Privacy and Cyber/Spaces:

Medical and Other Cases

edited by

Richard Sobel

Harvard University

January 2004

Based on a panel at

The Berkman Center for Internet in Society at

Harvard Law School

[13 May 1998]

I. Introduction: Charles Nesson

Charles Nesson is director of the Berkman Center for Internet and Society, which he founded in 1997 at Harvard Law School with a bequest from Jack and Lillian Berkman. Professor Nesson was also the moderator for the PBS series, "The Constitution: That Delicate Balance."

The mission of the Berkman Center is to understand how law works in cyberspace. There's a query on that sentence, because my disposition is that law has a limited role in cyberspace. The idea of studying how law develops and how communities function in cyberspace is a subject that doesn't exist in books. And so the mode of operation of the Center is to build out into the space. Rather than taking it as a traditional academic subject, we confront issues as we go, study them and see if we can make progress in rationalizing them.

The first issue, from the user's point of view, as we build out into cyberspace, is privacy. And we, in fact, have started a cybercourse on privacy, which Molly Shaffer van Houweling speaks about here. The issue that is a part of this panel is that there's a clear and deeply powerful conflict emerging with respect to issues of privacy. On the one hand, we see things like the health care system striving to develop standards. And they want the standards because they need them for credibility. They have been impeached by the profit motive and they're looking for ways to say they practice good medicine. The very process of articulating that in credible form calls for the development of much more elaborate information systems that allow auditing of decisions with respect to patients. This is an honorable enterprise, and at the same time clearly poses enormous possibilities for use and misuse of information that's acquired.

Likewise, on the national security front, we've recently seen a Department of Defense simulation of virus warfare spread along the Mexican border.[1] That simulation produced not a rational response with evacuation and containment, but rather a breakdown of the relevant agencies into stalemated squabbling, with contagion taking over. This clearly is a prelude to the Department of Defense recognizing the need for greatly elaborated information systems for containment of any form of network infection, whether biological or electronic. What that system suggests is audit trails so that when damage is done, it can be sensed and responded to in order to create containment. This is an extremely powerful force pushing in the direction of much elaborated information systems. And it comes up once again against the notion of privacy.

For me the key question is, how will we go forward into the future? Can we identify or develop a process by which our sensibilities about privacy are lined up with the actual practical steps that have to be made? Can each be flexible in a way that produces a resolution that enables us to have excellent health care, excellent security, and an excellent sense of personal privacy? These are some of the issues that motivated the panel "Privacy and Cyber/Spaces" cosponsored by the Berkman Center on May 13, 1998 at Harvard Law School.

This report presents the material from that panel on “Privacy and Cyber/Spaces.” Each of the six panelists discussed an important element of privacy, government databanks, identification, and computer networks. The panel addressed "cyberspaces" because its members discussed more than one government databank or identification scheme. Four of the presentations focus on the important issues of confidentiality in

[1] Judith Miller and William J. Broad. “Exercise Finds U.S. Unable to Handle Germ War Threat.”

medical care particularly related to the Health Insurance Portability and Accountability Act (HIPAA) of 1996. This is the controversial law that mandates a "unique health identifier" for every American. The panelists also touch upon the intersection of private and public medical databases. The last two panelists discuss broader issues of privacy, other government data collection, and other cyberspaces. Together they raise issues of how government databanks and identification schemes bring constitutional questions forward. These provocative analyses inform debate on a pressing set of national issues.

Professor Phyllis Freeman, from the University of Massachusetts/Boston, begins with a discussion of confidentiality in medical research and administrations in "Privacy Issues in Health Care." Her very interesting paper, which she summarizes here, overviews the health data privacy debate. She presents in overview a very complicated subject about the kind of dilemmas that individuals are facing when seeking health care and which this panel tries to clarify.

Dr. Denise Nagel from the National Coalition for Patients Rights critiques Professor Freeman's paper and the erosion of confidentiality in the pursuit of profit. In "Patient Confidentiality and Pursuit of Profit," she defends the need for doctors and patients to maintain a confidential relationship. This cornerstone of good medical care is threatened when informed consent is removed through databank access.

Dr. Philip Caper from Codman Research Associates discusses medical data from a research perspective. He outlines the possibilities and arguments about the beneficial uses of medical data as well as some of the privacy issues involved in "The Benefits of Appropriate Use of Medical Data." His fundamental question coincides with the subtitle

---

The New York Times 26 April 1998: A1.

of Phyllis Freeman's paper; "can we achieve comprehension before closure?" These issues deserve extensive debate, and yet HIPAA regulations may be in place before the debate fully addresses them.

Dr. Harold Bursztajn from Harvard Medical School examines ethical issues of managed care in "Questions about Confidentiality in Managed Care." In raising a number of key questions, he uses the humorous aspect of time constraint to bring home a very important point about time and money restrictions on current health care. He examines the manner in which databases are abused in denying patients rights and benefits, foremost of which is patient confidentiality. This completes the subpanel on medical privacy.

John Roberts from the Massachusetts Civil Liberty Union talks about other government databanks and related privacy questions. In "Security in Government and the Private Sector," he addresses the question of privacy and identification, including the expanding use of Social Security Numbers. He emphasizes both the individual role and the larger societal roles in maintaining privacy and places the intermix of public and private data within the larger question of government databanks.

Molly Shaffer van Houweling, former editor for The Harvard Journal of Law and Technology, talks about the cybercourse, "Privacy and Cyberspace." This was the first Berkman Center cyber offering, and one of the inspirations for this panel. The course was run by Professor Arthur Miller, one of the co-directors of the Berkman Center, and a pioneer on the legal question about privacy and computers. Ms. Shaffer van Houweling uses her experience as teaching fellow in the cybercourse in order to illustrate the extent to which people want their personal information preserved. In "Learning from a Cyber

Course on Privacy," she points out the lack of legal controls placed on the use of information in cyberspace.

Finally, Richard Sobel, a Berkman Center Fellow who moderated the panel, provides a final note, "Reflections," on the constitutional issues these presentations raise. He focuses on the role of the government concerning privacy in cyberspace and calls our attention to three contradicting aspects of American Democracy regarding streamlined data collection: the derivation of American governmental powers, the structure of the U.S. government (federalism with separation of powers), and the protections against government intrusions the Founding Fathers wrote into the Constitution and the Bill of Rights.

In short, this publication presents in edited form the essence of an early, yet sophisticated, discussion of central issue of privacy regarding medical and other data collections. The report is the first of what may be many Berkman Center publications on cyberspace issues. The panel was cosponsored by the Harvard Information Infrastructure Project (HIIP) at the Kennedy School and the *Harvard Journal of Law and Technology* (JOLT). The website for the panel at *cyber.law.harvard.edu/spaces.html* includes a transcript of remarks and questions. The presentations were also video taped.

