UIC John Marshall Journal of Information Technology & Privacy Law

Volume 10
Issue 2 *Computer/Law Journal - Spring 1990*

Article 2

Spring 1990

The Scarlet Letter "A": AIDS in a Computer Society, 10 Computer L.J. 233 (1990)

M. Nicole van Dam

NOTE

THE SCARLET LETTER "A": AIDS IN A COMPUTER SOCIETY

I. INTRODUCTION

The logistics of reporting and ultimately tracking the names and medical records of AIDS victims/carriers will inevitably entail the construction of an AIDS database to more efficiently analyze and control the medical diagnosis information.[1] Such a database would likely contain the AIDS carrier's name, medical history, previous and present sexual contacts, and certain other extremely personal characteristics (i.e., drug use) which researchers feel might prove helpful, at least in an explanatory sense, in tracking the likely causes and spread of the disease. This Note explores the question of whether creating such a database would be prudent given the current state of computer-matching as well as the minimal safeguards available against unwarranted access to the database. More specifically, the Note focus is upon the desirability of, and the legal issues raised by, the creation and maintenance of a state or federal computer database which would contain the names of individuals who have tested "seropositive"[2] but have not yet been diagnosed as having AIDS.

---

1. "Like the credit industry, hospitals and insurance companies maintained manual data collection systems throughout most of the twentieth century. Computerized information retrieval systems are products of the last two decades." Note, *Toward a Uniform Right to Medical Records: A Proposal for a Model Patient Access and Information Practices Statute*, 30 UCLA L. REV. 1349, 1354 (1983) [hereinafter *Uniform Right*] (citing PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 58 n.3 (1977); Telephone interview with Jim Corbett, Gen. Counsel, MIB (Dec. 8, 1982)). The Center for Disease Control (C.D.C.) in Atlanta established an AIDS database in mid-1983; this computer surveillance system enables them "to monitor national AIDS trends more efficiently." R. SHILTS, AND THE BAND PLAYED ON 351 (1987).

In addition, eight states currently use some method of tracking those who test seropositive for AIDS, and as the nation's hysteria grows, more states are likely to follow suit. L.A. Times, Sept. 20, 1987, at 20, col. 6.

2. *See infra* text accompanying note 9.

II. BACKGROUND ON AIDS

> Every day, Danny Joe Ware closes his eyes and prays that people won't be as cruel to his children as they have been to him.
>
> Just 24 years old, the father of three is dying of AIDS in Dallas, the city to which he fled recently from his home in Kilgore, Texas. He has on different occasions been pelted with rocks and jumped by three men, who shattered a beer bottle over his head, broke his nose and bruised some ribs.
>
> "What are you doing?" Mr. Ware recalls screaming during the attack, too weak to defend himself. "Killing AIDS," replied one of the men. "And when we're done with you, we're going to kill your wife and kids, just in case they've got it.[3]

Such violent scenarios are, in part, a fearful response to a virus[4] that kills. AIDS was initially labeled a gay disease—"gay cancer."[5] Common sense has prevailed, however, and it is generally accepted that "the HIV virus, which causes AIDS, knows nothing of homosexuality or drug abuse."[6] The HIV virus is a delicate virus which has not been shown to survive in an airborne state. Thus, it is believed to be transmitted only through blood or semen.[7]

It is important to distinguish between testing positive[8] for the HIV virus and having AIDS. Testing seropositive[9] indicates that one has

---

3. Wall St. J., Nov. 13, 1987, at 1, col. 1.

4. The official name of the AIDS virus is "HIV," although it has also been referred to as "LAV" and "HTLV-III."

5. *See generally* R. SHILTS, *supra* note 1.

6. Wall St. J., Nov. 13, 1987, at 6, col. 1.

> AIDS is by no means restricted to homosexuals. Of the more than 40,000 reported cases of AIDS in the U.S., 65% involve homosexual or bisexual men; 17% intravenous drug abusers. The rest are people sexually involved with infected individuals; hemophiliacs, and others who contracted the disease through contaminated blood. Federal statistics from the Centers of Disease Control report 595 cases of AIDS in children under the age of 13.

Id. at 1, col. 1.

See also AIDS: Everything You and Your Family Need to Know But Were Afraid to Ask (Home Box Office, Inc., Cable Television Broadcast, Oct. 12, 1987) [hereinafter *AIDS*] (statement of Dr. C. Everett Koop, U.S. Surgeon General).

7. Note, *Reportability of Exposure to the AIDS Virus: An Equal Protection Analysis*, 7 CARDOZO L. REV. 1103, 1103 (1986) [hereinafter *Reportability*]. *See also AIDS*, *supra* note 6.

8. "Testing positive" is synonymous with the terms "testing seropositive" and "testing HIV positive."

9. As noted in the *AIDS Project L.A. Newspaper*, AIDS is detected through the use of blood tests:

> Originally introduced in 1985 as part of an emergency effort to safeguard the nation's blood supply, the test to identify HIV infected blood is fairly simple. There are three laboratory versions of the test available, commonly referred to as the ELISA (Enzyme-Linked Immunosorbent Assay), the Western Blot and the IFA (Immuno Fluorescent Assay). Because the ELISA was developed to protect the

been infected with the virus, or more specifically, that the virus has been present in the individual's bloodstream long enough (generally less than six months)[10] for the body to trigger production of antibodies to the virus.[11] However,

> a positive antibody test result does not, by itself, indicate that a person has AIDS. The current Centers for Disease Control definition of a person with AIDS requires three things: (1) infection with the virus, (2) a lowered immune system, and (3) the presence of at least one of a number of opportunistic infections associated with AIDS.[12]

Regardless of the niceties associated with this distinction between testing seropositive for the AIDS virus and actually having AIDS, a positive test result renders the individual who possess the AIDS antibody as potentially infectious as the patient who is actually suffering from AIDS.[13]

When AIDS does occur, the HIV virus attacks, and ultimately destroys, the body's natural immune system thereby preventing persons

---

> nation's blood supply from contaminated or infected blood, it is highly sensitive, and often shows numerous "false positive" test results. For this reason, it is essential that blood showing a positive result with the ELISA be retested with the more specific (and costly) Western Blot or IFA to confirm the actual positive status.

Pickett, *Issues in Testing: A Matter of Informed Choice*, AIDS Project L.A. Newspaper, Fall, 1987, at 1, col. 1.

> Objections to ELISA as a diagnostic tool have two bases. First, the test is not reliable in most populations. The test's sensitivity—its accuracy in correctly identifying persons exposed to HTLV-III—is high. The test's specificity—its accuracy in correctly identifying persons not exposed to HTLV-III—is relatively low. This combination results in a great number of positive results; unfortunately, many of them are false. The test is very effective among the urban gay male population (nearly 100%), less so among IV drug users, and highly inaccurate (30-35%) in low-risk populations.

Reportability, *supra* note 7, at 1111 (citation omitted).

See also Weiss, Goedert, Sarngadharan, Bodner, The AIDS Seroepidemiology Collaborative Working Group, Gallo & Blattner, *Screening Test for HTLV-III Antibodies*, 253 J. A.M.A. 221 (1985); A. FETTNER & W. CHECK, THE TRUTH ABOUT AIDS 265 (rev. ed. 1985).

10. "None of these tests are totally conclusive as it can take from two weeks to six months to produce the HIV antibody after the person has been infected. This is referred to as a window period." Pickett, *supra* note 9, at 1, col. 1.

11. *Id.* "There is thought to be a long period (up to seven years) between [testing positive to HIV] and development of AIDS. . . . [D]ue to the brief history of the disease, the possibility of longer incubation periods cannot be excluded." Comment, *Protecting Confidentiality in the Effort to Control AIDS*, 24 HARV. J. ON LEGIS. 315, 317 (1987) [hereinafter Comment] (citing *Update: AIDS—United States*, MORBIDITY & MORTALITY WEEKLY REP., Jan. 17, 1987, at 17).

12. Pickett, *supra* note 9, at 1, col. 2; *see generally* R. SHILTS, *supra* note 1.

13. "[T]here is medical agreement that an HIV infected person is potentially infectious to others, [so] a positive test result brings a burden to bear upon that individual to not engage in behavior that could spread the virus to others (e.g., unprotected sexual activities, [intravenous] needle-sharing, pregnancy)." Pickett, *supra* note 9, at 1, col. 2.

with the syndrome from fighting off even the weakest infections.[14] It is a disease for which "[t]here is no vaccine and no cure."[15] Many people with AIDS die within eighteen months of diagnosis. Most are dead within three years.[16] "[A] San Francisco Public Health Department study found that 78% of a group of HIV positive gay males developed signs of immune-system damage within 6 1/2 years of their exposure to the virus."[17] "[This] San Francisco study [also] indicated that AIDS may be *seven times* as likely to develop in the sixth or seventh year after infection as in the first or second year."[18] Moreover, the "AIDS fatality rate—the likelihood that a person with AIDS will die from an AIDS related disease is 100%."[19] Among patients diagnosed prior to July 1984, seventy-one percent are reported to have died.[20] Today, between 1 million and 1.5 million Americans are already infected with the AIDS virus.[21] Of these Americans, perhaps 250,000 to 500,000 already show signs of AIDS-Related Complex, or ARC.[22]

Despite the bleak consensus that no cure for AIDS presently exists, "[s]everal experimental treatments appear to slow the virus' progression in infected individuals and may enhance the survival prospects of HIV carriers."[23] One AIDS researcher has even predicted that "[w]ithin 12 to 18 months, we will be able to arrest the disease at whatever stage it is in except for people who are very sick."[24] While such optimism remains rare when discussing AIDS, "recent medical reports confirm that the extraordinarily expensive Burroughs Wellcome

14. *Reportability, supra* note 7, at 1106 (citing A. FETTNER & W. CHECK, THE TRUTH ABOUT AIDS 265 (rev. ed. 1985)); *see also* Comment, *supra* note 11, at 316.

