UIC John Marshall Journal of Information Technology & Privacy Law

Volume 10
Issue 4 *Computer/Law Journal - Winter 1990*

Article 6

Winter 1990

A Normative Analysis of Disclsoure, Privacy, and Computers: The State Cases, 10 Computer L.J. 603 (1990)

Eve H. Karasik

A NORMATIVE ANALYSIS OF DISCLOSURE, PRIVACY, AND COMPUTERS: THE STATE CASES

I. INTRODUCTION

Privacy. Disclosure. Computers. These words are red flags that symbolize too much and are waved by many to create the fear of a totalitarian Orwellian society. Portraits of monstrous computer databases open to all that contain society's most personal thoughts, goals, and activities swarm through our minds. Yet, it is necessary to break these assertions apart. What types of information does society expect and desire to be confidential? In the large, complex bureaucratic society in which we work, marry, seek medical attention, and go to schools, automated data collection is mandatory. In addition, granting access to information may serve societal purposes, such as fighting crime and preventing drug abuse. Furthermore, does the computer really exacerbate an invasion of the personal realm by facilitating access and disclosure? Or can the computer be viewed as a mechanism which creates a compromise between society's privacy values and disclosure needs? The computer can make data anonymous by replacing personal identifiers with neutral codes while making the data available to those with warranted disclosure requests.

This Note attempts to dissect these "buzz words" and to ascertain what constitutes our society's values in privacy and disclosure. This Note considers a survey of state court decisions which involve various types of personal information stored in computerized databases. It is significant that the computer dimension exists both in the background and in the foreground. It exists in the background since all of the cases studied involve automated data systems. Yet, it is in the foreground too, since computers may provide the way to satisfactorily permit the coexistence of confidentiality interests and disclosure needs.

Before the analysis begins, it is important to describe the parameters of this paper. This Note assumes that the collecting actor initially gathered the data in a legitimate manner. It does not address the hard questions about initial collection. For example, this Note does not focus on the First or Fourth Constitutional Amendments' protections and prohibitions against gathering information about other people. These important issues require independent consideration beyond the scope of

this paper. Instead, this Note considers the dissemination problems that arise after individuals or entities properly collect personal information about other people. This Note examines when it is normatively acceptable to disclose legitimately obtained personal information stored in an automated database to strangers without the subject party's consent.

This Note is divided into the following sections. The first section will examine our values in disclosure. The second section will examine our interests in privacy. The third section will look at how the computer dimension affects the balancing of these values. Finally, the fourth section will suggest an approach to reduce the clash between privacy concerns and disclosure requirements in an automated society.

II. DISCLOSURE

Disclosure is one of the many "buzz" words which permeate this topic. The term must be dissected to determine what the courts and society really mean when they use the word disclosure. Once this amorphous term is defined sufficiently, the circumstances or uses which normatively merit disclosure must be considered. Therefore, this section of the Note will focus on two inquiries. The first will examine the nature of disclosure. The second will evaluate the circumstances in which courts have considered disclosure appropriate.

A. THE COLLECTION/DISCLOSURE CONTINUUM

The question of what courts and society mean when they use the word "disclosure" is not easy to answer. However, it is possible to view disclosure on a continuum. At one end of this continuum lies "collection," somewhere in the middle rests "meta-collection," and at the other end is "disclosure." In between these major data points, of course, lie gradations. In the following paragraphs, these major data points will be defined and examined by applying them to pertinent state cases.

It is important to note that the cases may not fit perfectly into these nicely created categories. Some cases contain aspects of more than one category, indicating that there is no true continuum with fine, discrete points. A case used to illustrate one form of disclosure may be used again to demonstrate another disclosure type. This overlap may be an essential element of the disclosure continuum. Maybe the continuum is described more accurately as a core with concentric circles. Collection is the core, meta-collections are circles surrounding the core, and disclosure is the outer circle. Disclosure is inclusive; it contains both collection and meta-collection as necessary parts of its whole. However, the fact that the cases may overlap within the continuum does not eradicate the continuum's value. The continuum illustrates the broad range

of disclosure activity and helps to isolate the particular disclosure activities which society should sanction.

1. *Collection*

Collection activity lies at one end of the continuum. Collection occurs when individuals or government entities obtain, store, and use data for a specific, agreed upon, purpose. In its most benign form, parties voluntarily provide the desired data about themselves to legitimate collectors. These parties approve of the collection project and consent to the storage of information about themselves in databases. Although there are no cases that discuss this type of activity, this is not surprising because the parties consented to the collection and use of the information.

Yet, there are collection situations which are somewhat more controversial. These occur when individuals or government entities collect data for a particular purpose *without* a person's permission or approval. This will often occur in the law enforcement context. *A.C.L.U. Foundation v. Deukmejian*[1] is one example of such a case. In *A.C.L.U.*, the California Attorney General's Office collected information about persons suspected of organized crime activities and stored it in a computerized database. The Attorney General's Office stated that it needed the database to control organized crime in the state. The A.C.L.U. was concerned that police intelligence officers used the information to harass suspects without cause. In this case, the Attorney General's Office's creation of a data pool without the subject's consent exemplifies controversial collection activity. Although the government collected the data for passive storage, people may not want to be subjects of the data pool.

2. *Meta-Collection*

Meta-collection activity occupies a space somewhere in the middle of the continuum. Meta-collection describes the process in which individuals or government entities collect and store information for a particular purpose, but they use or release the data for an expanded version of the same purpose or to a greater number of people than expected. Here, the problem is that the collectors use the personal information for a broader purpose within the confines of the same general scope. A few illustrative cases follow.

Peninsula Counseling Center v. Rahm[2] is a good example of the meta-collection phenomenon. In *Peninsula*, the state government required a local mental health clinic to create and maintain a patient database containing the patients' medical histories and other personal

1. 32 Cal. 3d 440, 651 P.2d 822, 186 Cal. Rptr. 235 (1982).
2. 105 Wash. 2d 929, 719 P.2d 926 (1986).

information. The state required that the local clinic store and collect this information for accounting purposes. While the Center ostensibly collected the data for local and state financial purposes, the Center shared the information with federal agencies for national financial purposes. The federal government subsidized mental health clinics, including the Peninsula Counseling Center, and often requested such information before they would grant needed funds. In both instances, the data was to be used to satisfy accounting requirements, but the Center expanded the exposure scope to satisfy federal requirements. Essentially, the state clinics and federal authorities would use the data for the same general purpose, but the Center would share the data with more people than it originally expected when it collected the information.

A second example is found in *Koppes v. City of Waterloo*[3] and *Davidson v. Dill*.[4] In these cases, the authorities arrested people for trespass and loitering violations, respectively, and placed their names in an arrest database for processing. After the courts acquitted the parties in both cases, the authorities wanted to retain their names in the databases to facilitate future law enforcement. Here, the police collected the data to process the specific arrests and wanted to retain the information for future use if the parties committed another offense. The authorities collected the data for one purpose and wished to use it in the future for a different, yet closely related, purpose.

While there virtually are no cases which addressed the collection mode, the meta-collection form attracted more cases because the meta-collection process is more controversial. In meta-collection, individuals or government entities obtain data for a specified purpose and then stretch this purpose. They either expand the circle of people who will be exposed to the information or use the information for a slightly different, but connected, purpose. In both instances, data about people leaks out of its controlled area. Although courts seem reluctant to forbid this leakage, possibly because the expanded scope or use is quite similar to the original scope or use, the leaked information may concern the subjects of the information and, often, the collectors. Meta-collection activity likely bothers people because the leaked information further diminishes the control the subjects relinquished when they originally released the information.

3. *Disclosure*

Disclosure lies at the opposite end of the continuum from collection. Disclosure occurs when individuals or government entities collect

3. 445 N.W.2d 774 (Iowa 1989).
4. 180 Colo. 123, 503 P.2d 157 (1972).

data for one purpose and use or release the information for a purpose distinct from the original goal. A plethora of the state cases cluster around this point on the continuum. Issues of both consent and control, slowly emerging in the meta-collection cases, are present at the disclosure stage. In disclosure cases, people consent to the release of information about themselves for a particular purpose or for use by certain people. This consent, granting a collector restricted use of the information, gives people a sense of control over information about themselves. People have a proprietary feeling about personal information and it is likely that subjects will only feel good about sharing personal information when collectors ask their consent and respect their restrictions on use. However, in disclosure cases, collectors abuse this consent and wrest away this control by using or releasing data beyond the agreed upon scope.