II. Phyllis Freeman, Discussing Privacy Issues in Health Care

Professor Phyllis Freeman is a lawyer and Chair of the Law Center in the College of Public and Community Service, on the faculty of the Public Policy Ph.D. program and a Senior Fellow at the McCormack Institute of Public Affairs at the University of Massachusetts in Boston. Previously, she served as counsel to the Subcommittee on Oversight and Investigation of the Energy and Commerce Committee in the United States House of Representatives. She was also a Scholar in Residence at the Institute of Medicine at the National Academy of Sciences in Washington.

The arguments in the national health information privacy debate have changed little over the last 25 years. In order to understand this year's version of the health privacy debate, one needs to understand in which related areas the Congress has concentrated its efforts most recently. What is new is the 1996 Congressional enactment of the Health Care Portability and Accountability Act (HIPAA.)

HIPAA was known as the Kennedy-Kassebaum bill in its earlier years. I think of it as the dregs of the Clinton health care reform efforts. It contains a provision saying, that if you have health insurance, and if you move from one job to another, the insurance industry is not permitted to cancel your coverage. But you have to be able to pay the full premium, so this provision alone does not solve many problems for the vast number of people for whom ability to pay is a major barrier.

HIPAA raises incredibly difficult privacy concerns that may be difficult to resolve. These are raised by the so called "administrative simplification" provisions. HIPAA requires assignment of a unique patient identifier for everyone who participates in any kind of medical services in this country. It also calls for a uniform, standardized,

electronic data set for any information in transactions that involve administrative and financial issues. So for any transactions involving money and administration of the health care system, a unique identifier is required. These features are the special characteristics that frame this moment in this long debate.

What makes me dubious about whether we can expect any reasonable law to come out of the Congress (aside from having worked there for three years), is that the Congress has set itself a deadline for setting privacy policy and writing a law for August 1999. While this deadline has been known since 1996, I don't think we have made extraordinary gains towards clarifying the issues, never mind resolving them.

Understanding the sources of support and enthusiasm for these provisions (the unique identifier and administrative simplification) will help us make sense of the privacy struggle. In the shortest form, most health legislation is NOT about health. And this is no exception. Most health legislation is about the economy. It is about global economic competition, the cost of health care insurance and services -- the cost of the whole system we run. All the other issues, including our health, turn out to be subtext or footnotes--not the main points. So the most enthusiastic proponents of HIPAA are those concerned with how the U.S. fares in the global economy. Those active around administrative simplification in particular, are principally concerned with financial and managerial aspects of the health care system: eligibility determination, enrollment and billing. Another group is very concerned with curbing fraud and abuse, which by some Health and Human Services (HHS) estimates amounts to something like 10% of our trillion dollar health care enterprise--billions of dollars of investment that are thought to be wasted.

There is another set of enthusiasts whom I would categorize differently, and those are the researchers and health providers most concerned with the quality of clinical care and improving clinical outcomes. For example, health services researchers have enormous enthusiasm for large data sets and for sharing and linking them, and for studying outcomes over time. (While individuals data are often drawn from medical records, for research purposes the individual identity of the patients can be stripped or coded, so many of the privacy objections can be overcome.)

The most enthusiastic proponents of "administrative simplification" then, are those principally concerned with efficiency of billing and other administrative functions. The struggle over privacy emanates from this starting point--and from the observation that health care provider entities and insurers have been known to give away or sell identifiable health information for commercial gain.

I am very concerned that we are likely to end up with poor health privacy law. The field is incredibly complex, and most parties to the debate do not understand the full range of issues. There are thousands of data elements, and innumerable ways in which they might be handled, and myriad purposes for which they might be used. Even the experts understand less than I would hope for and the general public is largely unaware of most of the implications for themselves, never mind for society 10, 20, 50 years from now.

We have been engaged in this very same debate for at least 25 years since computers became a major presence in our lives. There is a vast literature in which virtually the same sets of privacy principals and the same controversies are discussed, year after year. Reports that are well known in the field document widespread trafficking

in health records, especially among commercial entities. This history was recounted in Congressional documents prepared during the Clinton era of health reform. There has been little dispute of the finding that if there had been a change in the 15 years leading to the 1994 Congressional debate, that "organized trafficking in health personal records, both legal and illegal, may have increased." The damage to individual human beings has included losses of jobs and pensions, health insurance, life insurance -- and other forms of discrimination.

Because the economic value of individually identified or identifiable information is ever greater in the commercial sphere, protecting individuals from intrusions will not become more popular with industry--hospitals, health plans, insurance companies, data management firms, pharmaceutical and medical device firms and many more. And commercial users of health data will lobby effectively with the Congress to protect their interests. As data, technology and the uses become ever more complicated, the likelihood of democratizing the discussions so that more people can knowledgeably participate in them-- and are able to explain what the stakes are for themselves to the Congress-- is much reduced.

The paper that my colleague, Dr. Anthony Robbins, and I wrote grew out of a lack of clarity I found at the level of people who handle patient records within the health care system.[2] (This is probably not at the level of folks who are participating in this panel, who are very sophisticated about the issues, but maybe one or several levels down in the organizations.) I would sit in on policy conversations in the wake of the new

[2] Phyllis Freeman and Anthony Robbins. "The U.S. Health Privacy Debate: Will there be Comprehension Before Closure?", *International Journal of Technology Assessment in Health Care*, Cambridge University Press, 15:2 (1999), 316-331

HIPAA law, and invariably discover that professionals in the field were not talking about the same issue or data element at the same time. They would be having what they thought was an intense policy debate about how we ought to manage health information to protect privacy, but they were not making the same assumptions about how identity would be handled; whether data were to be clearly identifiable or coded, or whether the identifier was to be stripped and anonymity guaranteed (except for some code keeper, who was supposed to be the point person for security). Consequently the conversations resembled theater of the absurd more closely than a productive policy debate. Even among professionals in the same field, the assumptions made were not shared and issues under debate were not being clarified or resolved while frustration and passions escalated. If this is the status of the debate among small groups of intelligent people who handle health records for a living, what expectations do we dare to have about the Congressional debate? I do not have a good feeling about the answer to my question.