15. *Reportability, supra* note 7, at 1103. *See also* Wall St. J., Feb. 11, 1988, at 17, col. 4.

16. *Reportability, supra* note 7, at 1106 (citing *AIDS: Chapter One* (WGBH Educational Foundation Television Broadcast, Feb. 12, 1985) (transcript, NOVA Series No. 1205)).

17. Wall St. J., Feb. 11, 1988, at 1, col. 1. "Some 30% developed AIDS, 21% ARC. Some 27% had persistent generalized lymphadenopathy (swollen lymph nodes), a condition sometimes classified as ARC." *Id.*

18. *Id.* (emphasis added).

19. *Reportability, supra* note 7, at 1106 (citing Krim, *AIDS: The Challenge to Science and Medicine*, in AIDS: THE EMERGING ETHICAL DILEMMAS 2, 3 (Hastings Center Rep., Spec. Supp., Aug. 1985). *See also* Wall St. J., Feb. 11, 1988, at 1, col. 1 (quoting New York Health Commissioner David Axelrod: "Virtually all those infected are doomed.").

See also Reidinger, *A Question of Balance: Policing the AIDS Epidemic*, A.B.A. J., June 1, 1987, at 69.

20. Comment, *supra* note 11, at 315 (citing *Update: AIDS—United States*, MORBIDITY & MORTALITY WEEKLY REP., Jan. 17, 1986, at 17).

21. Wall St. J., Feb. 11, 1988, at 1, col. 1 (citing the Federal Center for Disease Control in Atlanta).

22. *Id.*

23. *Id.*

24. *Id.* (quoting Dr. Bernard Bihari, physician and AIDS researcher at the State University of New York).

Co. drug, AZT, prolongs the life of AIDS and ARC patients—especially if they [begin treatment] in the early stages of the disease."[25] Many experts agree that "[t]he use of AZT treatments is resulting in significant reduction in progression to AIDS, hospitalization and death."[26] In addition, recent experimentation has shown that injecting a more advanced AIDS patient with blood plasma taken from an HIV positive individual not showing ARC or related disease symptoms, prolongs the life of the advanced patient.[27] Thus, while there may be no present cure for AIDS, *the sooner a seropositive individual is treated, the better that individual's prospects for survival.*

II. THE BENEFITS OF REPORTING NAMES AND CREATING AN AIDS DATABASE

Certain methods[28] have traditionally been employed to combat infectious diseases such as syphilis, tuberculosis, and smallpox. These methods—recording and tracking patient records—have also been instrumental for epidemiological purposes as they have "demonstrat[ed] the link between cigarette smoking and lung cancer; the link between mothers who took diethylstilbestrol (DES) during pregnancy and the risk of vaginal cancer to their daughters; and the link between women's use of estrogens for menopausal symptoms and the increased risk of endometrial or uterine cancer."[29] A frustrated Executive Director of Colorado's Department of Health stated that:

> If we can't use these methods [to combat AIDS], we are doing substantially less than we know how to do . . . . There are tried and true methodologies which have worked in the control of communicable disease before. To the extent they are applicable, they should be utilized. . . . .

---

25. *Id.* at 17, col. 4.

26. *Id.* (quoting Dr. Bernard Bihari, physician and AIDS researcher at the State University of New York). *See also CBS Evening News Report* (August 17, 1989, 5:00 PM) (report by Dr. Howard Torman). The report asserted the following: AZT slows down the progression of AIDS. Early AZT therapy has very clear benefits—all participants in a National Institute of Health (N.I.H.) study showed less than 500 T4 cells, and one half the usual rate of progression to ARC or other advanced diseases. Moreover, the N.I.H. study showed that AZT has relatively minor side effects—3% of those studied were nauseated. *Id.*

27. Apparently this type of treatment is effective because the HIV positive individual, not showing ARC or other advanced symptoms, has blood rich in HIV antibodies. *See NBC Evening News Reports* (Aug. 24-27, 1989).

28. "Traditional public health measures involve testing by name, reporting to the state health agency all positive cases, tracing and notifying others who might have been exposed and, when necessary, quarantining the most dangerously contagious cases." L.A. Times, Sept. 20, 1987, at A20, col. 1.

29. *Uniform Right, supra* note 1, at 1353 n.30 (citing *Privacy of Medical Records: Hearings on H.R. 2979 and H.R. 3444 Before the Subcomm. of the House Comm. on Gov't Operations*, 96th Cong., 1st Sess. 211, 479-82 (1980)).

> Only if we identify and track cases by name . . . could health authorities accurately follow the epidemiology of an infection. With names, they could track down individuals who do not return to clinics after testing positive. They could trace the infected person's partners. They could eliminate duplications in counts.[30]

In sum, "[i]t is antithetical to the practice of medicine; it is antithetical to the practice of public health, not to use names. . . . [T]hat's what public health disease control is all about."[31]

Regardless of the proven medical benefits these methods provide, the questions remain concerning whether the medical treatment of AIDS can be likened to the treatment of syphilis, tuberculosis, and smallpox, all of which have shorter incubation periods and can be treated effectively and whether sufficient epidemiological concerns exist to warrant intrusion into an AIDS victim's privacy. While it is true that a diagnosis of AIDS may not occur within six years of the initial date of infection, an individual *will* evidence the tell-tale antibodies to AIDS (i.e., test seropositive for AIDS and be as potentially infectious to others) within the first six months after infectious contact.[32] Given that the relative incubation period for syphilis, another sexually transmitted disease (for which contact tracing is permitted), is no less than three months,[33] the length of incubation argument, used to distinguish contact tracing for AIDS from the tracing of diseases such as syphilis, appears tenuous.

Opponents of contact tracing also urge that because there is no cure for AIDS, contact tracing will offer those individuals located through the trace no treatment but only despair. However, as previously discussed, the sooner a patient begins treatment for the disease the better the patient's chance of surviving for a longer period of time; early diagnosis offers concrete medical benefits.[34] For example, treatments in the form of early analysis, stepped-up hygiene programs, and drugs which hinder disease progression, such as AZT, have proven effective in many individuals diagnosed as seropositive.[35] In addition, the sooner an individual is made aware of his/her likely infected status, the sooner that

---

30. L.A. Times, Sept. 20, 1987, at 20, col. 1.

31. *Id.* at col. 2.

32. *See supra* text accompanying notes 10-11.

33. During the first stage of syphilis, when chancre sores appear, the blood will not be infected so a conclusive test for syphilis cannot be conducted. It is only after the appearance and disappearance of chancre sores that a conclusive test for syphilis can be administered. This sequence of events takes at least three months from the initial infection. Telephone conversation with the Los Angeles Health Department, North East Health Center (Feb. 22, 1988) (confirmed the accuracy of U.S. DEP'T OF HEALTH, EDUCATION AND WELFARE, SYPHILIS: A SYNOPSIS 45 (1968)).

34. *See supra* text accompanying notes 25-26.

35. *Id.*

person can be counseled to act responsibly toward future sexual partners and the sooner past partners may be targeted for treatment.

With respect to epidemiological concerns, computer-matching has long served as a vital aid to medical research. "[F]or example, although medical records are of the most sensitive nature, studies of cancer in relation to air pollution might well find it useful to process medical and demographic data together in the interests of scientific research."[36] Similar studies could be applied to AIDS to discern why some seropositive individuals' status ripens to AIDS earlier than other HIV positive persons.

Regardless of whether contact tracing is desired for the purpose of treatment or to alleviate epidemiological concerns, its use in the AIDS context has become highly controversial[37] and has met with fervent opposition,[38] primarily from the gay community which fears having, in essence, a roster made of its members.[39] These fears confound some health officials who not only assert that contact tracing has been done for years,[40] but also that the gay community has been the target of some of that tracing.[41]

The current confidential status of HIV-positive individuals also places many health care workers in troubling situations. Health care providers "find themselves in the position of watching silently as unaware individuals come into contact with people the health officials know are carrying the AIDS virus."[42] "[A] nurse epidemiologist . . . has watched as doctors and nurses wheel patients into surgery, patients she knows are carrying the AIDS virus. Although her colleagues might be making contact with the patient's blood, [she] cannot warn them."[43] Most horrifying is the fact that "[a] . . . physician . . . has treated a bisex-

36. Ruggles, *On the Needs and Values of Data Banks*, 53 MINN. L. REV. 211, 220 (1968).

37. Contact tracing is "the hunt for past sexual partners of someone who has developed AIDS. The chief goal of contact tracing is to let people know they have been exposed to, and may have been infected by the virus." Reidinger, *supra* note 19, at 70.

38. "Gay men come off the wall when this idea of contact tracing is done." L.A. Times, Sept. 20, 1987, at A22, col. 2 (quoting K. Gebbie, Director of the Oregon State Health Division).

39. *See generally* R. SHILTS, *supra* note 1.

40. L.A. Times, Sept. 20, 1987, at A22, col. 2. However, "[i]n traditional contact tracing with diseases where there is a cure, the initial 'index case' can remain anonymous. With AIDS, though, health officials are not really protecting a third party unless they identify who exposed them to the virus. Otherwise, the contact might continue." *Id.*

41. *Id.* at col. 2. "It's been done for years. We have a couple of investigators whose specialty is tracing syphilis through the gay community. I have drawers full of stuff like that and nobody has ever asked to see it." *Id.* (quoting K. Gebbie, Director of the Oregon State Health Division).