There seems to be two types of disclosure cases. The first type is where a private party or group maintains a database and a public entity wants to access the data. The second disclosure form is where public entities maintain automated record systems and private parties wish to obtain the data. The two cases which follow illustrate the former type of disclosure.

In *Doe v. Axelrod*,[5] the Commissioner of the New York State Department of Health approved a regulation that required doctors to write all prescriptions for benzodiazepines[6] in triplicate so that pharmacists could send a copy of each prescription to the social services department. The social services department would store the prescriptions in a central database. The database records would contain the name and address of the patient, the name, address and phone number of the pharmacist, the doctor's name, a substance code number, directions for dosage, and the pharmacy file number. The social services department created the database to monitor and prevent prescription drug abuse.

This case is an example of disclosure. The doctors and pharmacists collected medical data from patients to treat their individual medical problems. The government agency wants the data to aid their campaign against prescription drug abuse. In so doing, the government intends to monitor closely both the doctors and pharmacists, who prescribe the drugs, and the patients, who consume the medicines. When patients obtain prescription refills, the triplicate system will report them to the authorities. The medical community obtained information for a particular purpose and the government forces the release of the data to be used for distinct goals. When a public entity desires to access data privately

5. 144 Misc. 2d 777, 545 N.Y.S.2d 490 (1989).

6. Benzodiazepines are tranquilizers, including Valium and Xanax.

collected, neither the collector's nor the subject's protests likely will prevent the disclosure.

Another example of private to public disclosure is found in *In Re Rozas Gibson Pharmacy of Eunice, Inc.*[7] In this case a pharmacy collected and maintained a database to monitor its Medicaid prescription patients. The records included the patient's name, address, phone number, physician, and prescribed medicine. The government's Medicaid Fraud Unit wanted access to the data to conduct an investigation, since it suspected the pharmacy of Medicaid fraud activities. This case also presents a disclosure problem. The pharmacy collected the data for business and treatment purposes. The Medicaid Fraud Unit wanted access to the data to conduct an investigation. The two purposes are distinct. The pharmacy, a private collector, obtained personal information for a specific purpose and the Medicaid Fraud Unit, a public entity, demands disclosure for a different use.[8]

The second type of disclosure case is the public to private scenario. In these cases, the public entity, usually a government agency or department, collected data on its citizens for a certain purpose, and non-public individuals or groups wish to access the information for a different purpose. There are many of these disclosure cases and a sampling follow.

The Catholic Bulletin Publishing Company, in *Minnesota Medical Assoc. v. Minnesota*,[9] requested various information from a government database that stored publicly funded abortion records.[10] The Minnesota Department of Public Welfare created and used the database predominantly for accounting purposes. The Publishing Company wanted access to the names of all doctors who performed these abortions, the names of all hospitals and clinics where the physicians performed the operations, and the amount of state funding dispersed to these physicians and providers. While the Publishing Company did not state how they planned to use this information, it is unlikely that they intended to use the data for accounting purposes. It is more probable that they would use the information to further their anti-abortion campaign. Therefore, a public entity, the Minnesota Department of Public Welfare, collected the data for one purpose and the private requestor, the

7. 382 So. 2d 929 (La. 1980).

8. While the disclosure in this example does not appear to be as offensive as in the Doe v. Axelrod scenario, it is still an example of disclosure. The Note's next section will consider why some disclosures seem more offensive then others.

9. 274 N.W.2d 84 (Minn. 1978).

10. Two other state cases discuss the same factual scenario and both courts resolve their suits as the Minnesota court did. These cases are State *ex rel.* Stephan v. Harder, 230 Kan. 573, 641 P.2d 366 (1982) and Family Life League v. Dep't of Public Aid, 112 Ill. 2d 449, 493 N.E.2d 1054 (1986).

Publishing Company, likely desired the data for a much different purpose.

In *Doe v. Sears*,[11] the Managing Editor of the *Atlanta Constitution* requested access to the Atlanta Housing Authority's public housing database. The Housing Authority created the database to store information about the city's public housing system. Information in the database included the names of tenants, the number of people in the residence, and rent payment data. The Managing Editor suspected that the Housing Authority was corrupt. He wanted to investigate the Housing Authority's practices and felt that the database records would be helpful. Again, a public entity, the Atlanta Housing Authority, created a database to facilitate its operations and an individual, the Managing Editor, wished to use the data for another purpose.

A third example of the public to private disclosure phenomenon is found in *Industrial Foundation of the South v. Texas Industrial Accident Board*.[12] In *Industrial Foundation*, the Texas Accident Board maintained a workers' compensation claims database that contained various data on individual claimants, including the claimant's name, injury, attorney, social security number, and employer. The Board created the database to make their claims processing system more efficient. The Industrial Foundation of the South, a non-profit corporation formed by 282 southern companies, requested access to the employment records. While the Foundation did not state why it wanted the information or how it intended to use the data, it is unlikely that the Foundation would use the information for claims processing purposes. More likely, the Foundation intended to use the data to discriminate against applicants who had filed workers' compensation claims. The Foundation would discover the identity of claimants, divulge this information to the employers, and the employers could refuse to hire anyone with a workers' compensation claim. Again, a government entity collected data for one purpose and a private entity wants to access the materials for a different use.

A final example of this common disclosure problem is found in *Kestenbaum v. Michigan State University*.[13] In *Kestenbaum*, the University had a student directory in a database. The database included the students' names, addresses and phone numbers. The University published the directory to help its freshman acclimate to the new university environment. A non-student, running for a local political office, requested a computer tape of the data to obtain the names of potential

11. 245 Ga. 83, 263 S.E.2d 119 (1980), *cert. dismissed*, 446 U.S. 979 (1980).

12. 540 S.W.2d 668 (Tex. 1976), *cert. denied*, 430 U.S. 931 (1977).

13. 414 Mich. 510, 327 N.W.2d 783 (1982), *aff'g*, 97 Mich. App. 5, 294 N.W.2d 228 (1980).

voters. Again, a public entity created an information pool, and a private individual desired to access this data. However, the parties had distinct purposes for the information.

From the above discussion a description of disclosure emerges. Disclosure occurs when one individual or entity, either private or public, collects, stores, and uses information in a database for one purpose and a second individual or entity desires to access the data for a different use. Since many courts hold in favor of disclosing information to requestors, the next step is to evaluate the circumstances and uses of disclosure.[14]

B. THE DISCLOSURE WEIGHT

Why do courts sanction the release of information about individuals collected for one purpose but to be used for a distinct goal? Why do courts permit this disclosure in certain circumstances for specific uses and prohibit it in other situations? The answers to these questions lie in our society's norms: the shared values held by our communities. When a requestor wishes to access information for a use compatible with our norms, the courts will permit the disclosure. In other instances, when the requestor's desired new use will mar the value of the original use, the courts will prohibit disclosure. In the hardest cases, society values conflicting purposes, and the courts carefully must evaluate both uses to discover which use carries the most normative weight.

This section attempts to analyze various cases where the courts have considered the disclosure value. It will try to discover the normative underpinnings of these decisions and to determine whether our society should foster these norms. Four disclosure trends emerge from the data. These patterns show that courts permit disclosure for welfare state maintenance, law enforcement, informing the general public, and personal gain. While it must be recognized that these categories are artificial and somewhat generalized, they can provide a loose hierarchy of disclosure uses which can help to illuminate our society's values in disclosure.

1. *Welfare State Maintenance*

The United States is a welfare state. Although scaled back in comparison to past years, the federal and state governments have spent a great deal of time and money on programs designed to improve society's domestic welfare. In order to effectuate these goals and policies, the

14. A natural inquiry which springs from this analysis is to discover why disclosure is so objectionable. Essentially, the reason why there are so many cases in this area is that society values *both* disclosure and non-disclosure, and thus, a controversy arises. The non-disclosure value is discussed in a later section of this Note.

government needs information. As a result of the size of the welfare state's infra-structure and the number of people who consume these benefits, state and federal governments usually create, maintain, and store this information in huge computer databases. The government entities intend to use the data to benefit people in society by satisfying various public needs, such as providing health care, food and shelter. Despite the benign intent of these databases, there is potential for government to misuse the information and harm people. Public need must be balanced against the potential for misuse to determine the disclosure value.

One example of this welfare state value is found in the Washington state case *Peninsula Counseling Center v. Rahm*[15] discussed above. Briefly, this case involved the creation and maintenance of a state-wide combined storage and tracking database to monitor the costs of publicly funded mental health care agencies. The database contained patients' names, dates of birth, diagnoses, and referral clinics. While the agencies originally obtained the data for accounting and treatment purposes within each clinic, this data was to be disclosed to all mental health agencies in the state, as well as to federal authorities, which contributed funding to the clinics. The court concluded that the data could be disclosed.