This immersion in theatre of the absurd caused me to ask: If I were appointed czar for bringing a modicum of intellectual discipline to a discussion about these issues, how could we begin to talk about the same thing at the same time? Perhaps then we could discover what we understand, and about what issues do we disagree or agree. On what issues--despite the level of sophistication of the experts-- do we understand so little that we cannot honestly boast well informed opinions? I find there are a number of issues on which I do not yet have an opinion because I can't figure them out. (The cited paper offers examples). I wanted to help people sort out where as a society we are clear and less clear, based on my attachment to the obvious notion that it is easier to make policy on issues we can define and describe than it is on ones we cannot.

After presenting a historical picture of the 25 years of unproductive policy debate, our paper proposes a way for reproducibly describing any data transaction in detail. That is, we lay out a scheme for each participant in the debate to be sure s/he can see just which data elements are going where, for what purposes will each be used, who will use what, and who will glean the primary benefit from a particular data transfer. However remarkable it may seem, this prerequisite for sensible dialogue has eluded us to date.

Next the paper suggests how to proceed once we can better understand where we agree and disagree -- and which issues we simply do not understand not at all. To move toward resolution on privacy concerns, it would be very useful discover where we agree on the purposes for which identifiable ought to be used--and by whom. For example, the most familiar situation is the medical care setting -- where the person who is meant to be the primary beneficiary of any data transfer is the patient--not the provider or the insurer although they are both involved. In patient care, individuals trade privacy against the involvement of more providers with varied expertise because the additional providers might contribute something that would make the patient's outcome better. And individuals also trade off privacy for payment--they permit information to go to insurers, because without sharing some information with the insurer, the patient might be denied a desired service. Even in this most familiar of situations--patient-providers-insurers--there is an endless supply of policy issues we have not resolved. For example, for claims to be paid, just how much information needs to go--and to whom-- and at what level of identification? Even in this relatively small domain of activity (compared to the universe of data transactions in this debate) there is an uproar of passionate disagreement. But

there are also some issues that we can talk about quite sensibly because many people do understand the issues and what is at stake for whom.

A third area we write about is the commercial use of data. All those industries I mentioned earlier which have enormous interests in the economic value of the data, want very few restrictions on their use of health data. Their greatest economic gains derive from innovation in using identified data in as many ways as possible. Many firms market products to us based on their knowledge of clinical encounters including prescription drug purchases. Thus, patients suffering from clinical depression may find in their mail offers for new anti-depressives.

From a policy standpoint, I have a very simple view of commercial exploitation of personal health data. I do not understand why personally identified health data gathered in a patient care setting should ever be available for commercial exploitation without the knowledge and consent of the data subject. Period. I am prepared to have the industry try to explain to me-- and to all of us --why that is not right and to convince me there may be some interest I do not understand that would bring me to a different conclusion. But I have yet to have that presentation made or for me to be convinced.

Next it is important to discuss what I believe to be the most complicated area: uses of personal health data to achieve public purposes to benefit society. Not only is this area most complex, it has been the subject of the least public attention. It is complex because there are many public purposes for which we use data. We use personal health data for research to understand which interventions actually help people recover from serious illnesses better than others; and we use it for public health interventions to prevent exposures that cause disease. We use personal health information in licensing

health facilities and in certifying professionals. And many folks are concerned with availability of data to assist in law enforcement. Uses of health data for this public purpose have been the most controversial.

Some data are personally identified. Some are not. And for each public purpose--be it public health, licensure, certification or law enforcement--there are different experts who have a grip on how we have managed data in the past and what seems good or bad about that history. It is the experts who know what privacy issues are raised in each area. And the experts in one area are unlikely to talk to those in another. Health services researchers and law enforcement officials, for example, do not speak the same language. In those public policy discussions that reminded me of theater of the absurd, participants often lumped all these public purposes together--apparently assuming we could sensibly balance privacy against a host of public purposes all at once. Of course this will not work. There are different trade offs in each area.

Assessing trade offs is the next step for anyone wishing to develop a persuasive position on how to balance privacy against the host of other considerations. It is important to keep in mind that the trade offs differ when one is in the domain of medical care--where benefit a particular individual is paramount; or that of public purposes intended to benefit society at large, or in the commercial domain where economic advantage is expected for a particular entity and its owners. A productive policy debate about which trade offs we should codify in our law requires that all participants be informed about data practices--better informed than we are today. It also depends on broad appreciation of the variety of purposes for which data are used. Only then can

each participant in the debate weigh and present to others a reasoned policy position about how much--how--and why--to limit transfers of data.

I came to the privacy debate through my interest in public health. I am attached to the simple notion that it is desirable for health care legislation to have something to do with improving the health of the entire population. I am desperately eager for the privacy debate to give equal time and attention to public health as to billing. I understand that the cooperation--or even tolerance of the public with regard to use of data for research and interventions to improve population health-- depends on public confidence in those who may see their data, but whom the data subjects may never meet. This creates an important burden of persuasion on health professionals for engaging with the public in a way that has nearly invisible to date.

Additionally I came to understand the importance of this debate through my students. Many of them work in public and community services. They routinely handle personal data of vulnerable individuals -- without any help in understanding the consequences of their activities in terms of loss of privacy and potential for discrimination. I thought we would do well to add this area to our curriculum so more of us can appreciate both intended and unintended consequences of routine ways in which public and private sector service agencies handle data. As I gathered material for a new course, I was fascinated that in all of the literature I could find no comprehensive--nor comprehensible-- map for learning how data migrate from a clinical encounter into commercial or public realms. And I have yet to meet a single human who pretends to possess such a map, even an unpublished one. I had eagerly read the most recent study of the National Research Council in search of just such a map, but it is not there. So my

students and I did our best to construct one from what data and admissions filtered into the policy literature and into the popular press.

Despite the many queries by privacy advocates, it continues to be the case that commercial entities with the huge economic interests prefer not to divulge their data handling practices. I have met individuals who work for managed care organizations who believe their organizations provide good health care -- but do not want their employees to talk about all the ways data are handled internally. Such employees cannot always distinguish with confidence when patient data are used for the patient's care versus uses to help the organization survive in the fiercely competitive marketplace.

These are but a few examples that lead me to conclude that the health care policy debate is in a most humble state. That's a very kind characterization, one intended to caution us about what can expect from the Congress in 1999.

Perhaps Phil Caper can help us understand some opportunities to improve health if we use data carefully. He is one of the few I know with a detailed understanding of the area in this debate that I believe is most in need of discussion. It is not without privacy complications. How we protect privacy but continue to gain health benefits from data based on research? This topic is too often neglected in the policy debate. I look forward to hearing Phil Caper's thoughts so he can provoke us into more productive discussion.