42. *Id.*

43. *Id.*

ual AIDS patient who wouldn't tell his wife, as well as a male prostitute with AIDS who wouldn't cease his sexual activity."[44] Furthermore, if a doctor were to warn his colleagues of an individual's HIV-positive status, even for the protection of noninfected patients, legal liability could result.[45]

Regardless of the "confidentiality" question raised by contact tracing, the use of a computer database to maintain lists of HIV-positive individuals would lend the speed, efficiency, reduced research costs, and powerful statistical and database-matching capabilities inherent in computer technology[46] to the study and control of the AIDS epidemic. With respect to medical treatment, for example, contact tracing for syphilis currently enables Colorado to "call 49 other states and get an instantaneous response to find that individual and get him into treatment."[47] Unfortunately, this can be done "for AIDS contacts in something like only eight or ten states."[48]

Also, a database could function as an extremely efficient means of monitoring the spread of AIDS by identifying HIV-positive individuals who are irresponsibly spreading the disease. While the use of contact tracing would not, in and of itself, force seropositive individuals to act responsibly, its existence might deter[49] such conduct and illuminate irresponsible parties for treatment or punishment, as the legislature and courts deem appropriate.[50]

In conclusion, the construction of an HIV-positive/AIDS database would not be a panacea to the disease, but rather an effective way of documenting its spread, getting traced individuals tested and, if in-

---

44. *Id.*

45. *See* Wall St. J., Feb. 11, 1988, at A17, col. 2. A Florida medical technician lost his job when his doctor divulged his positive blood test status to his employers—administrators at the hospital where the technician worked—in order to protect the hospital's patients. The medical technician has since gained similar employment in San Francisco and has filed suit against his doctor for unlawful disclosure. *Id.*

46. "Largely because of the computer, scholars now are increasingly able to process the available data and base their hypotheses on mathematical models rather than on 'intuitive feeling and casual empiricism.'" A. MILLER, THE ASSAULT ON PRIVACY, COMPUTERS, DATA BANKS, AND DOSSIERS 36 (1971) [hereinafter ASSAULT] (quoting Ruggles, *On the Needs and Values of Databanks*, 53 MINN. L. REV. 211, 216 (1968)).

47. L.A. Times, Sept. 20, 1987, at A20, col. 2.

48. *Id.*

49. Issues still exist as to whether one could realistically deter an already dying individual, and as to whether that individual would be alive when his irresponsible acts are discovered. However, recall that while the sexual partner might not actually develop AIDS for over six years, that same partner can conclusively be tested for production of the HIV antibody within six months, and often as little as two weeks. *See, e.g.*, Pickett, *supra* note 9, at 1, col. 1.

50. Should the seropositive individual continue to infect other persons, this would become apparent when the newly infected individual participates in a contact trace.

fected, treated at the earliest stage possible in order to best enjoy scientific advances.

Many urge that contact tracing should not be used because it cannot effectively stop the spread of AIDS; there is no cure of AIDS and the incubation period is quite long. In addition, they insist that "the inclusion of victims' names in official reports does not significantly contribute to research, counseling, or treatment, while it does increase the chances of infringing victims' privacy interests,"[51] given the relatively short incubation period with respect to the development of AIDS antibodies, as opposed to AIDS itself.

However, as previously argued, contact tracing does produce advantages connected with early treatment of the disease and its symptoms, as well as the possibility of policing and documenting the spread of the disease via the inclusion of seropositive names in a state held database. Ultimately, the benefits to be gained from contact tracing must be weighed against the privacy interests and other constitutional rights of HIV-positive individuals.

THE PROBLEMS WITH REPORTING NAMES

Several arguments have been advanced against the reporting of the names of AIDS victims. These arguments will be outlined below.

A. REPORTING NAMES UNDULY BURDENS THOSE WHO TEST POSITIVE

This argument hinges inextricably on both the equal protection and privacy arguments discussed below. The burdens associated with reporting seropositive names include: the fear of loss of employment and insurance; the fear of difficulties in receiving medical care; the fear of physical bodily harm; and the fear of a lack of control over where such sensitive personal information flows.

Given that the medical record is "a prime source of information for decision making and control in a variety of nontreatment contexts,"[52]

---

51. Comment, *supra* note 11, at 339.

52. *Uniform Right*, *supra* note 1, at 1353. For example:

> "[T]he medical record has assumed primary importance . . . in insurance company assessments of an applicant's eligibility for health and life insurance. The medical record also plays a central role in insurance claims processing and in public and private efforts to detect medical fraud. Private employers, educational institutions, credit investigators, and law enforcement agencies also use personal medical information."

Id. at 1353-54 (citing *Privacy of Medical Records: Hearings on H.R. 2979 and H.R. 3444 Before the Subcomm. of the House Comm. on Gov't Operations*, 96th Cong., 1st Sess. 219, 579 (1980); PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 279 (1977)).

placing the information that an individual tested seropositive into a national database could have dramatic consequences.

First, both insurance companies and employers have a financial interest in knowing whether an employee or prospective employee has tested HIV-positive. "Insurance companies . . . have a strong interest in discovering the identities of potential or confirmed AIDS victims because they are loathe to cover the astronomical medical bills of such policy applicants."[53] Similarly, "[e]mployers are also interested in knowing whether present or prospective employees have AIDS in order to avoid increased group insurance premiums or possible infection of other employees."[54]

Not only could the news of testing seropositive cause the loss of employment and insurance,[55] but "[a] relatively small number of doctors say they won't treat AIDS patients. Some say they are afraid they will cut themselves during surgery and thereby become exposed to contaminated blood."[56]

As if these consequences are not sufficiently damaging, many people react violently to already vulnerable AIDS victims.[57]

> [V]iolence, which remains a fringe reaction to sufferers of acquired immune deficiency syndrome, reflects another virulent disease, one that

---

53. Comment, *supra* note 11, at 320. "[T]he typical AIDS patient needed $100,000 in medical care." R. SHILTS, *supra* note 1, at 469.

54. Comment, *supra* note 11, at 320. "When the National Gay Rights Advocates asked the nation's 1000 biggest companies whether employee medical plans covered AIDS-related expenses, one anonymous answer read: 'Just enough to defray the cost of the bullet.' " Wall St. J., Nov. 13, 1987, at 6, col. 2.

55. *See also* Wall St. J., Feb. 11, 1988, at 17, col. 1. The article includes a brief story illuminating the fear of job and insurance loss: " 'I am perfectly up front about being gay,' says a bartender, 'but I'd lose my job tomorrow if my boss knew I tested positive.' Already suffering some ARC symptoms, he says he has absorbed nearly $4,000 in medical bills rather than file a tell-tale insurance claim." *Id.*

56. Wall St. J., Nov. 13, 1987, at 6, col. 2. However, "Arthur Caplan, a director of the center for biomedical ethics at the University of Minnesota in Minneapolis, believes that doctors and nurses who refuse AIDS patients do so out of disapproval. 'They know how to deal with violent patients and infectious diseases like hepatitis. . . . It's more than fear. They're making a value . . . judgment about AIDS victims. They're saying they won't treat people [they find] disgusting.' " *Id.* at col. 3. Furthermore, "[t]he handful of health-care workers who appear to have become infected in the course of their work were splashed either in the mouth or in a cut with the blood of infected patients. A researcher who became infected was working with an extremely high concentration of the virus and had abrasions on his hand. In all such cases, the possibility of sexual or drug-related transmission can't be absolutely ruled out, either. When sex and drugs are involved, people don't always tell the truth." *Id.* at col. 1.

57. *Id.* at 1, col. 1. "Gay-rights groups note that physical attacks against homosexuals have risen sharply since the disease that came to be called AIDS was first publicized in 1981. The National Gay and Lesbian Task Force says it studies suggest that 63% of such assaults now are related in some way to the emotions AIDS raises." *Id.*

> may threaten America's moral fabric: hatred and fear. Practically every day, the news brings word of yet another senseless response to AIDS—from the Florida minister who bars from church three hemophiliac children carrying the virus, to the Texas man who shoots his nephew to death in the belief he has AIDS.[58]

For those who manage to escape the overwhelming consequences of insurance loss, job loss, lack of medical care, or violence, there is little chance of escaping the stigma which tends to attach to AIDS victims:

> Being a poor person is unfortunate, being a leper is unclean. It is bad to be sick. And our society makes value judgments about people on the basis of the state of their health that it does not make on the state of their finances .... A person will be more hurt by words getting about that he has an illness than that he has no money.[59]

Computer technology, to a certain degree, tends to validate these fears[60] because of the ease of access to the computer's stored information, in combination with the computer's "insatiable appetite for information, [an] image of infallibility, and [an] inability to forget anything that's stored in it. . . ."[61] The crux of the fears concerning large federal data bases is that "[t]he technology for information collection, storage, and retrieval has outpaced the technology for safeguarding databanks of personal information."[62] These fears are well-founded; "stories are legion about the fifteen-year-old computer wizard who can crack the most secure computer system. Computer security is largely unregulated, and the penalties for stealing personal data are unclear."[63]

Even when theft or wrongdoing associated with data files is negligible, problems relating to the data input and use of data can still arise. For example, "[n]ames in medical records have been confused, illnesses have been ascribed to the wrong person, and unsolicited and misleading comments by doctors about a patient's sexual health have been in-

---

58. *Id.*

59. *Uniform Right*, *supra* note 1, at 1357 (quoting the transcript of *President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research* at 436 (testimony of Dr. Robert Gorden, M.D., M.H.S., Special Ass't to the Dir., National Institutes of Health, Bethesda, Md.)).

60. "Despite . . . freedom-generating prospects, the scientific advances in data accumulation remain a double-edged sword. If the new technology is properly used, society benefits; if it is abused, it can become a tool of enslavement by those who control data flow." Peck, *Extending the Constitutional Right to Privacy in the New Technological Age*, 12 HOFSTRA L. REV. 893, 897 (1984).