The *Peninsula* case provides an example of the disclosure value. The government should provide people, who are mentally ill and cannot afford private medical attention, with an opportunity to receive treatment for their illnesses. While Washington State may want to offer mental health services to a part of its population, it has limited resources. The database tracking system can help the state monitor its use of funds and determine the most efficient way to use its resources. Furthermore, the federal government conditioned its aid to Washington on the availability of such data to ensure that the state agencies properly used the federal funds. While confidentiality concerns are present, there also are strong disclosure interests. Disclosure will allow the state to continue providing much needed care to a sector of its population.

In New York's *Doe v. Axelrod*,[16] a second state case which examines a welfare state value, the court wrestled with the problem of prescription drug abuse. This case involved a regulation drafted by the Commissioner of the New York State Department of Health which required pharmacists to send copies of benzodiazepine prescriptions, with patient identity and diagnosis information, to the appointed state representative for entry into a central database. The Commissioner stated

15. 105 Wash. 2d 929, 719 P.2d 926 (1986).

16. 144 Misc. 2d 777, 545 N.Y.S.2d 490 (1989).

that the database was necessary to combat prescription drug abuse. He claimed that doctors often either over-prescribed or privately sold these drugs, and that young people recreationally used these drugs.

The court approved New York's prescription drug accountability system. Here, as with *Peninsula*'s[17] mental health data, there seems to be a strong value in permitting disclosure. Drug abuse is one of society's major maladies and it takes all forms. People are addicted to illegal drugs, over-the-counter medicines, and prescribed medications, and disclosure may work to prevent prescribed drug addiction. Remember, the goal of this section is to determine the weightiness of disclosure values and not to evaluate non-disclosure values. Therefore, in *Axelrod*[18] competing non-disclosure values may outweigh the drug prevention value, deeming the court's decision normatively incorrect.

A third set of welfare state maintenance cases concerned with child abuse prevention is represented by the Iowa and New Hampshire cases *Roth v. Reagen*[19] and *Petition of Bagley*,[20] respectively. In both of these cases, the authorities accused the parties of child abuse. They collected and stored data about the parties in a database as part of the investigation. While an administrative officer acquitted the parties, the authorities wished to retain the parties in a child abuse offender database for an extended period. They wanted to keep this information as an extra safeguard to protect the children from the possibility that the administrative officer had mistakenly acquitted the parties. The court permitted the personal data to remain in the database.

While there clearly are confidentiality problems with retaining acquitted parties' names in child abuse registries, maintaining and, possibly, disclosing this data has merit. Children are victimized and vulnerable. They often do not know they can talk to others about the abuse, or they feel they deserve the harm. Methods which can protect children from such harm are valuable. Information systems designed to track potential offenders may help prevent or mitigate this type of harm. Therefore, society may force parties cleared of child abuse accusations to suffer some stigma in order to achieve the societal goal of child abuse prevention.

2. *Law Enforcement*

In addition to welfare state goals, courts also sanction the state use of data to satisfy law enforcement purposes. Law enforcement officials may need access to records and the ability to maintain databases on in-

17. 105 Wash. 2d 929, 719 P.2d 926 (1986).
18. 144 Misc. 2d 777, 545 N.Y.S.2d 490 (1989).
19. 422 N.W.2d 464 (Iowa 1988).
20. 128 N.H. 275, 513 A.2d 331 (1986).

dividuals to ensure public safety. Although authorities may use this information to protect the public, there is a great potential for selective discretion by authorities. Public safety should not be ensured at the price of due process values. In the law enforcement situation, disclosure may be valuable, but it must be monitored closely because of the great potential for abuse. The two state cases which follow illustrate the law enforcement value.

In *In re Rozas Gibson Pharmacy of Eunice, Inc.*,[21] a Louisiana case discussed above, the Medicaid Fraud Control Unit of the Louisiana Attorney General's Office conducted a fraud investigation and subpoenaed the accused pharmacist's database. The pharmacist allegedly charged Medicaid patients above the determined price and retained the difference. The investigators wanted the pharmacist's business records database. In this database the pharmacist recorded various data, including the prescription type and number, the customer's name and address, the physician, and the price. The investigators claimed that the evidence was indispensable to their case and that the pharmacist, who voluntarily became a Medicaid provider, should have expected these regulatory investigations.

The court permitted disclosure of the data to the Medicaid Fraud Control Unit. In this case, disclosure serves the important state goal of assuring that its Medicaid program is administered effectively. The Medicaid program is designed to help people who cannot afford to pay for the medical attention they need. These people include the more vulnerable members of society, such as the poor, the disabled, the elderly, and the very young. The accused had abused his Medicaid provider status and weakened the medical aid program. In this example, there seems to be a good reason to permit disclosure of data.

Another set of cases, also discussed briefly above, illustrate the danger of giving too much weight to the law enforcement disclosure value. These are the Iowa case *Koppes v. City of Waterloo*[22] and the Colorado case *Davidson v. Dill*.[23] In these cases the local authorities arrested the plaintiffs for trespass and loitering violations, respectively, and the courts acquitted them. The police departments wanted to retain the plaintiffs' names in a database of arrestees to facilitate future law enforcement. The plaintiffs' wanted their names removed from the database since the courts had acquitted them.

In both cases, the courts concluded that the law enforcement agencies could retain the acquitted parties' arrest records. Despite the courts' findings, the disclosure value is minimal in these cases. First, a

21. 382 So. 2d 929 (La. 1980).

22. 445 N.W.2d 774 (Iowa 1989).

23. 180 Colo. 123, 503 P.2d 157 (1972).

judicial body acquitted these people of their accused crimes, and there seems to be no viable reason why they should be stigmatized by a criminal arrest record. Second, in contrast to the child abuse cases discussed above, the crimes in these cases do not seem to be as serious. While trespass and loitering are criminal offenses, they are not heinous crimes. There seems to be less value in a database maintained to protect the general public from acquitted parties who may commit similar future offenses. Essentially, some law enforcement situations will trigger a higher disclosure value than others.

3. *Informing the General Public*

Another interest in disclosure which parties, the courts, and the legislatures espouse is the public's right to know the activities of their government. This idea is the basic premise of the federal Freedom of Information Act ("F.O.I.A.")[24] and its offspring statutes in various states.[25] Generally, under these acts, the public is given the right to request any records or information maintained by the government, as long as the request does not result clearly in an unwarranted invasion of privacy. The existence of these federal and state legislative acts indicates that society values disclosure for a general purpose of informing the populace. Essentially, this disclosure value is rooted in the American democratic tradition which grants citizens the right and responsibility to check government action. The cases exhibit much judicial deference to the legislatures' F.O.I.A.s which permit disclosure in support of the public's "right to know."

Several cases from different states discuss the valued public's right to know. The state courts in Minnesota,[26] Illinois[27] and Kansas[28] considered whether records of publicly funded abortions may be disclosed to the public. In all three cases, the courts decided that the computerized records could be disclosed to private interest groups after the government entity removed the patient identity information. The facts of the Kansas case will be summarized below as representative of these three cases.

For example, in *State ex rel. Stephan v. Harder*,[29] the Right to Life of Kansas, Inc. wanted to access publicly funded abortion records. The Kansas Department of Social Welfare maintained these records in a

24. Freedom of Information Act, 5. U.S.C. § 552 (1967).

25. *See, e.g.*, Michigan's Freedom of Information Act, Mich. Comp. Laws § 15231 *et. seq.* and Mich. Stat. Ann. § 4.1801(1), *et. seq.* and New York's Pub. Officers Freedom of Information Law, Article 6 § 84 *et. seq.*

26. Minn. Medical Assoc. v. Minn., 274 N.W.2d 84 (Minn. 1978).

27. Family Life Leaque v. Dep't of Public Aid, 112 Ill. 2d 449, 493 N.E.2d 1054 (1986).

28. State *ex rel.* Stephen v. Harder, 230 Kan. 573, 641 P.2d 366 (1982).

29. *Id.*

database that included the patients' names and addresses, the names and addresses of the doctors and providers who performed the abortions, and the amount paid for the abortions. The Right to Life of Kansas, Inc., stated only that they had a right to know how the government spends their tax dollars. They requested, pursuant to Kansas' public records act, the names of the doctors and providers and the monetary compensation received from performing the abortion procedures.