III. Denise Nagel, "Patient Confidentiality and Pursuit of Profit"

Dr. Denise Nagel, a practicing psychiatrist, is the executive director of the National Coalition for Patient Rights. The National Coalition is a non-profit organization that is dedicated to restoring medical privacy through advocacy and public education. In addition, she is a clinical instructor at Harvard Medical School, and she has testified before key congressional committees on the issue of patient privacy. Dr. Nagel has been widely quoted in The New York Times, The Wall Street Journal, and Time Magazine, and has appeared on ABC News "Nightline." In Spring 1998 she also participated in Professor Arthur Miller's cybercourse on "Privacy in Cyberspace" concerning the issue of medical confidentiality.

There's a cartoon by John McPherson that I used to think exaggerated the threat to our medical privacy. The cartoon shows a middle-aged couple eating dessert in a restaurant. The woman is raising a fork full of cheesecake to her mouth when two men in suits accost her. One approaches from behind and grabs the arm holding her fork. The other flashes a badge and barks: "Mrs. Stalnaker? Neil Haggerty, Unity National Health Insurance. Put down the cheesecake now, or we'll double your premium."

There are other examples of where health care and profits intersect. Prescription drugs are now marketed, in part, through the grocery-store checkout line. Depending on what shoppers have in their baskets, they might receive an instant "coupon" referring them to a toll-free number for more information about prescription drugs for high cholesterol, allergies or depression.

In medical magazines [such as Health Data Management], it's easy to find ads such as one from Metromail announcing the world's finest list of who has what:

Diabetes, 1.26 million people; bladder-control problems, 945,000; high cholesterol, 2.5 million. Names and addresses like these are often compiled by maximum-security prisoners.

In the financial press, the articles themselves are no more reassuring. A recent *Fortune* article describes how the bakery company Sara Lee teamed up with its insurer, a subsidiary of Cigna, to cross check the list of patients using a lot of medical services with the list of employees missing the most days at work or performing below par. The article concluded: "It won't be surprising if those sluggish workers are told of the wonders of SSRI's [anti-depressants]."[3] As a psychiatrist I am all in favor of early intervention for depression but…

Some suggest that the sacrosanct notion of a private doctor-patient relationship is quaint in these days of computerized records and cost-cutting HMOs, yet it is the foundation upon which good medical care must rest. Despite that, commercial interests and even the federal government are aggressively pushing for laws that would abolish the idea of informed consent and confidentiality and instead standardize the collection, exchange, and release of our most intimate information. Just because we have the technology to mine every patient record for nuggets of commercial “gold” doesn’t mean it should be done. We need pro-patient access and disclosure policies that assure patient privacy while applying the benefits of technology. People deserve the right to keep certain sensitive information out of databases without being penalized by their employers, insurers or the government.

---

[3] Thomas A. Stewart. "A New Way to Think About Employees," *Fortune* 13 April 1998: 169-170

Medical information is a hot commodity. Dr. Charles Welch, chairman of a Massachusetts Medical Society task force on privacy and confidentiality, put it this way: "There is a long gravy train forming around medical records. The insurance companies are making money; the politicians are making money. And there's only one party that's paying, and that's the patient.

There's a huge amount of money at stake. The New York Times has described the whole exchange of computerized medical information as a $40-billion-dollar industry. Pharmaceutical firms spent almost $875 million on consumer advertising in 1997, compared to $164 million in 1993. They sold about $80 billion in prescription drugs, both generic and branded.

One way to target potential customers is to buy names collected from database houses that have purchased lists from doctors, clinics, pharmacies, hospitals, and HMOs. One database marketing firm, Elensys, does a brisk business with 15,000 pharmacies each week, receiving electronic prescription records from the drugstores, tracking prescription refills, and sending out letters either urging them to keep taking their medicine or touting new products that would also be appropriate for their illness. Often, prescription drug makers underwrite this service, although Elensys has insisted in published reports that it does not share pharmacy records with the drug companies**.**

Two companies that had used Elensys in order to contact people who had not refilled prescriptions, Giant Food Inc. and the CVS Corp., stopped the practice and apologized after a report in The Washington Post on February 15, 1998 provoked a huge

customer outcry.[4] The companies had initially defended their efforts, saying they were just trying to help customers stay healthy. But others were harshly critical.

Dr. George D. Lundberg, editor of the Journal of the American Medical Association, was quoted in The Washington Post as saying the practice was "a gross invasion" and a "breach of fundamental medical ethical issues." He asked: "Do you want… the great computer in the sky to have a computer list of every drug you take, from which can be deduced your likely diseases - all without your permission?"[5] The temptation to misuse such information is great, and the consequences are grave. In addition to the embarrassment and shame of a sensitive medical condition becoming widely known are the very real possibilities of higher insurance premiums, loss of insurance altogether, and being fired from a job.

An employee of the Southeastern Pennsylvania Transit Authority, SEPTA, for example, discovered that hard truth a few years ago. He was taking medication for AIDS when his condition was discovered by a high-level administrator at the transit authority. [6] Rite Aid, which administered Southeastern Pennsylvania Transit Authority's (SEPTA) prescription-drug plan, routinely sent records with patient names on them to a high-level executive. That executive started making inquiries about the employee with AIDS, leading many people to find out about his disease and to make his life miserable.

The employee sued. A federal jury agreed that he was wronged, and awarded him $125,000. But an appeals court overturned the ruling, declaring that a "self-insured

---

[4] Robert O'Harrow Jr. "Prescription Sales, Privacy Fears, CVS, Giant Share Customer Records with Drug Marketing Firm." Washington Post 15 February 1998: A1. [herein Robert O'Harrow Jr.]
[5] Robert O'Harrow Jr.
[6] EPIC. EPIC Alert. 24 January 1996 12. accessed on February 2004 www.epic.org/alert/EPIC_Alert_3.02.html.

employer's need for access to employee prescription records under its health-insurance plan… outweighs an employee's interest in keeping his prescription drug purchases confidential."

This leads to another problem. Most people do not realize that if an employer is self-insured, it is entitled to all sorts of information about its employees' medical treatment. And Human Resources executives at many firms have told me about receiving very detailed, personally identifiable information about employees from their insurance carriers even when it has not been requested.

Many of the problems with the current system stem from the fact that insurers view corporations, not patients, as their customers. Some of the most egregious privacy problems would dissolve if the needs of patients were primary. So it is disturbing to read Professor Freeman's paper and discover some bias embedded in a work presented as a balanced view.[7] In the very description of "parties to the debate" that is laid out in the first table, clinicians are listed as just one of 28 groups that are considered necessary to the health-privacy debate. They are not given any special status, but instead are listed as "professionals" along with data managers, administrators and law enforcers. The "professionals" are separated from entities that include data management firms, employers and insurance carriers. There is no doubt one could argue that these are all "parties to the debate." However, there needs to be real differentiation among the parties.