61. ASSAULT, *supra* note 46, at 17.

62. Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991, 993-94 (citing SUBCOMM. ON TRANSPORTATION, AVIATION, AND MATERIALS OF THE HOUSE COMM. ON SCIENCE AND TECHNOLOGY, 98TH CONG., 2D SESS., COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY 17-19, 24-27 (Comm. Print 1984)).

63. *Id.*

cluded."[64] Also, the results of information taken out of context, as is apt to happen with computer data, can be devastating.[65]

The above computer-related fears are all based on problems generated by human error or deception and the abuse of computer technology, rather than on problems that are intrinsic to computer use.[66] Arguably, appropriate safeguards could be developed to avoid many of the undesirable results. For instance, with respect to fears of inaccurate data entry, informational privacy could be effectively protected by

---

64. *Uniform Right*, *supra* note 1, at 1362-63 (citations omitted). False conclusions caused by inaccuracy of files is a noteworthy risk:

> According to a study initiated by the United States Office of Technology Assessment, only twelve percent of the criminal history record summaries routinely transmitted from North Carolina to law enforcement and other agencies were correct. The figures for California were slightly better, but still not encouraging: nineteen percent. . . . Under these conditions, computer matching inevitably leads to a proliferation of false information. Both the error and the implications for the persons concerned are magnified.

Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 719 (citing D. BURNHAM, THE RISE OF THE COMPUTER STATE 74 (1983); Bing, *Data Protection and Social Policy*, in BEYOND 1984: THE LAW AND INFORMATION TECHNOLOGY IN TOMORROW'S SOCIETY 82, 89 (Council of Europe 1985) (proceedings of the 14th Colloquy on European Law, Lisbon, Sept. 26-28, 1984); Shattuck, *supra* note 62, at 1001-04)).

65. An important

> consequence of automated processing is the loss of context. The very moment matching begins, the data are itemized and disconnected from their original collection situation. Yet neither hard facts nor judgments can be separated at will from their context without distorting information. Consequently, every step towards routine processing accentuates the danger of misrepresentations and false conclusions. The more complex a case, the greater the danger of an improper result.

Simitis, *supra* note 64, at 718.

In New York, a middle-aged man was denied a taxi-driver's license when a computerized credit report showed that at thirteen he had been placed in a Massachusetts mental institution. "What the files did not show was that he was an orphan and the institution was the only home the state authorities could find for him for a period of four years." Shattuck, *supra* note 62, at 994 (citing A. NEIER, DOSSIER 73-74 (1975)).

In general,

> [c]omputer systems that handle personal information may inflict harm to data subject in two significant ways: (1) by disseminating evidence of present or past actions or associations to a wider audience than the individual anticipated when he originally surrendered the information (deprivation of control over access), and (2) by introducing factual or contextual inaccuracies in the data that create an erroneous impression of the subject's actual conduct or achievements in the minds of those to whom the information is exposed (deprivation of control over accuracy).

ASSAULT, *supra* note 46, at 41 (citing Karst, *The Files: Legal Controls Over the Accuracy of Stored Personal Data*, 31 LAW & CONTEMP. PROBS. 342, 343 (1966)).

66. Humans program and control computers. That is "the reality of our electronic way of life rather than the popular image projected by Hal, the neurotic but domineering computer in 2001: A Space Odyssey." ASSAULT, *supra* note 46, at 17 (1971). Similarly, "machines are morally neutral, and it is only the men who, therefore, bear the responsibility for distinguishing between right and wrong." *Id.* at 37.

screening data before it is recorded.[67] Such data screening is especially important given the frequent assertion by computer experts that "total reliance on post-collection procedures may be too little, too late."[68] In the event that a discrepancy arises with respect to a medical file's contents, it is crucial that the AIDS system act promptly to resolve the dispute. The databank manager should identify and contact likely sources of the disputed information and flag the information as questionable. After reinvestigation, the manager should then re-record the current status of that data. Investigations should be initiated and completed within a reasonable period of time. Unverifiable or inaccurate data should be promptly deleted and formal, sealed notices should be sent to all recipients of the incorrect data. Where the information is verified but incomplete, additional information should be included to clarify the item, such as the fact of a recovery or an improvement in medical condition.[69]

With respect to protecting an AIDS database from improper access, the solution to combatting human abuse will likely be more illusive. Generally,

> [t]he choice of an appropriate protective scheme depends upon the character of the particular system's hardware and software, how much storage and transmission security its data base is likely to need, and the nature of both the user class and those who are likely to attempt to gain access to the information without authorization . . . . In addition, since systems change their purposes and dimensions over time, it is often impossible to predict the character of future security problems at the initial stages of development.[70]

---

67. See *Uniform Right*, *supra* note 1, at 1355-56.

> These [databank] companies process a great number of requests for patient medical information. When information is obtained from industry data exchanges rather than from the patient, the risk of a mishap multiplies. Each collection, report, and coding is a source of potential error. The Medical Information Bureau (MIB), for example, does not verify its data with the original source of the information. As a result, unless detected earlier, any incorrect data that MIB provides can circulate throughout the entire insurance industry for as many as seven years. *Id.*
>
> Like many other information banks, the MIB does not directly verify any patient information sent to it. The accuracy of the programmed information depends, therefore, on the verification of the member reporting companies. The source data is obtained from 'consumer reports.' Unless challenged by the medical consumer these reports are not confirmed by either the insurance applicant himself or by the medical facility that originally released the information.

Id. at 1356 n.46 (citing Boyer, *Computerized Medical Records and the Right to Privacy: The Emerging Federal Response*, 25 BUFFALO L. REV. 37 (1975); Young, *Your Health, Their Business*, NEW YORK, Oct. 27, 1980, at 39, 44)).

68. ASSAULT, *supra* note 46, at 264.

69. *See Uniform Right*, *supra* note 1, at 1356 n.47 (citing FTC News Release, Federal Trade Commission (Nov. 17, 1982)).

70. ASSAULT, *supra* note 46, at 256. For instance, "In the case of remote-access sys-

Regardless of the protective schemes employed, "experts have flatly asserted that most program languages are easy to decipher, that digital transmission of data 'does not provide any more privacy than . . . Morse Code,' and that 'modest resources suffice to launch a low-level infiltration effort."[71] Hence,

> [t]he reality of the situation seems to be that once personal information has been entered into a computerized file, the data subject, and, to a lesser degree, the system's operators have little capacity to control who will be able to peruse it . . . . In a typical remote-access time-sharing system, there are at least six points through which improper access to the data may be gained or at which distortion of the information may occur.[72]

Thus, the burden of protecting the privacy interests of documented AIDS carriers may be better accomplised by stringent regulation and careful labor practices than through use of mechanical protective devices.[73] As one scholar has stated:

> No set of technological devices or security procedures, however extensive or carefully designed they may be, can assure the integrity or privacy of the content of an information system. A computer's data store essentially is a file, and whatever has been placed in it can be extracted or altered by someone who knows the appropriate pathway to follow.[74]

---

tems carrying sensitive personal information, a high level of protection against wiretapping can be achieved by coding the data or using 'scramblers' to garble them before transmission and installing complementary devices in the authorized terminals to reconstitute the signal." *Id.* at 256-57. Similarly, "In the long run, the most promising method of accurate user identification may be automatic scanning of fingerprints or voiceprints, but these procedures are not yet available." *Id.* at 259. Such devices should be incorporated into the original hardware and software system design for optimum efficiency. *Id.* at 259 (citing *House Hearings on the Computer and Invasion of Privacy* 126 (statement of Paul Baran)). "One pragmatic consideration is that the cost of scrambling devices and the development of completely break-proof codes is quite high." *Id.* at 257.

71. *Id.* at 42 (citing Allen, *Danger Ahead! Safeguarding Your Computer*, HARV. BUS. REV., Nov.-Dec. 1968, at 97, 100 (quoting Petersen & Turn, *System Implications of Information Policy*, 30 AFIPS CONF. PROC. 291, 298 (1967))).

72. *Id.* at 42 (citing Ware, *Security and Privacy in Computer Systems*, 30 AFIPS CONF. PROC. 279 (1967)). For instance, as if straight from James Bond, "[T]here is some evidence that computer equipment radiates when in operation and that by using eavesdropping techniques the emanations can be captured, reconstituted in their original machine-readable format, and then deciphered. To guard against this possibility, the physical surroundings . . . can be shielded with protective materials . . . ." *Id.* at 256.

73. ASSAULT, *supra* note 46, at 263.

74. *Id.* at 263 (citing *House Hearings on the Computer and Invasion of Privacy* 126 (statement of Paul Baran)).

> Occasionally, medical record disclosures are authorized neither by the patient nor by statute. In 1975, the Denver District Attorney and a grand jury discovered that a private investigative reporting service had been engaging in a nationwide medical information theft ring involving medical information reports on almost 2000 unsuspecting citizens. The firm boasted a 99% success rate in acquiring unconsented-to disclosure of medical information. Purchasers of this information

With respect to labor concerns:

> [e]ffective technical and procedural safeguards, combined with input-output controls, although vital prerequisites to maintaining the security and factual reliability of computerized information, are not sufficient by themselves. Even the most sophisticated set of mechanical and administrative regulations can be undermined by people working within the system and by outsiders who gain access illicitly. In the long run, those who live on intimate terms with databases and the technology may prove to be an even more dangerous group than malicious or profit-seeking interlopers, despite their lack of personal interest in the informational content of the material in their care. Thus, it would be sheer folly to treat the technicians who design and operate computer systems as a brahmin caste whose very act or decision is presumed socially desirable and beyond review.[75]

In summary,

> [p]rivacy-oriented technical safeguards must be supported by workable regulations designed to prevent people from bypassing the security devices. These procedural rules must be comprehensible to everyone who might gain access to the data, cover every aspect of the system's data-handling activities that bears on information security, and be reinforced by realistic penalties for noncompliance.[76]

"Careful hiring practices and the proper philosophical direction during the training period can be extremely valuable in developing a cadre of systems personnel who are sensitive to privacy considerations."[77] Again, this points to stringent regulation and enforcement, and necessitates a cursory discussion of some current state managed/utilized databases and their regulation.