The Kansas court permitted disclosure of the requested data and determined that the public had the right to know how the government uses tax revenues. Unlike the cases previously noted, this is truly a hard case. The legislatures have concluded that our society values public access to records of its government's activities. In this case, the requesting party wants to determine how much public money the government spends on a certain medical procedure funded with tax dollars. The request seems to fall within the valued purview of the public records acts. Yet, it is still troubling. While the information requested appears innocuous, the abortion context presents a possible harmful dimension. For example, abortion services may diminish as a result of political pressure. In addition, people may be deterred from obtaining abortions because they fear harassment. Furthermore, women faced with this emotionally difficult decision should not have to suffer from additional external pressures. The legislatures designed F.O.I.A.s to ensure that a corrupt government could not hide its activities from the populace. It is questionable whether the legislatures intended F.O.I.A.s to be applied in contexts, such as abortion, where private groups morally oppose government acts and plan to use the official records to further their cause at the expense of harming third parties.

Doe v. Sears,[30] a Georgia case discussed briefly above, demonstrates a more valid use of the valued public's right to know. In this case, the Managing Editor of the *Atlanta Constitution* requested the names, addresses, and income sources of public housing tenants from the Atlanta Housing Authority's automated database. The editor stated that he was investigating a charge of political corruption in the Housing Authority and that he needed the data to confirm his investigation. He suggested that tenants, delinquent in their rent, had special ties to the Housing Authority and to local politicians. The editor felt that the people of Atlanta had a right to know that their government was involved in such practices.

The *Sears* court permitted the disclosure of the government information, supporting a generalized disclosure value in the public's right to know. In this case, the public's right to know is consonant with the pur-

30. 245 Ga. 83, 263 S.E.2d 119 (1980), *cert. denied* and *appeal dismissed*, 446 U.S. 979 (1980).

poses of the public records acts. Legislatures designed the open records systems to combat government corruption. The F.O.I.A.s decreased the opportunities for government officials to hide behind official records. In *Sears*, the Housing Authority may have engaged in such suspect activities. However, in the abortion context where the requesting party seeks disclosure not to investigate suspicious or corrupt government behavior but because the party disagrees morally with how government funds are spent, the disclosure request seems less valid.

A final group of "right to know" cases premise their access requests on the public's general right to know, but voice no reason or intended use for the data. These cases, often based on a state's public records act, claim that the statutes do not condition disclosure upon a person's motivations, and, therefore, requesting parties never need to establish why they want information. While legislatures likely decided that requestors could be silent about their motivation for fear that government entities could arbitrarily refuse disclosure based on these goals, this alternative seems equally dangerous. The arbitrary factor remains, but now rests in the requestor instead of the requestee. It is difficult to determine whether disclosure normatively will be appropriate if the requesting party is not required to divulge the intended use of the data. Possibly legislatures should create some inclusive list of "use" criteria for data disclosure. Two cases which follow provide examples of the troubling "right to know" cases.

In *Industrial Foundation of the South v. Texas Industrial Accident Board*[31] mentioned above, Industrial Foundation of the South, a nonprofit data collecting corporation composed of 282 companies that employed southern workers, requested access to workers' compensation information stored in the Texas Accident Board's computers. These records included the claimant's name, injury, attorney, social security number and employer. The Foundation did not state why it wanted the data and the court explicitly held that the Texas Public Records Act did not require a requestor to give reasons for a data request. In a situation such as the *Industrial Foundation* scenario where the opportunity of employment discrimination is foreseeable, it seems that the legislature should require that requestors provide some reasons for their requests.

In *Family Life League v. Department of Public Aid*,[32] an Illinois publicly funded abortion case, the Family Life League requested the names and addresses of doctors and providers who perform abortions, the amount of compensation they received, and the number of abortions performed. Although the League did not offer reasons why it wanted the records, the court stated that the requesting parties need not ex-

31. 540 S.W.2d 668 (Tex. 1976), *cert. denied*, 430 U.S. 931 (1977).

32. 112 Ill. 2d 449, 493 N.E.2d 1054 (1986).

plain their requests, since the public records law legitimates most requests on a generalized right to know. Again, it is hard to discern the disclosure value when requestors do not provide reasons for their data request. A data request based on a desire to determine if unqualified doctors are performing abortions and hurting patients may be given a different weight than a desire to harass doctors or their patients. If a party declines to give a reason for a request, then the government body should have the power to deny it. While this authority does provide an opportunity for government entities or courts to exercise selective discretion when they analyze the reasons justifying disclosure, courts and government bodies frequently make such value-based decisions.

4. *Private Use or Personal Gain*

A fourth area where state courts must determine the value of disclosure is when parties request to access data for personal use or gain as opposed to a socially beneficial purpose. While the socially motivated purposes for disclosure normatively appear to merit a greater disclosure value than disclosure for personal use, courts often do not preclude individually motivated disclosure. Courts may permit disclosure for personal benefit because they wish to defer to F.O.I.A. "right to know" precepts or because the information requested has little harm potential. A few cases from different states illustrate these ideas.

In *Kestenbaum v. Michigan State University*,[33] a Michigan case briefly discussed above, a non-student candidate in a local election requested computerized data from Michigan State University's Freedom of Information Officer. The candidate wanted a computer tape of the Michigan State University Student Directory. The directory contained the names, addresses and phone numbers of all undergraduate students at the University. The candidate wanted the data for political mailings he wished to send before the upcoming election. The court precluded the disclosure.

This case is interesting because it is one of the few cases where a court refused to permit disclosure of individuals' names and addresses contained in public records. Generally, courts permit this type of disclosure. The courts, likely, are somewhat desensitized to disclosing name and address data, since it is released commonly. Also, society may benefit tangentially from disclosure for use in a political campaign, since the mailings will help to educate and involve people in the political process. However, the requestor obtains a greater benefit from the disclosure because the mailings directly will aid his campaign efforts. While our democratic system values stimulating involvement in the electoral sys-

33. 414 Mich. 510, 327 N.W.2d 783 (1982), *aff'g*, 97 Mich. App. 5, 194 N.W.2d 228 (1980).

tem and fighting voter apathy, encouraging these values through the disclosure of personal information without the subject's consent, at least, should be questioned.

The following New York case involves the disclosure of assessment data for personal gain. In the *Matter of Szikszay v. Buelow*,[34] an individual who owned Peter's Quality Tree Service requested access to county assessment rolls stored on computer tape at the Cattaraugus County Real Property Tax Service. These records contained the names and addresses of land owners. The requester needed the data for business because he wanted to locate tracts of land that might be suitable for forest timbering.

In this case the court allowed disclosure of the assessment data. The *Szikszay* case illustrates the situation where requestors would acquire individual gain from the disclosure of personal information about other people. While it appears that disclosure serves no beneficial social purpose in this situation, it does seem to support a societal ideal of economic autonomy. Disclosure may provide the means for people to realize their entrepreneurial dreams. Thus, in *Szikszay*, the disclosure supports the development of the requestors' tree business. More significantly, disclosure of assessment-type data is less likely to harm people than other, more personal information.

A final case provides a disclosure example where private gain and social benefit intersect. In this type of case, courts seem more likely to grant disclosure requests. In *Stenger v. LeHigh Valley Hospital Center*,[35] a recent Pennsylvania case, a woman sought access to various automated data from a hospital and blood bank for use as evidence in her negligence case against the hospital and the blood bank. The hospital gave the woman a blood transfusion after she was injured in an accident. A blood donor contaminated the blood with the A.I.D.S. virus and the woman's entire family, including herself, contracted the disease. The woman requested the identity of the blood donor, the identity of other recipients of the donor's blood, anonymous A.I.D.S. tests results of the recipients, and the date the blood bank delivered the blood. The court permitted disclosure of all the requested information except for the identity of the other recipients of the donor's blood.

In *Stenger*, the data requested served both private and social interests. First, the requested data would serve a private interest because it would help the plaintiff prove her case. Yet, the value of disclosure in this situation seems tarnished, as it was in the abortion context. The A.I.D.S. issue is very personal. A.I.D.S. victims can be stigmatized and ostracized if others know of their condition. The plaintiff's desire to

34. 107 Misc. 2d 886, 436 N.Y.S.2d 558 (1981).

35. 382 Pa. Super. 75, 563 A.2d 531 (1989).

prove her case may pale in comparison. Thus, the harm to the other donor recipients may outweigh the private benefit enjoyed by the plaintiff. Yet, on a second level, such disclosure is socially important. A.I.D.S. is a serious disease and medical providers are in a position to affect its transmission. The disclosure can act as a further check on the medical community, forcing them to exercise extreme care. In addition to a private interest in litigation, there is a strong societal disclosure value in protecting people from this disease. In *Stenger*, the societal and personal interests intersected in favor of disclosure, although the disclosure seriously could harm third parties. The court compromised and permitted disclosure of all but the most harmful data.