Contrast this to the way the Canadian Medical Society has addressed this same issue. "The depiction of physicians as but one of several 'stakeholders'...fails to

---

[7] Phyllis Freeman and Anthony Robbins. "The U.S. Health Privacy Debate: Will there be Comprehension Before Closure?", *International Journal of Technology Assessment in Health Care*, Cambridge University Press, 15:2 (1999), 316-331

recognize that the information in question has been confided to physicians in the context of a very special trust. Also missed is the fact that physicians therefore have a greater stake and moral claim to shape policy decisions affecting this trust. Represented as but one among many groups of stakeholders, the fiduciary perspective is diluted, not 'balanced.'" This may seem like a small point, but actually it is central to the whole discussion of patient privacy, national ID numbers, government databases, and so on.

Why do patients share information? They do it because they believe it will be used to make them well. One of the critical factors -- in fact, the cornerstone of that trust - is the privacy and confidentiality of the doctor-patient relationship. Sometimes patients will share intimate information they haven't told another soul in the world. The expectation since the time of Hippocrates has been that if patients did not want their information revealed, it would not be except in very limited situations. Now all of that is changing. But it is imperative to keep oneself grounded in the simple truth about why people share information and how they expect it to be used.

It used to be that people could consider a visit with their doctor to be an extremely private encounter. They expected that anything told to the physician would not be repeated unless they gave explicit and informed consent. But the definition of informed consent is changing in a very insidious way. The new definition that insurers, data-collection agencies and even Congress would have us adopt is this: In exchange for medical benefits, an individual agrees to allow his private medical information to be used by the system for prescribed purposes. "The system" is actually a group of "authorized knowers" too numerous to name, but including everyone from employers and insurers to government bureaucrats and police.

Most people are astounded when they find out what is going on and how key policy makers are setting out to codify certain egregious practices and overturn some good existing state law. They say to me: Isn't medical privacy like medical-school ethics 101? Not anymore.

Professor Freeman's paper mentions three arenas to consider in the debate: Patient care, public purposes and commerce. Let's look at public purposes. She says, "Those who understand activities where societal interest must supersede privacy will need to come forward, explain the benefits and answer the doubters...[because otherwise] victimized consumers, may band together to rewrite laws and restrict socially important data uses. Such a reaction is not unthinkable as voters in the U.S. often put individual liberties ahead of the common good."[8] This was very troubling to read in a paper that set out to be neutral. So far as I understand, individual liberties are considered a common good in this country.

Now let's be clear here. What is being discussed here is not whether we should have public-health reporting on tuberculosis or e.coli outbreaks, but rather whether we should be able to track everyone's abortion, impotence or psychotherapy through national ID numbers, databanks and cross-linking technologies.

Should we develop a DNA databank on every individual from birth and make that information available for various purposes? Should we require doctors to report every patient visit to a government database? Should we allow every person who has a new idea about how to operate more efficiently or "improve health care" to go rummaging

---

[8] Phyllis Freeman and Anthony Robbins. "The U.S. Health Privacy Debate: Will there be Comprehension Before Closure?", *International Journal of Technology Assessment in Health Care*, Cambridge University Press, 15:2 (1999), 316-331

through our most intimate secrets? My answer is no to all of these. The most important question should be: How do we maximize patient care while carefully guarding each patient's privacy? Often, good patient care gets pitted against privacy as if we can only have one or the other. If access and disclosure policies are set in place thoughtfully, we should be able to use the capabilities of the computer to our advantage for both purposes.

Yet our public officials are busy trying to codify the invasion of our medical privacy. The vehicle is a section of the 1996 Health Insurance Portability and Accountability Act, which is supposed to allow people to change jobs without losing their insurance. But sneaked into that law during a conference committee was a provision that has very dark implications for patient privacy and the doctor-patient relationship.

That provision is known benignly as "administrative simplification." It mandates many of the key features of the National Health Care Databank legislation that did not pass in 1994. The idea behind a health-care databank was this: If universal access to care were to be provided, everyone's medical data had to be widely available. Doctors were to report every patient visit, even those paid for privately, to this national databank. They were to be fined $1,000 each time they didn't. Each person was to have a unique identification number that would be linked to his or her every doctor visit, essentially a womb-to-tomb medical record.

What started as an idea for creating comprehensive, population-based health-care databases to ensure coverage remains essentially intact, only now without any guarantees of coverage. In fact, it puts additional information into the hands of insurers and others at

the same time as we are seeing evidence that these very facts are used as often to discriminate and cherry pick patients as it is to increase quality and care.

Administrative simplification essentially creates the infrastructure for a national databank. It requires a national ID number or some other kind of identifier - a fingerprint, perhaps, or eye scan - and it lays the groundwork for the electronic collection and exchange of the information contained in all of our medical records. Vice President Al Gore announced a temporary moratorium on the assignment of the unique ID number after a Page One story in The New York Times on July 20, 1998 caused a public outcry.[9] But we need to make sure that Gore's action isn't a stalling measure until public attention shifts somewhere else. We need to repeal patient ID.

As data become more usable and accessible, more and more people are clamoring for access. They all they think they deserve it. But we haven't seen anything yet. Here is what health-care economist Uwe Reinhardt has said:

> The central idea of 'managing health' would be to identify the predisposition to illness among enrolled families -- perhaps through genetic screening -- and then to have health plans help families manage their lives so as to reduce the likelihood of actual illness. To the extent that this is done at the behest of the family, and with diligent maintenance of the family's privacy, this would be all for the good. But one could imagine such an exercise to become oppressive, particularly if it is accompanied with the financial carrots and sticks that undoubtedly will be designed by the exuberant consultants now swarming around health care like hungry bees and even more so if, as is very likely, American families lose in the process all semblance of personal privacy... If that should happen, for example, if Americans passively accept ever deeper inroads into their private lives, an American health maintenance organization may come to resemble nothing so much as a commune that views the health of the individual the entire

[9] Sheryl Gay Stolberg. "Health Identifier for all Americans Runs into Hurdles." *The New York Times*. 20 July 1998: A1.

> [Chinese] commune's affair. It is not a scenario easily reconciled in my mind with this nation's much-celebrated individualism.