Current state databases offer virtually no protection to individual privacy interests primarily because "the technological capability to collect, maintain, cross-index, and disclose vast quantities of information about private lives has far outpaced the legal protection of privacy in the United States."[78] Modern computer "technology permits the collection and dissemination of personal information with ease. The computerization of society has important and possibly unsettling implications for personal privacy that invite a reexamination of the

---

included more than 100 of the most prominent insurance companies in the nation.

Uniform Right, *supra* note 1, at 1357 n.52 (citing *Privacy of Medical Records: Hearings on H.R. 2979 and H.R. 3444 Before the Subcomm. of the House Comm. on Gov't Operations*, 96th Cong., 1st Sess. 1063-66 (1980) (statements of Dale Tooley, Denver District Attorney)).

75. ASSAULT, *supra* note 46, at 268.

76. *Id.* at 260 (citing Peters, *Security Considerations in a Multi-Programmed Computer System*, 30 AFIPS CONF. PROC. 283, 283-84 (1967)).

77. *Id.*

78. Shattuck, *supra* note 62, at 993.

still-emerging constitutional right to privacy."[79]

In the midst of the right to privacy's infancy, an immense number of state-oriented databases have emerged and are already in use.[80] An example of a giant federal data bank is the National Crime Information Center (NCIC), which is used both for dissemination of information concerning the noncriminal activities of persons under surveillance by the Secret Service and for computer-matching investigations by the federal government to detect fraud, abuse, and waste in the administration of federal programs.[81] It has been noted that

> [t]here are many types of public records, and many of them are open to anyone who wishes to consult them. If one buys real estate, it must be registered. City directories list the names of individuals and businesses. Phone books provide people's names, addresses and phone numbers. The individual wishing to obtain a driver's license must provide identification information, sometimes even fingerprints and photographs. If he receives income, he must make out an income tax return. His employers must report information about him to social security.
>
> In addition, various government organizations keep their own records. The police maintains files on individuals with whom they come in contact. The FBI may investigate any individual for security clearances or suspected criminal activities. The army maintains records on all who pass through it. Schools keep records on all students. Employers maintain files on employees, and credit agencies built up credit information on individuals and businesses.[82]

It is important to emphasize that, thus far, computerization has been used by the federal government to achieve positive ends. "[I]nformation systems containing sensitive data are being constructed to facilitate important social objectives, such as better law enforcement, faster delivery of public services, more efficient management of credit and insurance programs, improvement of telecommunications, and streamlining of financial activities."[83] Some claim, however, that "these high technology systems are also being used at an increasing rate by large public and private agencies to enhance their control of individu-

---

79. Peck, *supra* note 60, at 893-94.

80. As Justice Douglas noted:

> The ability of the government and private agencies to gather, retain, and catalogue information on anyone for their unfettered use raises problems concerning the privacy and dignity of individuals. Public and private agencies are storing more and more data. "If your name is not in the records of at least one credit bureau, it doesn't mean that you don't rate. What it does mean is that you are either under twenty-one or dead.

Tarver v. Smith, 402 U.S. 1000, 1000 (1971) (Douglas, J., dissenting) (quoting H. BLACK, BUY NOW, PAY LATER 37 (1961)).

81. Shattuck, *supra* note 62, at 992.

82. Ruggles, *supra* note 36, at 212.

83. Shattuck, *supra* note 62, at 993.

als,"[84] and that "groups are seeing their privacy eroded by the increasing requirements of a growing bureaucracy."[85]

In sum, a modern society requires vast amounts of information to function. Generally, individuals provide information because they recognize it is essential to allow society to operate safely (as in motor vehicle license information), efficiently (as in income tax information), and effectively (as in social security information). As Arthur R. Miller once stated:

> I do not oppose data centers. I am overwhelmed by their capabilities; I am concerned about their proliferation; but I think it is absolutely ludicrous and unrealistic to advocate the elimination of a modern technology that can carry out important governmental and nongovernmental operations simply because that technology might be abused.[86]

Pursuant to this view, what is necessary is not the destruction or prevention of federal databases but rather stringent regulatory control governing data entry and use.

Medical databases, such as the AIDS database at issue here, are particularly sensitive and require strict governmental regulation, especially in light of the AIDS hysteria and frequent acts of injustice and violence towards AIDS victims. Unfortunately, "[t]hese advanced systems of recordkeeping are so new to the health care field that the legal system has not provided health care consumers with privacy protection, access, and accuracy rights . . . ."[87] Such a lack of protection to the medical consumer is especially grievous given that "the number of persons outside the doctor-patient relationship with access to a patient's records is reportedly 'staggering' and expected to grow."[88]

A variety of factors contribute to the increase in the number of people who gain access to medical records outside of the traditional "doctor-patient" relationship:

> Medical records now frequently include intimate details about a patient's habits or social life, such as patterns of alcohol and drug use, sexual proclivities, and family relationships . . . . The rise of disease control data for research and the requirements of government-subsidized medical care have expanded both the role and the content of medical records. As a result of these changes, the responsibility for protecting and managing personal medical information has become diffused. A patient's medical information may be scattered or stored beyond the physical, administrative, and ethical control of the health care

84. *Id.*

85. Ruggles, *supra* note 36, at 213.

86. Miller, *On Proposals and Requirements for Solutions*, 53 MINN. L. REV. 224, 227 (1968).

87. *Uniform Right*, *supra* note 1, at 1356.

88. *Id.* at 1350 (quoting PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 277, 290 (1977)).

provider who initially created the record.[89]

Thus,

> it is inevitable that personal and medical information about potential and confirmed AIDS carriers and victims would be exposed to many outside the doctor-patient relationship. Physicians must collect such information in order to render adequate professional services to their patients. Employees of state and federal public health organizations must receive all available AIDS-related information in order to conduct the scientific battle to contain and find a cure for the disease. Red Cross and blood-bank employees discover AIDS cases in the course of monitoring the nation's blood supply. Private organizations offering legal or medical advice to AIDS carriers or establishing AIDS victim support groups are also privy to personally identifiable AIDS-related information. This widespread collection and possession of information poses the danger that it will be improperly disclosed to unauthorized third parties.[90]

"Even in states that regulate disclosure to insurers, employers, and other private parties, the problem of unconsented-to *re*disclosure by these parties to still others, is usually not addressed by statute."[91] Once again, these facts point to the crucial role played by regulation of data entry and use.

2. HOW TO REGULATE

The quest should be to develop a rational pattern of regulation to ensure that maximum social utility is derived from computers at a minimum social cost in terms of injury to individual privacy.[92] This is especially important in light of the fact that "[r]ecorded information always is vulnerable to human and mechanical foibles; therefore, the most crucial regulations for assuring a high level of data security are those dealing with the information that may be gathered, the ways in which it is manipulated, and the identity of the people to whom the data may be disclosed."[93]

Four elements have been identified as essential to efficient processing regulation:[94]

> First, the unique nature of the personal data processing must be recognized. Second, requests for personal information must specify the pur-

89. *Id.* at 1352, 1353 (citing *Privacy of Medical Records: Hearings on H.R. 2979 and H.R. 3444 Before the Subcomm. of the House Comm. on Gov't Operations*, 96th Cong., 1st Sess. 211, 479-82 (1980); PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 282, 283, 290-91 (1977)).

90. Comment, *supra* note 11, at 320.

91. *Uniform Right*, *supra* note 1, at 1361 (citation omitted).

92. *See* Miller, *supra* note 86, at 227.

93. ASSAULT, *supra* note 46, at 263.

94. Simitis, *supra* note 64, at 737.

> pose for which the data will be used, thereby excluding all attempts at multifunctional processing. Third, data protection regulations must be reviewed and updated constantly to reflect changes in technology. Finally, there must be an independent authority to enforce data regulations.[95]

The first step towards development of a rational pattern of regulation is to impress upon both governmental and private agencies that the collection and retrieval of personal data is an exceptional means of obtaining information, and not the norm. Technocratic concerns, such as viewing the computer as the ultimate convenience, should not be the controlling factor. Priorities on information use are to be clearly set, so that the burden is on the user to show his need.[96] Additional protective measures are also in order:

> Hardware and software should, like motor vehicles or medicine, meet certain safety requirements before being put on the market. They should have a minimum of built-in protective devices. This requirement is by no means a utopian expectation. Smart cards and videotext can, at least for payment purposes, be designed in a way that demands almost no collection of personal data.[97]

B. CONSTITUTIONAL QUESTIONS

Even if we assume that such regulation will be developed, implemented, and operated with the utmost success, the reporting of HIV-positive names and the ensuing creation of a state medical/AIDS focused database may violate certain constitutional guarantees.

The two primary constitutional concerns relating to the creation of an AIDS database are equal protection and privacy. For the purpose of this discussion, it will be assumed that the three tests used to identify HIV-infected blood yield accurate results.[98]

1. *The Reporting of Names of Those Who Test Seropositive May Violate the Equal Protection[99] Guarantees of the United States Constitution*

Discriminatory treatment will generally not violate the equal pro-

---

95. *Id.* at 737-38.

96. *Id.* at 738-39.