C. DISCLOSURE CONCLUDED

This section attempted to demystify the term disclosure. Its goal was twofold. First, it attempted to define disclosure using a continuum analogy. Disclosure was placed on the continuum along with the collection and meta-collection concepts. Second, this section tried to ascertain why society values disclosure and how society should weight these disclosure values. This section investigated these disclosure values through a survey of uses and circumstances.

Four disclosure values emerge from the data. They include interests in disclosure for welfare state maintenance, for law enforcement needs, for a general public "right to know," and for personal use or private gain. If these interests were plotted along a continuum, where the left side represented a high disclosure value and the right side represented a low disclosure value, then the four values would lie on the scale in the order listed above. When the requestor intends to use the requested data for a beneficial social program designed to help individuals or groups, such as a crime or drug prevention program, then the disclosure interest seems high. Law enforcement purposes also rate high on the scale, but the potential for selective enforcement abuses taint this public safety interest. The public's "right to know" is important both because it is derived legislatively and because of its traditional democratic rationale. Yet, the "right to know" may permit indiscriminate disclosure. Finally, disclosure for private gain is the least valued simply because it benefits only the requestor. However, it should be recognized that these groups do not represent static categories. They are general categorizations that help to form an analytical scheme. It is possible to have a case that falls into the personal benefit category, but its effect is to benefit society generally which may give it an increased weight. The *Stenger* case above is an example of this type of case.

Finally, it should be emphasized that giving disclosure a high or low weight often will not determine whether a requestor will receive the

personal data. The disclosure value must also be weighed against the non-disclosure value. Assigning the disclosure weight is a threshold consideration; it indicates how much weight to place on the disclosure side of the scale. Yet, it is possible that when the scales are weighted, a low valued disclosure interest will outweigh a lower valued non-disclosure concern. The next section considers society's values in non-disclosure.

III. PRIVACY

Privacy is the "buzz" word of "buzz" words. It is used to mean anything and everything. The privacy concept is most often coupled with a cry of invasion, and this cry has grown louder with the advent of the computer age. It is essential to ascertain what courts and people mean when they wave the privacy right flag. This section attempts to dissect this amorphous, expansive value.

A. THE STATE CASES: A NORMATIVE GRADATION OF WRONG

This section focusses on two inquiries. The first inquiry examines the records to determine the characteristics of the personal information which caused the invasion claims. Once the reason for the invasive feeling is pinpointed, the second inquiry ranks the harm that resulted from the perceived invasion. The harm is scaled according to a normative gradation of wrong.[36] On the least offensive end of the continuum is "hurt," which can occur when the automated database works to *obstruct* one's interests or goals. One is still able to achieve one's interests or goals but the means are made much more difficult. In the middle of the harm scale lies "harm," which results when the computerized information *disables* one's ability to achieve one's interests or goals. Here, essentially, one can no longer achieve the things one wants. On the most offensive end of the scale exists "the purely bad thing," where the collection, storage, and use of the data violates a sense of our moral norms. The wrong is *the invasion itself*, regardless of the existence of any harm. This Note does not present the normative gradation of wrong analysis as *the way* to sort out the privacy mess. Instead, it is hoped that this analysis partially will illuminate a very clouded subject. The cases follow.

1. *Sexuality*

In *Planned Parenthood v. Van de Kamp*,[37] the California Attorney

36. Please note that this idea of ranking and the particular termination evolved from extensive discussions with Ronald R. Garet, Professor of Law and Religion, University of Southern California Law Center.

37. 181 Cal. App. 3d 245, 226 Cal. Rptr. 361 (1986).

General and Alameda County District Attorney interpreted a state child abuse prevention law. Their interpretation required physicians and mental health professionals to report minor patients who engaged in sexual activities with other minors. They broadly read this law to include *consensual* sexual activity between minors within its expanded scope. The authorities would retain the identity of these youth "offenders" in a central database which would enable them to track the minors and prevent future violations. Planned Parenthood, physicians and other mental health professionals objected to the broad reading of the law. They felt that the legislature enacted the law to prevent child abuse and not to scrutinize normal social and sexual adolescent development.

Allowing authorities to track sexual activity between consenting adolescents seems wrong. Part of the reason may be that sexuality is one of many dimensions which comprise a person's core being. Sexuality helps shape a person's self-perception and contributes to the making of a complete human being. Most significantly, beginning sexual exploration may have a sharp effect on the individual development process. The first exposures to human sexual experiences determinatively can shape a person's feelings about his or herself. Since sexuality is so central to one's sense of self, people want their sexual experiences and practices free from outer view or control, unless they give their informed consent.

The California database ranks as a "purely bad thing." It violates a moral norm. One's sexuality is core and should remain inviolate. Our society should value healthy, well-adjusted people. A database which tracks the sexual activity of society's young people at the most crucial stage of their self discovery seems counter to these ideals. Therefore, a database that monitors sexual development is intrinsically offensive. Whether or not adolescents suffer harm as a result, it is a "purely bad thing."

2. *Emotional Health*

There are a number of cases in which parties objected to the computerized database because it posed the threat of emotional harm. In *Webb v. City of Shreveport*,[38] a Louisiana labor union organizer requested access to Shreveport's municipal employee personnel database so that he could organize the employees into a union. *Hinderliter v. Humphries*,[39] a Virginia case, involved a city council member's inappropriate release of a policeman's employment record. The policeman arrested the member's daughter, and the member, intending to bring

38. 371 So. 2d 316 (La. App. 1979), *writ denied*, 374 So. 2d 657 (La. 1979).

39. 224 Va. 439, 297 S.E.2d 684 (1982).

brutality charges against the policeman, wanted to use the personnel file as leverage. In *Mullin v. Detroit Police Department*,[40] a person calling himself a traffic researcher requested access to the police department's traffic accident database. The data-base included information about parties involved in accidents and about the police officers, present at the scene of the accident. In each of these cases, the parties objected to the request for data. The objectors claimed that the subjects of the records could suffer emotional harm from embarrassment or reputational damage if the requestor used or purviewed the records.

The parties' claims to prevent emotional harm appear viable. A tarnished reputation, ridicule, and embarrassment threaten a person's self-esteem and confidence. Feeling good about, and being proud of, one's self is part of being a complete, functional human being, and, therefore, society should place a high value on people's emotional health. When third parties access data which has the potential to damage self-perception, the risk is great that emotional harm may occur.

This emotional harm seems to fit into the crippling "harm" category. Yet, it is harder to rank on the normative wrong scale than the sexuality example discussed above. Emotional harm seems to merit placement in the higher valued harm category because society should not sanction the damaging of people's emotional well-being. Self-esteem and confidence are good feelings for people to have about themselves. However, emotional harm does not merit placement in the "purely bad thing" category. First, a "purely bad thing" exists whether or not there is harm. Here, the triggering point is the emotional *harm*. Second, there are circumstances when such harm, although not intentional, will be a necessary by-product. For example, if a policeman brutally arrested a person, then a disclosure of his personnel file may be necessary to evaluate the arrest. In contrast, there are no circumstances when a "purely bad thing" normatively would be acceptable. Therefore, emotional harm may fall under the "harm" category on the gradation scale. Such harm can be disabling. As a result of such information being divulged, a person can feel so poorly about herself that she may not be able to hold a job or maintain relationships. The emotional harm threat fits best in the debilitating "harm" category.

3. *Employment Discrimination*

In *Industrial Foundation of the South v. Texas Accident Board*,[41] a non-profit corporation, composed of 282 employers in the south, requested the use of the Texas Accident Board's workers' compensation database. This database contained various information about workers'

40. 133 Mich. App. 46, 348 N.W.2d 708 (1984).

41. 540 S.W.2d 668 (Tex. 1976), *cert. denied*, 430 U.S. 931, (1977).

compensation claimants, including the claimant's name, injury, social security number, employer and attorney. The Accident Board did not want to release the information because it feared that the Foundation would use the data for discriminatory purposes. Essentially, the Foundation likely would release the information to bar workers, who had made injury claims, from employment in many southern companies.