The Washington Post, in an editorial, noted: "Once complete health information is available in a government database accessible on grounds of research or law enforcement, the odds of leakage or misuse are tremendous…. You have a recipe for driving people out of the medical system altogether."[10]

Who decides what is in the public's good? In the Supreme Court case *Jaffee v. Redmond 518 U.S. 1(1996)*, there was almost unanimous agreement that it was in the public good for an individual to be able to talk in confidence to a psychiatrist without having to worry that the notes could later be subpoenaed in court. The justices in fact took judicial notice that privacy was required so as not to chill conversation between patient and therapist.

One of the most puzzling parts of this debate is that many of those arguing for more access all but say that people are too dumb to make these decisions themselves and that they should "trust " the government to tell them what is in their best interest. One federal official, U.S. Health and Human Resources Secretary Donna E. Shalala, has even gone so far as to propose that Americans surrender their privacy to "the critical needs of our health-care system and the nation." Shalala, in her recommendations for implementing administrative simplification, says certain national priorities "should permit the disclosures of health information without patient consent." These "priorities" include law enforcement, cost containment and research that may have nothing to do with patient care and everything to do with economics.

---

[10] "One-Stop Snooping." Editorial. *Washington Post* 19 September 1998: A14.

Interestingly, Justice Louis Brandeis issued a prescient warning 60 years ago in *Olmstead v. United States 277 U.S. 438 (1928).* He wrote, "Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding." It is the opinion of many people, and certainly of National Coalition for Patients' Rights (CPR), that the mandated use of a national health identification number [by well-meaning government offices] will render health-care privacy obsolete.

Twenty-five years ago, a committee initially under the direction of Elliot Richardson advised the Department of Health, Education, and Welfare, (now the Department of Health and Human Services) in a report titled Records, Computers, and the Rights of Citizens.[11] The committee said, in part, "in practice, the dangers inherent in establishing a standard universal identifier…. far outweigh any of its practical benefits. Therefore we take the position that a standard universal identifier should not be established in the United States now or in the foreseeable future."

The current health care environment, widespread computerization, and the marketing of prescription drugs have made our most sensitive personal information a hot commodity. But allowing the free access to our medical histories will not improve health care or society. Patients who feel they cannot be candid with their doctors are patients who won't get top-quality health care. They may delay going for treatment or they may

[11] United States. Secretary's Advisory Committee on Automated Personal Data Systems. *Records, Computers, and the Rights of Citizens*. Washington: GPO, 1973.

be so guarded in the examining room that their doctors are unable to make a proper diagnosis. Insurers will end up spending more money for delayed or inappropriate treatment. Meanwhile, once our medical records are routinely stored on linked computer systems, there will be people (both within government and outside it) who will find ever increasing reasons and rationalizations for trumping our right to medical privacy. The consequences of this will make current medical-privacy violations seem tame and isolated. Quality care and patient privacy are not mutually exclusive. In fact, trust and its prerequisite-private confidential communication-remain the foundation for a good doctor-patient relationship that has always been recognized as essential for quality care.

I spoke at a conference called "The Employers Health Management Association Conference" and was surprised that insurers came up to see me as an ally against the employers. They started to give me examples which gave me some ideas about the confusion that existed over whether the data was being used to improve quality or if it used to lower cost? The particular case of what are called the HEDIS measurements, (Health Plan Employer Data and Information Set) could illustrate this problem. This example also shows why we touted health measurement to try to see if treatment in particular areas, like immunization or asthma, are being done appropriately. An insurer gave me information about when an insurance company is being measured on a particular criteria, like asthma, and that's what's going to be used to rate them. The information, in fact, goes out to U.S. News and World Report, and all these studies are published saying how they're rated. They then focus, they use their data and they concentrate all this extra money to improve getting people with asthma to the emergency room quickly. They gave me data showing that this particular insurance company would send cabs out to get

the people to the emergency room so that particular HEDIS score would come out better. It's difficult to be able to separate, 'What is quality improvement as it's described? And what is really a financial profit and the bottom line?'

IV. Philip Caper, "The Benefits of Appropriate Use of Medical Data"

Dr. Philip Caper is chairman and CEO of Codman Research Group, a software and consulting firm. The company is widely recognized for cost and quality management initiatives based on systems of statistical analysis of administrative and clinical data. His organization has been called by The Wall Street Journal "one of America's corporate stars of the future." He is also an adjunct lecturer on health policy and management at Harvard School of Public Health. He was a staff member of the Senate Labor and Human Resources subcommittee on health, and from 1976 to 1980, he served as vice chancellor for health affairs at the University of Massachusetts Medical Center in Worcester.

The focus of my remarks is going to be on the benefits of the appropriate use of data. We hear plenty about the dangers, and they're very real. Nevertheless, it is important to establish -in our minds at least -the notion that there may be a compelling argument and a necessary argument to use data in an appropriate way in order to improve access to medical care, improve the quality of medical care, and restrain the rising cost of medical care. I believe these are the primary obstacles to the creation of national broader health insurance programs. If our objective is to try to broaden access to medical care, the cost problem simply to be controlled.

Although I started out as a clinician, my career has always been focused on the delivery of medical care to populations. As a staff member of the US Senate I worked in the early 1970s on national health insurance, HMO legislation, health planning legislation and other ways of improving the management of medical care in the public sector. I moved on to become a manager in a public-sector academic medical center,

UMass Medical Center in Worcester and ran the hospital for about four years, and was chief of the medical staff. I then moved back to academia, where I taught at the Kennedy School's health policy and management program for about four years in the early 1980s.

It was in the mid-1980s that I founded the Codman Research Group, primarily to take advantage of the growing availability of data and the growing power of both analytic techniques and computer hardware and software in manipulating data. At Codman Research, we try to convert the principals of epidemiology into management tools for a health care system I saw to be increasingly in need of management. We are improving our ability to manage medical care delivered to defined populations- though not as quickly as I thought we would. In 1971, Elliot Richardson predicted that 80% of Americans would be enrolled in HMOs by the year 1980. That hasn't quite happened, but we're getting closer.

I also believe that managing this medical care enterprise is a good thing. It's too large, it's too expensive, it's too important, and it's too highly specialized and fragmented not to be managed if we're to control costs and in a systematic way learn how to better deliver medical care to defined populations. We currently spend about one and a half times per capita what any other country in the world does on medical care. I think for that price, we have obtained some of the best technology in the world. We have a long way to go in the way we organize services so that people have access on anything approaching an equitable basis. Structures and techniques for managing medical care are certainly an important part of the solution to that problem.

What's happened as we've moved from a cottage industry into large and complex enterprises to deliver a broad range of medical services is that the culture of medicine has

begun to change, and the vocabulary of medicine has begun to change. We've changed from a focus on doctors and patients- which is all we could see in a fee-for-service system, since any data which showed up was basically a result of an encounter between the doctor and the patient- to a focus on defined populations like members of health plans. In this context I see the most powerful and the most beneficial applications of database management, accountability and quality assurance structures.