97. *Id.* at 739-40.

98. *See supra* note 9 and accompanying text.

99. U.S. CONST. amend. XIV, § 1. *See, e.g., Reportability, supra* note 7, at 1103. The Fourteenth Amendment Equal Protection Clause limits actions only by state, not federal government. "The Fourteenth Amendment provides that "[n]o State shall make or enforce any law which shall . . . deny to any person within its jurisdiction the equal protection of the laws." *Id.* at 1115 (quoting U.S. CONST. amend. XIV, § 1). While there is no analogous provision applying to the federal government, the Fifth Amendment Due

tection clause if the statutory classification meets the applicable relevancy test. The modern view of relevancy

> is more sophisticated than that used in the cases . . . dealing with tuberculosis and venereal disease. The decisions rendered thirty years ago simply do not reflect the contemporary notions of constitutional protections. Some recent commentators have indicated that the courts today are likely to apply strict scrutiny to any mandatory public health measure. Such an analysis requires the state to prove a compelling state interest justifying the public health measure, and then to prove that the particular regulation in question is the least restrictive alternative to accomplish the desired end.[100]

In order to apply strict scrutiny to statutes which require the reporting of names of those who test seropositive, gays, hemophiliacs, and drug users would have to be deemed a suspect class, a classification usually reserved for racial groups.[101] The author believes, as do other authorities, that "it is unlikely . . . that the Supreme Court would consider gays, hemophiliacs, or intravenous drug users (members of the groups considered to be a high risk for contracting AIDS) to be members of a suspect classification."[102]

With respect to the reporting of seropositive individuals, the law is neutral on its face, although a disproportionate number of gays, hemophiliacs, and intravenous drug users represent the segments of the population most likely to test positive.[103] In *Washington v. Davis*,[104]

Process Clause may apply. However, a Fifth Amendment Due Process Clause analysis is beyond the scope of this Note.

100. Gray, *The Parameters of Mandatory Public Health Measures and the AIDS Epidemic*, 20 SUFFOLK U.L. REV. 505, 516-17 [hereinafter *Parameters*] (citing Note, *The Constitutional Rights of AIDS Carriers*, 99 HARV. L. REV. 1274, 1282-84 (1986)).

101. Religion has not even been treated as a suspect class. *See* L. TRIBE, AMERICAN CONSTITUTIONAL LAW §§ 16-13, at 1465 (2d ed. 1988). *See also* United Jewish Organizations of Williamsburgh, Inc. v. Carey, 430 U.S. 144 (1977) (where, to effect the delineation of voting districts, strict scrutiny was applied to nonwhites (blacks and Puerto Ricans), but was not considered, even in dicta, in relation to the Hasidic community, a religious minority).

102. *Parameters*, *supra* note 100, at 517. *See also* Bowers V. Hardwick, 478 U.S. 186 (1986) (denying that the right to engage in homosexual sodomy is fundamental).

103. According to the American Red Cross:

> About 98 percent of all AIDS cases reported to date have occurred in the following groups:
> — Sexually active homosexuals and bisexual men (or men who have had sex with another man since 1977) (65 percent)
> — Present or past users of illegal intravenous (IV) drugs (17 percent)
> — Homosexual and bisexual men who are also IV drug abusers (8 percent)
> — Persons who have had transfusions of blood or blood products (2 percent)
> — Persons with hemophilia or other blood clotting disorders who have received blood clotting factors (1 percent)
> — Heterosexual men and women (these include sex partners of persons with AIDS or at risk for AIDS, and people born in countries where heterosexual transmission is thought to be more common than in the United States (4 percent)

two black applicants challenged a Police Department's recruiting process, and more particularly, a written test given to all prospective Government employees because it excluded a disproportionately high number of black candidates. The Court held that the test was valid because the ends it was created to achieve were rationally related to a constitutionally permissible state interest.

Similarly, given that a disproportionate number of gays, hemophiliacs, and intravenous drug users will be affected by any statute that requires the reporting of the names of seropositive individuals, the test to determine whether the statute violates the Equal Protection Clause is whether the reporting of seropositive names is rationally related to a legitimate state interest. First, the legitimate state interest is the preservation of public health. As was previously discussed, recording of names into a state database would enable contact tracing of those who test seropositive, an event that has a relatively short incubation period. This would allow many victims, otherwise unaware of their infected status, to receive treatment early, thereby hindering the progression of the disease. While

> [t]here are few absolutes or universal truths to be gleaned from the available precedent in the area of mandatory public health measures, [it] appears beyond cavil that the state, in the exercise of its innate police power, has the authority to impose reasonable compulsory requirements to protect the general public from an epidemic. When the courts are called upon to consider the validity of compulsory public health measures directed at the AIDS epidemic, the inquiry—regardless of the level of scrutiny—will be whether the courts can conclude that the measure is reasonable.[105]

Thus, courts must ultimately ask whether reporting seropositive names is a reasonable measure related to the control of AIDS.

> In determining "reasonableness," courts generally balance the injury inflicted against the benefits obtained. The ability to articulate a noble objective, such as the preservation of public health, is, of course, insufficient. The proffered measure must, as a matter of reasonable medical certainty, afford protection to the public health.[106]

"A measure that is designed to merely curtail the unsupported fear of the community will probably not be seen as a sufficiently compelling

— Infants born to mothers infected with the AIDS virus (1 percent). AMERICAN RED CROSS, AIDS, SEX, AND YOU (Oct. 1986 Brochure).

104. 426 U.S. 229 (1976).

105. *Parameters*, *supra* note 100, at 518.

106. *Id.* at 518. "In considering forced testing, quarantine, or similar measures, the appropriate test would be to weigh the degree of intrusion on personal liberties against the degree of protection that the measure can actually give to the general populace." *Id.* at 517 (citing Note, *The Constitutional Rights of AIDS Carriers*, 99 HARV. L. REV. 1274, 1282-84 (1986)).

objective."[107] However, as previously discussed, there are very real benefits to the early diagnosis of seropositive individuals. To briefly reiterate the main benefits: (1) AZT has been shown to dramatically slow the progression of AIDS (i.e., the onset of ARC, or other advanced diseases in the HIV positive individual); (2) the blood plasma from recently infected HIV positive individuals is rich in antibodies valuable to those in the more advanced stages of AIDS, and it is theorized that perhaps something in this plasma can "teach" the sicker patient's immune system to defend itself; (3) moreover, the newly infected HIV positive individual can be educated in hygene and safe sex, to prolong his own existence and avoid infecting loved ones.

In response to the above, it is argued that the ELISA test is inaccurate and likely to be both under- and over-inclusive so that there is no reasonable medical certainty that the public health would be afforded greater protection by its widespread implementation. The author disagrees. First, the ELISA inaccuracies can be checked against two other more accurate tests.[108] Second, a statute can be under-inclusive and still pass the muster of equal protection.[109] Also, given the geometric progression of the disease, it is vital to track the sexually active person in order to prevent harm to many others.

The over-inclusive nature of the ELISA test presents a tougher problem; the other two antibody tests do not correct for this flaw. As a result, the burden falls upon uninfected individuals who test positive. Ultimately, their privacy must be sacrificied in order to achieve the greater good. Despite this dilemma, the author believes that the possibility of tracking individuals who test positive and encouraging responsible behavior on their part, outweighs any burden placed upon uninfected persons who incorrectly test positive.

2. *The Reporting of Seropositive Names May Violate the Privacy Guarantees of the United States Constitution, Especially in Light of the High Costs of Information Abuse*[110]

First, it is important to understand the modern concept of a "right to privacy." Professor Kurland has identified three rights within the concept of privacy: "freedom from intrusion or observation in one's pri-

---

107. *Id.* at 518-19 (citing City of Cleburne v. Cleburne Living Center, 473 U.S. 432, 448 (1985) (unsubstantiated negative attitudes or fears are not permissible bases for treating home for mentally retarded differently from other multiple dwellings in zoning proceeding)).

108. *See supra* note 9 and accompanying text.

109. *See, e.g.*, Williamson v. Lee Optical Co., 348 U.S. 483 (1955).

110. *See, e.g.*, Closen, Connoy, Kaufman & Woscik, *AIDS: Testing Democracy—Irrational Responses to the Public Health Crises and the Need for Privacy in Serologic Testing*, 19 J. MARSHALL L. REV. 835 (1986).

vate affairs; the right to maintain control over certain personal information; and the freedom to act without outside interference."[111] An AIDS database would arguably infringe on all three facets of privacy, as sexual habits would be exposed, recorded in the databank, and tracked to see if the AIDS carrier is acting responsibly. Similarly, "Dean Prosser, who took up the Warren-Brandeis cause of establishing privacy as a tort, gave it a four-part definition: (1) intrusion into solitude or personal affairs; (2) public disclosure of embarrassing facts; (3) publicity that puts one in a false light; or (4) appropriation by another of one's name or likeness."[112] With respect to Prosser's definition, elements one and two of privacy are potentially infringed by the creation of a database.

Whether the courts protect the right to privacy in the computer technology context is uncertain.

> In 1977, the Supreme Court, in *Whalen v. Roe*,[113] demonstrated great sensitivity to the privacy needs of an information-based society in upholding a statute that required that centralized computer records be maintained on all persons who purchased certain lawfully prescribed drugs for which there also was an illicit market. The statute at issue required that a system be established to protect the records against disclosure, and that data be destroyed after five years. In addition, public disclosure of a patient's identity was expressly prohibited. The Court found that the security precautions required by the statute sufficiently protected information against disclosure and thus did not violate the constitutional right to privacy.[114]

The *Whalen* Court stated:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized databanks . . . . The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed.[115]

Unfortunately, legal precedent is hazy in this area and technology makes us continually redetermine the boundaries of privacy.