A few cases,[42] described in detail in previous sections of this Note, dealt tangentially with discrimination. These cases' factual scenarios involved parties acquitted of trespass and loitering crimes and cleared of child abuse accusations. In these cases, although the judicial or administrative bodies cleared the parties of all wrongdoing, the authorities wished to maintain information about the parties in a central database for future law enforcement needs. The acquitted people objected to their names remaining in the databases for several reasons, including the belief that employers could obtain the information and deny them employment opportunities.

The Board's and the cleared plaintiffs' concerns have merit. The cases above present situations ripe for such unfair activity. The data, be it a workers' compensation claim or an acquittal record, can be used by employers to discriminate. If discrimination is permitted, then a chilling effect can occur. For example, as a result of the Texas case, workers may opt not to report their serious injuries for fear that they could lose work opportunities. In addition to the individual worker having to suffer serious injury without compensation, the employer will have little incentive to remedy the unreported dangerous situation which may result in harm to others. Our society should not support discriminatory employment practices because people should have the equal opportunity to obtain work. Work is an essential part of peoples' lives. It is necessary to work to earn the means for food, shelter, medical care, and for the non-necessities that enrich one's life. More significantly, work can provide emotional sustenance. People often get much pleasure and self-fulfillment from their occupations. Our society should discourage employment practices which discriminate.

Employment discrimination is a serious wrong. On one hand, discrimination seems to merit placement as a "purely bad thing." Whether or not a person is actually harmed by discrimination is irrelevant. Our society should not permit the unfair and unequal treatment of people because they are of different races, genders or physical makeup. Yet, while work is core to our lives, it does not seem to be as essential as sexuality and emotional well-being. It seems that one can be fulfilled

42. Petition of Bagley, 128 N.H. 275, 513 A.2d 331 (1986); Davidson v. Dill, 180 Colo. 123, 503 P.2d 157 (1972); Roth v. Reagen, 422 N.W.2d 464 (Iowa 1988); Koppes v. City of Waterloo, 445 N.W. 2d 774 (Iowa 1989).

and whole, despite discrimination in the workplace. Nevertheless, discrimination is inherently wrong, and our society should not practice or permit discrimination, irrespective of whether it causes harm. While our society may consider employment to be less fundamental than sexuality or emotional health, discrimination in the workplace can make people feel bad about themselves and directly impact their emotional and sexual well-being. The non-discrimination value may approach the "purely bad thing" data point on the normative gradation of wrong.

4. *Identifiers: Name and Address*

Many of the state cases involved name and address databases.[43] The factual scenario in *Kestenbaum v. Michigan State University*[44] is representative of this group of cases. In *Kestenbaum*, a political candidate in the local election requested access to the University's student directory database. The candidate wanted to use the names, addresses and phone numbers in the database to expand his electoral mail campaign.

There are at least two arguments that explain why people consider identifier data, i.e., name, address and phone number, inviolate. First, our names, and our addresses to a degree, are a significant part of ourselves. People have a certain proprietary feeling about their names. Although on a more superficial level, our names are a part of us. For example, when we meet people, we often describe ourselves by using our names and where we live. We recognize others by their names which helps us to communicate. Also, while we freely give others this identifier data, we prefer to do the giving. We are bothered when we find junk mail in our mailboxes or receive a phone call from a telemarketing agent as a result of being on a mailing list. People would prefer to decide when others can receive their personal information.

The second argument, set forth by the *Kestenbaum* court, is that address and telephone data function as conduits for potential intrusion in to the home. Constitutional jurisprudence gives the home special significance.[45] The courts consider the home to be an intrusion free zone, since it is within the home environment that people develop their most personal relationships with spouse, family, and friends. Names and addresses are invitations to intrude into the sacred home realm.

---

43. *See*, Webb v. City of Shreveport, 371 So. 2d 316 (La. 1979), *writ denied*, 374 So. 2d 657 (La. 1979); Mich. State Employees Assoc. v. Dep't of Management & Budget, 428 Mich. 104, 404 N.W.2d 606, *aff'g*, 135 Mich. App. 248, 353 N.W.2d 496 (1984); Matter of Szikszay v. Buelow, 107 Misc. 2d 886, 436 N.Y.S.2d 558 (1981).

44. 414 Mich. 510, 327 N.W.2d 783, *aff'g*, 97 Mich. App. 5, 294 N.W.2d 228 (1980). Note that this case is unique as the court in *Kestenbaum* held that the name, address, and telephone data should be protected from disclosure.

45. F.C.C. v. Pacifica Found., 438 U.S. 726 (1978).

It is questionable whether this data category even should lie on the normative gradation of wrong. Name and address data is so common that virtually it is impossible to view its use as a "purely bad thing" which violates a moral norm. Also, such data use does not seem to disable the subject person, as the "harm" range suggests. It is even difficult to consider identifier data as a "hurt," obstructing an interest or a goal. Yet, the parties could argue that the release of identifier data obstructs one's control over access to both one's self and one's home. If identifier data belongs on the continuum at all, then its place is on the farthest edge of the normative gradation wrong's "hurt" range.

5. *Medical History and Records*

There are a cluster of cases which discuss medical histories and records. In *Doe v. Axelrod*,[46] described in greater detail above, the New York Health Department wanted to create a database composed of personal data records from patients who used prescription benzodiazepines for mental health treatment. The public database would include the person's name, diagnosis, and doctor. In *Peninsula Health Care v. Rahm*,[47] also described above, the Washington State Health Department wanted to design and maintain a database of all people who sought therapy from publicly funded mental health clinics. Again, the data would have included a person's name, diagnosis and clinic. The information would have been available to all state social services departments and to pertinent federal agencies. In Pennsylvania's *Stenger v. LeHigh Valley Hospital Center*,[48] a woman who had received an A.I.D.S. contaminated blood transfusion wanted the blood donor's identity disclosed and access to all other donor recipients' records. Finally, in Illinois' *Family Life League v. Department of Public Aid*,[49] a private group wanted access to data on publicly funded abortions without patient identifiers. In all four of these cases, people opposed the disclosure of the medical data.

There is no easy answer to the question of why people wish to prevent the release of medical data about themselves. In the cases involving mental health and A.I.D.S., the desire for confidentiality may rest in a fear of prejudice. People suffering from mental illness or diseases like A.I.D.S. are often socially and emotionally ostracized. Therefore, people may wish to keep their records out of public view to protect themselves from discrimination or ridicule. In the abortion context, in addition to stigma, women are faced with a morally difficult decision. It seems wrong that other people should be allowed to contribute to the

46. 144 Misc. 2d 777, 545 N.Y.S.2d 490 (1989).
47. 105 Wash. 2d 929, 719 P.2d 926 (1986).
48. 386 Pa. Super. 574, 563 A.2d 531 (1989).
49. 112 Ill. 2d 449, 493 N.E.2d 1054 (1986).

emotional pain an individual suffers when groping with the complex choice of whether to have an abortion.

While data collection and release in the medical context is not a "purely bad thing," it likely ranks in the "harm" portion of the normative gradation continuum. It should not be characterized as a "purely bad thing" because there are circumstances that mandate such data collection and release. However, medical information disclosure significantly can impact a person's core being. There is a potential for great harm to both emotional and physical well-being. Ostracism, as a result of illness, can damage one's self-perception and it should be an individual's exclusive decision whether or not to undergo a certain medical procedures. In addition to mental and bodily integrity, there is the possibility of a serious chilling effect: Ill people may not seek the treatment they need for fear of ridicule or ostracism. Medical data disclosure ranks on the "harm" range in the normative gradation of wrong.

C. Privacy Concluded

The state cases reiterate that the privacy value is complex and amorphous. The cases indicate that privacy is a conglomeration of various interests inextricably linked to one's sense of self. Some of the areas deemed private in cases, such as sexuality, emotional well-being, physical health, employment opportunity, and personal identifiers, represent attributes which make people complete human beings. Some of these interests are core, such as sexuality, and some are more peripheral, such as personal identifiers. Yet, all of these values seem to add up to what "me" means and each individual should be sovereign over this "me."

The state cases show how people fear that data collection, storage and use will harm their "me" or sense of self. In an attempt to evaluate this fear, this section analyzed various privacy values, such as sexuality and emotional well-being, in light of the potential harm caused by disclosure. The various values and their disclosure harms were ranked on the normative gradation of wrong scale; the scale consists of "hurt," "harm" and "purely bad thing" data points. The normatively weighted scale will help to determine when disclosure of a certain type of data should be allowed.

IV. THE COMPUTER DIMENSION

A. Introduction

The computer has both a passive and an active role in the disclosure/privacy dilemma. In its passive role the automated database is in the background; the cases included in this study all involved informa-

tion stored or to be stored in computerized databases. In some cases, parties wanted to access data maintained in computers or to create new databases. In other cases, people protested the existence of databases and wanted the courts to deny others access to the data.