Here are just a couple of examples. This is difficult because we're dealing with a lot of imperfections in data which are very poor and which require a lot of tedious, expensive, and certainly frustrating work to translate into reasonable information. Since entering the private sector I found that once the power of that information is demonstrated, it feeds a process of continuing to develop these tools. Among our clients, for example, are a number of state Medicaid programs, which for the first time are beginning to measure systematically the rates of avoidable hospitalizations among Medicaid populations. Measuring rates requires a numerator and denominator, rather than just a number of events. And what we find is wide variations in the rates of hospitalizations for various conditions. One program in particular has begun to document savings achieved by reducing the number of avoidable hospitalizations through improvements in the primary care system. It has used that argument to go back to the legislature to in this particular state and argue successfully to apply those savings to an expansion of eligibility in the program. That's one example of a policy initiative that would have been impossible without the appropriate use of information.

Other clients are looking in a systematic way at the rates of emergency room use by asthmatics enrolled in their plan. That type of systematic monitoring would not have

been possible in a fee for service system. We are finding large variations depending upon cohort. There is a lot of interest in fraud, waste and abuse, which requires data to detect. Fraud means billing for something that hasn't been done, and abuse means billing for something you have done but which may not have been necessary. Waste means providing services which, although they may have some justification, have a very low cost benefit ratio. It's in systematically identifying those kinds of problems in the medical care system that I think we're going to get to the level of efficiency which will allow our continued expansion of benefits to the growing number of Americans without health insurance.

Finally, of course, there's quality improvement and outcome monitoring. Outcomes analysis, by its definition, requires longitudinal monitoring of what happens to cohorts of patients following treatment. What happens to a particular patient or cohort of patients simply requires individual identifiers. It does not require identifying the individual by name. It does require that you have an identification system capable of linking events to an individual, even though you may not know who that is. But I think there are ways of protecting the actual identity of individuals and still achieving the objective of being able to use these large databases for providing information about how more effectively to deliver medical care. Much of the benefits of the use of data, at least in medical care do not require identifying individuals. You don't have to be able to tell who somebody is. As I said earlier, it's very useful to be able to tell when an event happens to the same individual, but you don't have to know who that person is. Therefore, a lot of the concerns here may be addressed by focusing in a very targeted way on protecting the information we're most concerned about being misused.

One of the reasons this debate has gone on for so long (it was an important part of the debate when we were developing the National Health Planning legislation in 1973 through 1976) is because there are legitimate arguments on both sides. There are legitimate concerns about abuses of the availability of information. And there are legitimate benefits which may be compelling if we're to achieve other objectives for the use of data. But my message here is that this is not a black and white kind of issue. Just because a tool can be abused doesn't necessarily mean you outlaw the creation of the tool. You have to be very careful about safeguarding how it's used. That's the kind of situation we're faced with here.

The further we get into this debate, the more it's going to become evident through work of our firm and others like us, that there are very important and perhaps critical uses which will require the availability of data. On the other hand, as Denise Nagel has said, there are very real dangers to be avoided. We just have to chart a course among these benefits and dangers.

It seems to me that in many ways, the least danger lies in government databases. This is because they're visible, they're controllable, and their uses and access to them are publicly visible. My concern is with the privately accumulated databases, the ones over which there are no controls. I see this as a much greater danger in our society. I think it's going to be very difficult to stop this collection of data, given the advanced state of technology. It's also very difficult, particularly, in the private sector, to control ways in which it's used. A simple example, I order things through catalogs occasionally, L.L. Bean or Land’s End, and suddenly I'm deluged with catalogs from companies that I don't know. I don't remember giving anybody permission to sell my name to anybody else.

How does one control that? I suppose there are ways of passing laws, of prohibiting that kind of behavior.

I'm interested in national health insurance, and have been for 35 years. And I've found that any time anybody wanted to protect the status quo, they call for more studies. I'm convinced that our failure to be able to enact a national health insurance program is not due to a shortage of studies or data. It's a problem of a lack of political consensus. And that will never be solved by additional studies, no matter how many you do.

When there's an attempt to implement a simple solution to a complex problem, there's something called a law of unintended consequences. Often, attempts to fix unintended consequences show us how laws become more and more complex.

I think there have been and will be significant benefits to be gained from the appropriate use of information. I think we have to be very concerned about throwing the baby out with the bath water in attempting to address even very well founded concerns about confidentiality. I believe it's possible to put such draconian limitations on the use of data, that we lose all the benefits and potential benefits that can be obtained through using it. There's a big difference between passing a law that says, "Before any piece of data or any individual can use that particular instance has to receive permission of that individual for that use." Or having somebody when they sign up for a health plan or an insurance policy or whatever, say that I give permission for my information to be used for purposes of management, quality control and access as long as I'm not personally identified. These are political issues that have ethical values, and different people have different values. It's the process of hammering those differences out that is the core of these debates.

V. Harold Bursztajn, "Questions about Confidentiality in Managed Care"

Dr. Harold Bursztajn teaches, testifies and consults nationally on medical decision analysis, clinical ethics, general and forensic psychiatry. As a psychiatrist, he is associate clinical professor in the Department of Psychiatry at Harvard Medical School, co-director of the program on Psychiatry and the Law at Harvard Medical School and has had clinical appointments with Beth Israel Hospital and Massachusetts Mental Health Center. Also involved in risk management services, Dr. Bursztajn is co-author of the book Medical Choices and Medical Chances: How Patients, Families and Physicians Can Cope With Uncertainty.[12]

When I asked how much time I had to speak, I was told nine minutes. So, welcome to managed panel care. Now, the good news is, I was told about the time I would have. It's a case where what you see is really what you get, or what you were promised is what you get This is the way managed health care should work. However, all too often you promise nine minutes, and you are told that only three minutes are actually necessary. Basically, the benefits you are entitled to, because you paid your insurance company for them, are deemed to be either medically necessary or medically unnecessary, irrespective of whatever agreement you and your doctor have reached about your use of those benefits. And this is an area where the databases really come in. The prime area that I'll be focusing on today is the manner in which databases can be abused to take away from people, deny them what they've been promised, because it's supposedly unnecessary, and you are told you only really need three minutes.