---

111. Peck, *supra* note 60, 899-900 (citing Kurland, *The Private I*, U. CHI. MAG., Autumn 1976, at 7, 8). "Invasion of privacy as a separate and distinct tort only emerged at the end of the nineteenth century." Epstein, *Privacy, Property Rights, and Misrepresentations*, 12 GA. L. REV. 455, 463 (1978) [hereinafter *Misrepresentations*].

112. Peck, *supra* note 60, at 900 n.36 (citing Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960)).

113. 429 U.S. 589 (1977).

114. Peck, *supra* note 60, at 907-08.

115. *Whalen*, 429 U.S. at 605 (citation omitted).

> The constitutional problem concerning the protection of privacy is the difficulty of applying the principles of an eighteenth-century document, the Bill of Rights, to late twentieth-century life. The fourth amendment to the Constitution was adopted to protect 'persons, houses, papers and effects' against unreasonable search and seizure by the government. Massive collection and dissemination of sensitive personal information by private entities was unimagined at that time because personal information was difficult to collect and files were handwritten, rarely reproduced, and easily lost.[116]

In contrast, "[t]oday, the capacity to collect and preserve information has been radically altered by the relentless growth of an information technology that permits virtually unlimited permanent storage and retrieval of personal information."[117] Furthermore,

>] [m]ost personal information is now maintained outside the home and therefore generally falls outside fourth amendment protection. Individuals have almost no dominion over such information. They cannot prevent if from being collected; they often have no access to it and thus cannot challenge its accuracy; and they cannot prevent its dissemination. As a result, what once was gossip today may become part of the permanent record.[118]

Many view privacy as a vital ingredient for creative achievement and civic experimentation,[119] while others consider privacy to be central to human dignity and existence.[120] Privacy has also been likened to the

---

116. Shattuck, *supra* note 62, at 995 (citing J. SHATTUCK, RIGHTS OF PRIVACY 4-5 (1977)).

117. *Id.*

118. *Id.* (citing *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs: Hearings before the Subcomm. on Oversight of Gov't Mgmt. of the Senate Comm. on Governmental Affairs*, 97th Cong., 2d Sess. 1551-56 (1982) (testimony of Ronald Plesser)).

119. Peck, *supra* note 60, at 898.

> The chilling effect of a loss of privacy is the undesirable incentive to conform to perceived societal norms rather than assert one's individuality in ways that may threaten to cause a loss in personal or professional associations. Ultimately, what will be lost by this process are the private emotional releases that we all need, the range of human relationships that help us function, and, perhaps most importantly, the creativity that serves human achievement.

Id. at 898-99.

120. *Id.* at 898.

> The right to privacy is more than just a vague concept. To disparage this right is to disparage the personal autonomy that has flourished as a result of this nation's dedication to individual rights and the related concept of human dignity. While some have asserted that people have nothing to fear unless they have something to hide, protection against unwarranted intrusions into personal matters means much more than safety from minor embarrassments, or even possible incrimination. Invasions of privacy have the potential to reveal one's associations, private enjoyments, or personal views, all of which others might look upon with a disdain leading to social ostracism.

Id.

right one has in the autonomy of his person and creations[121] and has been touted as the primary prerequisite to true liberty.[122]

a. Privacy and Economic Theory:

Economic theory has been construed to limit the right to privacy despite its aforementioned attributes. Economists have shown that, in certain instances, the enforcement of one's right to privacy lends legal ability to an individual to misrepresent himself.[123]

As noted by one psychologist: "the wish for privacy expresses a desire . . . to control others' perceptions and beliefs vis-à-vis the self-concealing person."[124] "Even the strongest defenders of privacy describe the individual's right to privacy as the right to 'control information about him.' "[125]

However, the "seldom-remarked corollary to a right to misrepresent one's character is that others have a legitimate interest in unmasking the deception."[126] Specifically, with regard to this analysis, prospective employers, insurers, doctors, and lovers have a legitimate interest in knowing that an individual has AIDS. To some, this corollary suggests that personal disclosure has value and, therefore, the owner of the information should be able to bargain for the sale of this information.[127] However, whether such a solution is feasible depends

---

121. *See, e.g.*, Simitis, *supra* note 64.

> [T]he protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts . . . is merely an instance of the enforcement of the more general rights of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed.

Id. at 730-31 (quoting Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890)).

122. "La liberté du people est dans sav vie privée; ne la troublez point. Que le gouvernement . . . ne soit une force que pour protéger cet état de simplicité contre la force même." *Id.* at 730 (quoting de Saint-Just, *Fragments sur les institutions républicaines*, in 2 OEUVRES COMPLÈTES 492, 507 (C. Vellay ed. 1908) ("The liberty of the people lies in their private lives; do not disturb it. Let the government . . . be a force only to protect this state of simplicity against force itself . . . .")).

123. "Psychologists and sociologists have pointed out that even in everyday life people try to manipulate by misrepresentation other peoples' opinion of them." Posner, *The Right to Privacy*, 12 GA. L. REV. 393, 395 (1978) [hereinafter *Right of Privacy*] (*citing* E. GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 58 (1959)).

124. *Id.* (quoting Jourard, *Some Psychological Aspects of Privacy*, 31 LAW & CONTEMP. PROBS. 307, 307 (1966)).

125. *Id.* at 395 (quoting Stone, *The Scope of the Fourth Amendment: Privacy and the Police Use of Spies, Secret Agents, and Informers*, 1976 AM. B. FOUND. RES. J. 1193, 1207).

126. *Id.*

127. *Id.* at 397.

> That disclosure of personal information is resisted by, *i.e.*, is costly, to the person to whom the information pertains yet is valuable to others may seem to argue for

upon: "(1) the nature and provenance of the information and (2) transaction costs."[128]

Arguably, it is not appropriate for an AIDS carrier to be allowed to conceal his condition from insurance companies because without this information the insurance company cannot conduct proper actuarial calculations or assess accurate and profitable premiums. In response, some argue that it is better to spread the cost of AIDS care throughout society rather than to deprive the AIDS victim of insurance because of exorbitant premiums or outright refusal. If the general populace desires the costs to be so spread, a government run or subsidized insurance program should be founded, rather than to fortuitously place the burden of AIDS-related costs upon individual insurers.

Thus, a line drawing problem arises with regard to when maintaining secrecy about one's AIDS status becomes an act of fraud upon the individual's financial/sexual/medical partner(s).

> One consideration relevant to deciding whether a transacting party has crossed the line is whether the information he seeks to conceal is a product of significant investment. If not, the social costs of disclosure, which . . . arise from the effect of disclosure in dampening the incentive to invest in information gathering, will be low. This consideration may be decisive on the question, for example, whether the law should require the owner of a house to disclose latent, *i.e.*, nonobvious, defects to a purchaser. The ownership and maintenance of a house are, of course, productive activities in which it is costly to engage. But the owner acquires knowledge of the defects of his house costlessly or nearly so; hence forcing him to disclose those defects will not reduce his incentive to invest in discovering them.[129]

Thus, if the HIV positive individual gains this information through the regular course of his healthcare, then forcing him to disclose his disease should not reduce his incentive to be tested for AIDS. This brings us to an argument frequently made by advocates against reporting: If the names of seropositive individuals are reported, then individuals who suspect themselves to be HIV positive will be deterred from obtaining medical care. As a result, these individuals might suscribe to medical quackery, rather than to orthodox medical care. This would eliminate the gains that reporting is intended to produce, such as early treatment

---

> giving people property rights in information about themselves and letting them sell those rights freely. The process of voluntary exchange would then assure that the information was put to its most valuable use. . . .
>
> The interest in encouraging investment in the production of socially valuable information presents the strongest case for granting property rights in secrets. This is the economic rationale for according legal protection to the variety of commercial ideas, plans, and information encompassed by the term 'trade secret.'

Id.

128. *Id.*

129. *Id.* at 398 (citations omitted).

with AZT and potential blood plasma donations for other AIDS patients. However, by educating the general populace and increasing their understanding and tolerance of AIDS, HIV individuals will be encouraged to seek the benefits of early treatment, regardless of their fears of becoming an officially documented case.

Another economic argument in support of database reporting balances the value of secrecy to the infected party against the value of knowledge to the community wherein the infected party interacts.

> Consider, for example . . . whether the law should allow a magazine to sell its subscriber list to another magazine without obtaining the subscriber's consent . . . . [T]he costs of obtaining subscriber approval would be high relative to the value of the list. If, therefore, we believe that these lists are generally worth more to the purchasers than being shielded from possible unwanted solicitations is worth to the subscriber, we should assign the property right to the magazine; and the law does this.[130]

Similarly, if the knowledge that an individual is HIV positive is worth more to the individual's medical/financial/sexual partners than secrecy is to the individual, the right to the information should be assigned to the medical/financial/sexual partners.

Knowledge concerning one's medical condition is arguably far more harmful to the ill person than the inclusion of one's name on a magazine subscription list. Yet, there are still good reasons to assign the property right away from the seropositive individual.

> Much of the demand for privacy . . . concerns discreditable information, often information concerning past or present criminal activity or moral conduct at variance with a person's professed moral standards. And often the motive for concealment is, as suggested earlier, to mislead those with whom he transacts. Other private information that people wish to conceal, while not strictly discreditable, would, if revealed, correct misapprehensions that the individual is trying to exploit, as when a worker conceals a serious health problem from his employer or a prospective husband conceals his sterility from his fiancee. It is not clear why society should assign the property right in such information to the individual to whom it pertains; and the common law . . . generally does not.
>
> . . . .
>
> An analogy to the world of commerce may help explain why people should not—on economic grounds, in any event—have right to conceal material facts about themselves. We think it is wrong (and inefficient) that the law should permit a seller in hawking his wares to make false or incomplete representations as to their quality. But people "sell" themselves as well as their goods. They profess high standards of behavior in order to induce others to engage in social or

130. *Id.* at 398 (citing Shibley v. Time, Inc., 45 Ohio App. 2d 69, 341 N.E.2d 337 (1975)).