However, the computer has a greater role than that of a backdrop for the disclosure/privacy conflict. While the computer did not create the tension between privacy and disclosure, it has exacerbated this preexisting tension. First, the computer has increased people's access to information. By collecting, organizing and storing the data in a central repository, it is easier for people to obtain and use the data. Second, the volume of information available to the public is greater. The automated database has storage capacities that enormously exceed manual file storage. Computer disc drives can hold amounts of information equivalent to university libraries. Third, the computer has made it meaningfully and efficiently possible to combine voluminous groups of information. Computer matching permits the creation of profiles on individuals gathered from various databases. The disclosure problems and privacy concerns existed before the advent of computers, but the computer exacerbates these preexisting problems. Orwellian rhetoric abounds in all the cases and grows more shrill in the more recent judicial opinions.

B. THE STATE CASES

The state courts display varied responses to the impact of the computer on the privacy/disclosure dilemma. Some courts recognize the heightened dimension added by the automatic database. Other courts seem to ignore the computer aspect altogether or discount the computers impact on the conflict. A few of the cases and a brief discussion follow.

1. *The Computer's Significant Invasive Impact*

Many state courts have recognized the exacerbating effect that the computer may have on our society's conflict between its disclosure and privacy values. In *Kestenbaum v. Michigan State University*,[50] discussed in detail above, an election candidate desired access to a university computer tape that contained all of the students' names and addresses for his election campaign. In addition to denying his request, the court commented on the impact of the computer. The court stated that the "form" of data storage motivates the invasion. It felt that computers made more information available, readily accessible, and easily manipulable. The court concluded that the judicial system had a duty to be increasingly vigilant in its protection of individual rights as a re-

50. 414 Mich. 510, 327 N.W.2d 783 (1982), *aff'g*, 97 Mich. App. 5, 294 N.W.2d 228 (1980).

sult of the intrusive computer. In *Mullin v. Detroit Police Department*,[51] also described above, a private researcher wanted to access individual traffic records. The court did not permit the disclosure and claimed that the computer and its matching capability had increased the risk of privacy invasion. Like the *Kestenbaum* court, the *Mullin* court declared that the efficiency of the computer motivated intrusion in to individuals' personal lives.

The court in *Spargo v. New York*[52] permitted disclosure of a criminal investigation file. The New York State Commission on Government Integrity and the New York State Board of Elections needed the file to continue their investigation of illegal state campaign financing. The subject of the file, a key participant in the illegal scheme, claimed that the entities should not have access to the file since it would invade his personal privacy and violate New York's Personal Privacy Protection Law.[53] The court disagreed with the petitioner and expressly held that the law was enacted to protect against dangers to privacy posed by *computerized intrusion* into automated databases. Here, the requested file was a manually accessed paper record. Therefore, the court declared that the statute was inapplicable. The *Spargo* case is interesting because it indicates that the New York legislature may perceive a potential for increased harm from information stored in a computerized manner.

Finally, a series of cases generally refer to the perceived greater intrusion resulting from storage of data in computers. In *Petition of Bagley*,[54] a child abuse case discussed in more detail above, the court did not permit disclosure because of a distinct due process violation. However, the court did comment on the impact of automated databases and stated that although the records were to be kept confidential, the central registry posed the problem of an increased invasion of privacy. In *Perkey v. Department of Motor Vehicles*,[55] the California Supreme Court prohibited the California Department of Motor Vehicles from disseminating information from a computerized fingerprint file to third parties for uses unrelated to motor vehicle safety. The court emphasized that the computer instrumentally had increased the risk of privacy invasions. Finally, in *Industrial Foundation of the South v. Texas Industrial Accident Board*,[56] a workers' compensation case discussed in several sections above, the court noted that an automated records

51. 133 Mich. App. 46, 34 N.W.2d 708 (1984).

52. 140 A.D.2d 26, 531 N.Y.S.2d 417 (1988), *appeal denied*, 72 N.Y.2d 809, 531 N.E.2d 299, 534 N.Y.S.2d 667 (1988).

53. N.Y. PUB. OFF. LAW § 91 (Consol. 1990).

54. 128 N.H. 275, 513 A.2d 331 (1986).

55. 42 Cal. 3d 185, 721 P.2d 50, 228 Cal. Rptr. 169 (1986).

56. 540 S.W.2d 668 (Tex. 1976), *cert. denied*, 430 U.S. 931, (1977).

database with a direct tie-in improved efficiency. However, the court also recognized that the efficiency heightened the likelihood of intrusion into an individual's personal affairs. All of these cases, and others not listed,[57] suggest that the evolution of computerized technology has either threatened to decrease or actually diminished the scope of peoples' personal realms.

2. *The Computer has an Insignificant Impact*

Despite the multitude of cases which lament the decrease in individual privacy from automated databases, some courts have held that the computer has a negligible effect on privacy and disclosure problems. In the Ohio case *State v. Andrews*,[58] the court permitted the disclosure of drivers' license abstracts and offense data for persons who had committed multiple offenses. The Beacon Journal Publishing Company requested the data without stating why it wanted the information. The Journal merely mentioned the F.O.I.A. as its reason for obtaining the information. The Director of the State Motor Vehicle Department objected to the request on several grounds including the privacy of driving citizens, the existence of other information in the database and the cost of retrieval. The court considered the Director's Orwellian fears to be an invalid basis for retaining the information. It held that the mere storage of information in a computer should not become an excuse for non-disclosure. Furthermore, the court stated that a computer should not be used to make data unattainable.

In *Michigan State Employees Association (M.S.E.A.) v. Department of Management and Budget*,[59] discussed in detail above, the Association wanted to access the names and addresses of all state civil service employees. The Association wanted to mail organizational and informational material to inform employees of their labor rights. The Department protested the request on privacy grounds, but the court permitted the disclosure. The court dismissed the issue that the records were stored on a computer tape. It stated that the fact that the information is contained in computer form does not alter the presumption in favor of disclosure.

Two final cases briefly echo the views of the *Andrews'* and *Michigan Employees'* courts. In *Minnesota Medical Association v. Minnesota*,[60] a case involving records of publicly funded abortions described in previous sections, the court stated that there was no need for special

57. Family Life League v. Dep't of Public Aid, 112 Ill. 2d 449, 493 N.E.2d 1054 (1986); State v. Nixten, Nos. 86AP-139, 86AP-140 (Ohio App. filed Aug. 19, 1986).

58. No. 75AP-418 (Ohio App. filed Jan. 15, 1976).

59. 428 Mich. 104, 404 N.W.2d 606, *aff'g*, 135 Mich. App. 248, 353 N.W.2d 496 (1984).

60. 274 N.W.2d 84 (Minn. 1978).

rules to safeguard privacy merely because records were stored in computers. Also, in *Matter of Szikszay v. Buelow*,[61] a New York assessment data case detailed above, the court denied the Cattaraugus County Real Property Tax Service's request to prevent disclosure. The court declared that the computer form did not alter the public's right to official information. This set of cases diametrically opposes the views espoused by the courts in the previous section. Here, the courts seem to view the Orwellian cry of the computer as a mere ruse to restrict the flow of information to the public.

C. THE COMPUTER AS A SOLUTION TO THE DISCLOSURE/PRIVACY CONFLICT

The previous discussion indicates that the computer dimension has further complicated the disclosure/privacy dilemma. In addition, to courts weighing the respective values of disclosure and privacy, the courts now must contend with the impact that the computer has on the conflict. Some courts view the impact as greater than others, but most courts, at least, do examine the computer effect. Despite the courts' debate surrounding the computer's actual impact on the privacy/disclosure conflict, it is possible to view the computer as providing a partial solution to the privacy/disclosure problem. Computers have the technical capability to mask identifiers and to make their records anonymous. People and entities can access records for various purposes without connecting the record to a real person. Subjects of such access are less likely to be concerned about disclosure or privacy. If the people cannot be identified, they should not care if the collector obtained data for one purpose and used it for another. There is little chance that a person's private realm or sense of self will be impacted upon if there is no identifier in the record. Many courts have championed the computer's anonymity capability as a solution to the disclosure/privacy problem. A few of these cases follow.

