of the FCRA, a person who wishes to procure an investigation on an individual consumer, must generally notify the consumer that an investigative consumer report has been requested and inform the consumer of his right to request disclosure from the person procuring the report as to the nature and scope of the investigation requested. A person may cause a consumer report to be prepared without disclosing the fact of preparation, however, if "[t]he report is to be used for employment purposes for which the consumer has not specifically applied." In this case, the consumer might not discover that a report on him has been used unless the results are adverse to his interests. If the results are adverse to the consumer's interests, the person who has used the consumer report in reaching an adverse decision must advise the consumer of the basis for their decision and supply the name and address of the consumer reporting agency that generated the report. This requirement of disclosure in cases of adverse decisions also applies to situations of denied credit and insurance.

There are two points in time when a patient might discover that medical files are being created on him: first, when the person procuring the file requests the investigation (not including employment purposes for which the consumer has not applied) and second, whenever a decision is made which is adverse to the patient's interests. Let us momentarily assume that the patient discovers through fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f).

104. Id. § 1681d(a).
105. Id. § 1681d(b).
106. Id. § 1681d(a) (2).
107. Id. § 1681m(a).
some notification process that a consumer file has in fact been generated and that this file includes personal medical information about him. The patient's option would be to seek disclosure of his files to discover what information in the file led to an adverse decision. The patient's best approach would be to seek disclosure from the consumer reporting agency since the Act requires greater disclosure of the consumer report by the reporting agency than by the deciding party.108

Section 1681g of the FCRA would require the consumer reporting agency to disclose the "nature and substance of all information in its files."109 (Remember that the old prohibition against medical disclosure has supposedly been removed). At this time the credit reporting agency must also disclose the sources of the information110 and the recipients of any consumer report on the patient which was furnished for employment purposes within the last two years and any report issued within the last six months.111 If applied to medical files, the Act would allow consumers to force data bureaus to give them access to the same information to which others, such as insurance companies or employers, have access.

Any consumer reporting agency which violated provisions of the FCRA would risk civil liability. If a consumer reporting agency, for example, failed to properly disclose the contents of its files upon consumer request, and the court found such nondisclosure to be negligent, then the agency would be liable for actual damages and attorney's fees.112 If the court found, however, that this non-compliance and non-disclosure was willful, then in addition to damages and attorney's fees, the consumer could collect punitive damages from the agency.113 Also, those who obtain information from a reporting agency under false pretenses would be subject to a $5,000.00 fine and/or one year imprisonment.114

In addition to private enforcement of the FCRA as provided for under sections 1681n and 1681o, the FCRA provides for enforcement by the FTC. Although the FTC has the power to enforce the requirements of FCRA, the FTC has rarely exercised this power. Most

108. Reporting agencies must disclose to the consumer the nature and substance of their reports. 15 U.S.C. § 1681g(a)(1). The decision-making party, however, that originally requested the report be made need only disclose the nature and scope of the report. 15 U.S.C. § 1681d(b).
109. See Feldman, supra note 43.
111. Id. § 1681g(a)(3).
112. Id. § 1681o.
113. Id. § 1681n.
114. Id. § 1681q.
litigation involving the misuse of medical information has been brought by private individuals.

VIII. CONCLUSION

This Note has attempted to demonstrate how amending the Fair Credit Reporting Act might create a tool to prevent the misuse of medical information. It must be realized that the FCRA cannot be applied to halt the disclosure of medical information any more than it can halt the disclosure of credit information. That is not the function of this Act. The Act recognizes the conflicting interests between the growing needs of society for information and the resultant decrease in personal privacy. The Act requires that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, and insurance in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information. Hopefully, as doctors and businessmen realize that the consumer will have access to his own medical file, disclosures will be made in a more careful and responsible manner. In any event, the FCRA can be used to protect the consumer's privacy interests. Although it is not a complete solution, by giving consumers access to their own files, the FCRA is a step in the right direction.

John Morihara