> business dealings with them from which they derive an advantage but at the same time they conceal some of the facts that these acquaintances would find useful in forming an accurate picture of their character. There are practical reasons for not imposing a general duty of full and frank disclosure of one's material personal shortcomings—a duty not to be hypocrite. But everyone should be allowed to protect himself from disadvantageous transactions by ferreting out concealed facts about individuals which are material to the representations (implicit or explicit) that those individuals make concerning their moral qualities.[131]

With respect to having AIDS or testing seropositive for AIDS, a deadly and financially crippling disease, surely this is a material fact of which a prospective partner should be aware—whether this be a sexual partner or a financial partner (employer or insurer).

> It is no answer that such individuals have "the right to be let alone." Very few people want to be let alone. They want to manipulate the world around them by selective disclosure of facts about themselves. Why should others be asked to take their self-serving claims at face value and be prevented from obtaining the information necessary to verify or disprove these claims?[132]

Opponents of AIDS databases would urge that there are less intrusive alternatives. While this may be true in the sexual context (as in encouraging the entire populace to engage only in safe sex), this is not likely to be true in the financial context unless a system is created to defray the financial drain away from insurers and employers to society at large.

In general, there are two forces which combine in the economic arguments pertaining to privacy.

> The two main strands of the argument—related to personal facts and to communications—can be joined by remarking the difference in this context between ends and means. With regards to ends there is a prima facie case for assigning the property right in a secret that is a by-product of socially productive activity to the individual if its compelled disclosure would impair the incentives to engage in that activity; but there is a prima facie case for assigning the property right away from the individual where secrecy would reduce the social product by misleading people with whom he deals.[133]

This economic argument leads to dramatic results:

> the protections of trade and business secrets by which businessmen exploit their superior knowledge or skills (applied to the personal level,

131. *Id.* at 399-400.

132. *Id.* at 400 (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).

133. *Id.* at 403. In other words, "Reticence is generally a means rather than an end." *Id.* at 400.

> as it should be, the principle would, for example, entitle the social host or hostess to conceal the recipe of a successful dinner) . . . [and] . . . generally no protection for facts about people—my ill health, evil temper, even my income would not be facts over which I had property rights. . . .[134]

To overcome these drastic results many would turn to some philosophical or moral notion to preserve privacy rights over material facts concerning one's body. However,

> moral theory may be quite powerful when it insists that every person owns his own body, but it is vastly weaker when it makes the claim of ownership with respect to the control of information about that body. Within this void the economic theories of property rights are of some assistance because they point toward a private assignment of rights to information that is the product of individual effort and initiative and toward a public assignment of rights to newsworthy events.[135]

Here, testing seropositive for AIDS would be deemed a newsworthy event and not the result of some unique individual effort or achievement. Furthermore, many support this result against privacy over newsworthy events for noneconomic rationales.[136]

The primary fear of reporting names seems to be that those who receive the information will abuse it, perhaps even in a physically violent sense.

> This suppression of information is unwarranted, even if the person who hears it might misuse or misinterpret it. Persons should normally be told the truth. Society does not imprison individuals who are likely to make foolish or irrational decisions. So, too, it should not countenance their belief that they are incapable of handling the truth.[137]

Thus, despite the incredible intolerance frequently displayed toward vulnerable AIDS carriers, and despite the potential loss of job, medical treatment, insurance, and funds, many would urge that there is no privacy right whatsoever in the status of an HIV test. In support of this conclusion, it is important to note that

> [m]isrepresentation . . . is not a criminal matter, but a civil matter between two private parties. And in this context, the individual who is asked to risk his property and his reputation [in this instance referring to the non-AIDS infected individual] should not have his freedom compromised solely to advance the private interests of others . . . . Assume the possibility that he will misuse or misinterpret the information is real. It does not justify a suppression of the information (that in itself can be subject to abuse) but a disclosure of the information coupled

134. *Id.* at 404.

135. *Misrepresentations*, *supra* note 111, at 465.

136. *Id.* at 466.

137. *Id.* at 470-71.

with explanation about its import and effect.[138]

Thus, from an economic standpoint, not only should names be reported to a database, but access to this database should be a virtual free-for-all. The author believes this conclusion wholly ignores the needs of already struggling AIDS victims, and would, instead, advocate a system of stringent regulation that would protect reported names and permit only limited access to the names. The author also believes that education and a system of public welfare are needed to combat the hostile reaction to, and isolation of, AIDS carriers, and to support and insure AIDS victims.

IV. EDUCATION AND PUBLIC INSURANCE FOR AIDS CARRIERS

As the preceding discussion indicates, a strong case can be made for the reporting of seropositive names into a state database. However, the author supports such reporting only to the extent that the database is created in conjunction with a public insurance system for AIDS victims and a massive educational program for the general populace.

A. PUBLIC INSURANCE

AIDS is a unique problem because it (1) ultimately prohibits a person from being financially self-supportive, due to extensive sick-leaves; (2) is transmittable and fatal, thus leading to social isolation for many of its victims and further loss of financial support; and (3) is a disease for which the only partially effective drug, AZT, can cost in excess of $10,000 per year, not including any other medical costs. To date, victims, over-burdened hospitals, and insurance companies have divided up the financial whirlpool resulting from virtually every seropositive case. Dollars are scarce and many victims, who are forced to leave the workplace because of the unexpected illness, find themselves adjusting from once self-supportive lifestyles to a meager welfare existence, while they literally await a socially isolated death in a barren apartment or overcrowded hospital facility. These conditions are intolerable in a country which has stressed human dignity and freedom. It is essential, therefore, that some support system be designed to finance AIDS' health care, or, at the very least, to ease the financial worry of a victim's last period of life. One argument levied against such a system is that it would entail a financial cost to society which some members, probably those least at risk, would prefer not to pay or would prefer to transfer to other needy causes. However, unlike many other causes, the financial costs of AIDS to society already exist in dollar form, albeit some-

138. *Id.* at 472-73.

what obscured by the fact that the costs filter through the insurance industry to policy holders and to health care consumers through increased rates meant to subsidize the drain caused by impoverished AIDS patients. A public insurance system would be a means of spreading preexisting costs throughout society. While the set-up and bureaucratic costs of such a system would be high, given the extensive nature of the epidemic, these transaction costs could be amortized over a long period of time to reduce the initial impact. Such a system would also help ameliorate the financial havoc which could arise in conjunction with the reporting of seropositive names, should employers and insurers attain legal access to the database.

B. EDUCATION

> Much has been written and broadcast about AIDS that explains in detail who is and isn't at risk and how the disease is transmitted. Yet, for many people, little seems to have sunk in. A public-housing official in Rochester, N.Y., tried unsuccessfully to evict a man who was giving shelter to an AIDS victim; the official claimed that the apartment complex was endangered. When a maintenance man did work on the tenant's toilet, he wore a World War II mask, tall fishing boots, and rubber gloves.[139]

Apparently education has been, for the most part, ineffective. Uninfected individuals refuse to recognize the limited manner in which AIDS can be transmitted. The attitude which seems to prevail is a legitimate, bottom-line oriented, "why take the risk at all" attitude. This attitude is compounded by the public's distrust of what government leaders tell them.

> The government told us nuclear power was nothing to worry about, and then you have Three Mile Island. The government puts its best minds at NASA, and then you have the Challenger space-shuttle disaster . . . . And now, researchers and health care workers are contracting the AIDS virus. People wonder how much the government really knows.[140]

Thus, the first problem educators face is how to gain the respect of the people they are trying to educate. Former Surgeon General, C. Everett Koop, was unsuccessful in his attempt to gain this respect via cable television specials and an array of press releases. Contributing to the problem is the fact that current education strategies often focus on generic how-to-avoid-the-disease themes, rather than avoidance's corollary, how to treat and handle seropositive and AIDS patients. Consequently, education is much more likely to effect sexual habits before it helps the

139. Wall St. J., Nov. 13, 1987, at 1, col. 1.

140. *Id.* (quoting Lester Lave, economist specializing in risk analysis at Carnegie-Mellon University in Pittsburgh).

psychological plight of the vulnerable AIDS victim. This result is not necessarily a negative achievement, given that the primary goal should be to immobilize the spread of the disease. However, as "safe sex" becomes a household word, it is necessary to turn the focus of education toward the needs of the already infected individual. Respect for both forms of education will likely blossom as researchers enjoy more success in halting the progression of AIDS in individual patients, thereby gaining credibility. Ultimately, education will effect not only people's sexual practices, but also how they treat AIDS victims.

IV. CONCLUSION

It would be naive to claim that the potential for abuse of computer technology in the AIDS context does not exist. Despite the weaknesses inherent in any data protection scheme, stringent regulation can help to maintain the integrity of the AIDS carrier's medical record. Moreover, the benefits of using such an AIDS database for epidemiological and medical treatment purposes are substantial and support a rational basis test for claimed violations of equal protection. With regard to privacy, the AIDS carriers' interests are offset, at least in part, by society's interest in open and fair dealing. It is the opinion of this author that names should be reported, if only for medical treatment purposes via contact tracing, but that the maintenance of an AIDS database should only be implemented in conjunction with public AIDS insurance and education programs, so as to ameliorate a portion of the inevitable and substantial additional burdens which may befall the AIDS carrier as a direct or indirect consequence of name reporting and database creation.

M. Nicole van Dam