In *Webb v. City of Shreveport*,[62] a labor union organizer requested data about city employees to aid his attempt to organize a union. The city denied the request. It dually claimed that the records contained information which potentially could humiliate and embarrass the employees and that the employees furnished the data for limited purposes. The court permitted the disclosure. The court stated that as a result of the computerized nature of the records, the city easily could extract only the names and addresses of the employees for the labor organizer's use. Also, in *Bowie v. Evanston Community Consolidated School Dis-*

61. 107 Misc. 2d 886, 436 N.Y.S.2d 558 (1981).

62. 371 So. 2d 316 (La. App.), *writ denied*, 374 So. 2d 657 (La. 1979).

trict,[63] the Illinois court permitted disclosure of standardized test scores, identified by race, to parents with children in the District's schools, but who were unrelated to the student test takers. The court denied the Evanston Community Consolidated School District's attempt to prohibit release of the data. The court stated that since the information was computerized, it was easy and safe to redact the identifying information to comply with the parents' request. In addition, the Washington court in *Peninsula Counseling Center v. Rahm*,[64] a case discussed in detail above, permitted disclosure of public mental patient data to various government entities. The court felt that the automated records could be treated by encoding identifiers, which would remove any personal connection to the data. Other cases in Illinois[65] and Kansas[66] echo these courts' solutions.

However, the computer's ability to segregate identifier information will not resolve the disclosure/privacy conflict in all situations. Under certain circumstances anonymity will not suffice. The Colorado court, in *Sargent School District Number RE 33J v. Western Services, Inc.*[67] denied a non-profit group's attempt to obtain students' CTBS test scores. The group offered to replace the name record with an ethnic code and randomly to arrange the scores. The court stated that merely because the data can be parsed and manipulated does not necessarily compel access to the exempted information. In situations where "purely bad things"[68] are at issue, the removal of identifiers is insufficient. There are some areas so essential to self-definition that related information should not be disclosed, or sometimes, even collected. Data on sexuality, abortion, A.I.D.S., or data used to discriminate against people, discussed in the Privacy section above, are examples of core information. Essentially, computerized databases only partially resolve the disclosure/privacy conflict. Where merely eradicating identifier information will satisfy peoples' concerns about automated databases, the computer may be a viable solution to the conflict.

V. AN APPROACH TO THE DISCLOSURE/PRIVACY CONFLICT

This Note attempted to demystify the disclosure/privacy conflict in the automated data scenario. In so doing, it discovered that our society values both disclosure and privacy in distinct contexts. The Note's next

63. 128 Ill. 2d 373, 538 N.E.2d 557 (1989).

64. 105 Wash. 2d 929, 719 P.2d 926 (1986).

65. Family Life League v. Dep't of Pub. Aid, 112 Ill. 2d 449, 493 N.E.2d 1054 (1986); Hamer v. Lentz, 171 Ill. App. 3d 888, 525 N.E.2d 1045 (1988).

66. State *ex rel.* Stephan v. Harder, 230 Kan. 573, 641 P.2d 366 (1982).

67. 751 P.2d 56 (Colo. 1988).

68. For this Note's definition of a "purely bad thing" please see above section on Privacy.

goal is to propose a way for adjudicators to consider cases where disclosure values clash with privacy values. This section does not promise to provide *the* answer to this complex problem. Instead, it provides *an approach* to the disclosure/privacy dilemma.

A. An Approach

A mechanistic model will not offer the best method for solving the disclosure/privacy problem. No equation type analysis with fungible variables that would provide an answer in each circumstance would be viable. Furthermore, a voluminous list of "If this . . ., then that . . ." postulates also are not very useful. The disclosure/privacy dilemma involves norms. Cultural values meaningfully cannot be plugged into mechanical formulae. Norms demand individual discretion of themselves and the circumstances, especially when competing norms exist. Therefore, courts must use something other than a mathematical-type equation to solve these problems.

A normative case-by-case analysis may be the most useful tool for resolving the disclosure/privacy conflict. This analysis could be guided by a three step inquiry. First, the adjudicator could consider the disclosure value. The adjudicator could determine what type of disclosure was challenged, i.e., collection, meta-collection, or disclosure, and then ascertain the societal value placed upon the use of the requested information. Second, the adjudicator could evaluate the privacy value at stake. For example, he or she would ask whether the value involved a "purely bad thing," that no disclosure value could challenge, or a "hurt," that could be subordinated to disclosure when society deemed disclosure more valuable. Third, the adjudicator could try to resolve the conflict with the advantages of the computer. The computer's processing abilities can redact identifiers and remove the privacy concern altogether to satisfy society's interest in disclosure. Finally, if the computer does not provide a solution to the conflict, then the adjudicator would balance the two valued norms in each circumstance and determine whether the privacy or the disclosure value should take precedence.

This normative case-by-case approach is not without its drawbacks. As with any normative evaluation, adjudicators are given much discretion to shape and select our society's norms. It is quite possible that courts could be arbitrary in their normative disclosure/privacy evaluation. Furthermore, there is little accountability for such decisions. While some states periodically hold popular elections of adjudicators, other states place full responsibility for accountability within the appellate system. A type of cultural/normative tyranny can be envisioned.

However, fear of a cultural/normative tyranny may be unrealistic.

First, a case-by-case approach demands careful scrutiny of the facts and circumstances of each case. Because each case requires its own analysis, an adjudicator's systematic arbitrariness may be hindered. Second, the state legislatures can serve to check the courts' discretion. If courts' decisions resolve the disclosure/privacy conflict in a manner that is counter to society's accepted norms, then the elected representatives may enact legislation to embody the desired values and eradicate the erroneous decision's effect.

Third, and more significantly, it is foolish to believe that our courts adjudicate in a normative vacuum. Courts are made up of individuals shaped by our society's values. Their decisions necessarily incorporate these cultural and normative beliefs. Also, the law is rooted in our society's norms. "Policy" determines the rule structure assumed by our laws, and this "policy" is composed of norms. For example, our laws more stringently punish first degree murder than manslaughter, because our *norms* dictate that an intent to kill another human being deserves more punishment than a killing without such scienter or recklessness.

Despite the various criticisms, a normative, case-by-case analysis guided by inquiry steps may be the most honest and effective approach for adjudicators to employ when they encounter the disclosure/privacy dilemma in automated data cases.

VI. CONCLUSION

This Note provided a normative examination of when entities or individuals, who legally collected and stored personal information in a computer, can distribute this personal information to others without the subject party's consent. First, this Note discussed society's values in the disclosure of information to others. For this purpose, this Note dissected the term disclosure into three components: collection, meta-collection, and disclosure. Society's concern about disclosure was great when the activity was a "disclosure activity," i.e., the collector obtained the information for one purpose and used it for a conflicting purpose. The second section of this Note examined society's values in the amorphous idea of privacy. A normative gradation of harm was developed, consisting of a continuum with "purely bad thing," "harm" and "hurt" data regions. The concern for privacy was greatest when the collected data involved a "purely bad thing." Outside of the "purely bad thing" realm, compromises to satisfy significant disclosure values would be permissible under certain circumstances. The third part of this Note considered the computer dimension of the privacy/disclosure dilemma. Some courts viewed the computer as a frightful Orwellian invader of the personal realm while other courts felt that the computer had no im-

pact. Yet, most significantly, the computer may provide a partial solution to the dilemma. The computer can satisfy disclosure needs by offering access to information, while simultaneously allaying privacy concerns by masking the subject's identity with symbolic identifiers. The computer is a viable solution for all but the "purely bad thing" privacy category, which demands that no information of this type even be collected. Finally, this Note provides a model for adjudicators grappling with the privacy/disclosure dilemma. The model set forth is a balancing model guided by society's shared normative values.

The privacy/disclosure dilemma in the computer context is complex because of its normative character. Society has strong and valid values in both privacy and disclosure interests. While the computer may provide a partial solution to the problem, the conflicting values may provide problems that the computer's anonymity tools cannot solve. Each distinct fact situation may demand a unique result. Sometimes the disclosure values will be more significant than the privacy values. At other times society will more greatly revere the privacy concerns. While this ad hoc balancing approach lacks the certainties of bright line rulemaking, it may be the best method for adjudicating society's privacy/disclosure conflicts. The ad hoc method allows society to be dynamic and flexible as its needs change through time. The privacy/disclosure conflict is norm driven, and norms are fluid because they are derived from society's shared values. Society's values in privacy and disclosure may change, making a flexible analytical model requisite.

*Eve H. Karasik**

* Ms. Karasik received a B.A. in History from the University of California, at Berkeley, in 1985. She is currently a third year student at the University of Southern California Law Center, in Los Angeles, California, and will begin work as an associate with Stutman, Treister & Glatt in the fall of 1991.