[12] Harold Bursztajn, et al. *Medical Choices and Medical Chances: How Patients, Families, and Physicians Can Cope With Uncertainty*. New York: Delacorte, 2001

This is an area of abuse, which has to be studied, has to be considered in any potential legislation. Otherwise what we give is a very powerful tool, not for the goals that Phil Caper works for, in cost control or quality control. But for the goal of profit maximization at the expense of health care. This is all of our concern if databases will be used to maximize profit rather than to maximize the quality and access to health care. I'm going to focus on something that I consider to be some of the major questions that need to be answered before any national health care database is implemented. And that's not by simply debate, but by empirical study.

First, how do we leave control in the hands of patients and allow for informed consent when data are entered into databases? The way in which I exercise control in my consulting group is to make sure that my patients see anything, that goes out of my office to any insurance company. Nothing gets sent out unless it's given to the patient, we review it, and then the patient literally sends it out. I give people stamped, self-addressed envelopes. But that’s possible for the psychoanalyst in Cambridge, but is it really realistic when you look at every busy clinic in Roxbury?

This is an area which I've become very familiar with from being called to testify as an expert in a variety of managed health care cases. When these cases invariably get settled, I can't talk about them, which is really frustrating. What happens is you have managed health care organizations setting up profiling systems for health care providers. They then proceed to penalize you for hospitalizing or for getting a consultation on a psychotic, depressed, suicidal patient. The patient goes ahead and kills himself. Subsequently, both the physician and the managed care organization is sued. The managed care organization proceeds to deny responsibility and say it is protected by

ERISA, because its not really in the practice of medicine, per se. But then when you obtain their profiling system, and you see the extent to which they substantially control by a series of incentives, the kind of health care that's delivered, the case eventually winds up being settled with a gag clause attached to that says you can't discuss it.

Second, how do we prevent managed care organizations from using databases for enrollment and disenrollment of high quality health care providers through a practice which I call "predatory profiling?" Let's say you're not enrolled in one of these bad managed care plans, but you're enrolled in one of those good managed care plans that gives you first consultative services. The problem is that the bad tends to drive out the good very often in health care and the health care system. The extent that we can do it for you cheaper becomes the message that gets sent to the employer. Good health care providers then wind up leaving many of these health care systems because they really don't need this headache.

The best studies that we have show that if 30% of your patients are enrolled in a poorly managed care system, all of your patients get the same level of care. Let's say you go ahead at Harvard Law School and negotiated, and paid for high quality health care. What happens is that if you go to a doctor who sees 30% of the patients in a poorly managed care system, you will get the same kind of quality of care as everyone else does. It's fair, in a way, except you don't get what you pay for. It's like, you buy a first class ticket, but you still get coach, because that's what everyone gets in this particular system. How do we go ahead and avoid this kind of pattern of predatory profiling, which really drives quality down, and serves to maximize profit?

Third, how do we protect patient confidentiality from employers? The Americans with Disabilities Act aside, employers have access to these databases. And well before they get into a hiring decision, they make sure that they structure the interview process in such a way that they don't have to worry about Americans with Disabilities.

Fourth, can patients access their own data? I'd like to know what other people know about me, especially when it comes to health care.

Fifth, can patients opt out from being included in databases? If I really don't want to go ahead and have my information entered into that, do I have that choice? Is there an informed consent process?

Sixth, how do we create an informed consent process which would be adequate to informing patients about the experimental nature of health care databases in terms of their potential negative as well as the potential positive impact on patient health care? Can we imagine a real informed consent process? Because if not what we have is basically a situation that was covered in 1948 by the Nuremberg Code of medical records. It said that when you were doing any procedure that is experimental, and you are doing it on a group of people who have no choice about it, they are a captive patient population. Most people today don't have choice of health care available, have only one health care plan. Then you give those people the opportunity to say yes or no freely as to whether they want to be participating in an experimental process. And to the extent that what we are talking about a national health care databases is still experimental, we don't know at this point what the positive and negative consequences are going to be. Shouldn’t people be given a choice as to whether or not to participate in such an experimental process?

Seventh, how often do we pass laws before we do this study, and identify what might be some of the unintended consequences? In medicine, the National Institute of Health funds research about procedures that it is very interested in. When it comes to this area, who defines the research as to what will be the consequences of the data. And if people and organizations have a direct self-interest in the outcome of their research, it's as if all of the research on drugs was funded by drug companies and no one else. Under those circumstances, you have very unbalanced sets of research agendas and research realities. And there isn't enough reliable data as to what might be the research from not self-interested service. Do we have the data from unbiased sources which are not funded by the industry as to what the effects are going to be of a national healthcare database? If so, I'd love to go ahead and have access to it.

Eighth, the National Institute of Health funds research about medical procedures that we are very interested in. When it comes to who defines the research as to what will be the consequences of these databases besides people and organizations with a direct self-interest in the outcome of their research? It's almost as if all of the research on drugs was funded by drug companies and no one else. Under those circumstances, you have very unbalanced sets of research agendas and research realities. And there isn't reliable data on what might be the research results from not self-interested sources.

Ninth, on the dimension of voluntariness of these databases, how much is it in your control? As we progress technologically, we have more and different kinds of data are being collected. Telemedicine is becoming one of the major consultations areas of my practice Telemedicine provides the entire record of the doctor-patient interaction on line and accessible. . What do we do with it? And if you have a national database, that

interaction becomes potentially accessible to anyone under any circumstances. So what kinds of safeguards do we build into our system to make sure that whatever happens is still voluntary, that it preserves an informed consent process in the doctor-patient relationship? My concern is that we get to debate, and people get to do values long before we actually have the data. So much of what seems to be ethical conflict is often talking in a vacuum where there is vast amount of uncertainty as to what the consequences might actually be of a proposed model. I began long ago with physics where if you couldn't do the experiment, you at least did a gedank [thought] experiment. But in many medicine we do have the means for doing simulations of some of these things. And we do have the means for studying, though we often think these are not able to be studied. The values are important. But we really do need to have better data than we do before we go ahead and create this vast system of a national health care database. History was changed because of a privacy issue, Watergate. That was all about someone's privacy being invaded. And how we can do something about our medical privacy being invaded by government databanks.

VI. John Roberts, "Security in Government and the Private Sector"

John Roberts is the executive director of the American Civil Liberties Union of Massachusetts. He was community relations director of the ACLU affiliate in Chicago where he was also involved in the Community Renewal Society. He is the chair of the board of directors of the Massachusetts Immigrant and Refugee Advocacy Coalition. His degree from Union Theological Seminary provides another perspective on these medical and legal issues.

When the United States Constitution was written, people kept their papers and private effects in their homes. That is why the Fourth Amendment reads the way it does: "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated." Privacy violations in those days usually consisted of British troops storming through the door and searching the homes of colonists.

Now, almost none of our private effects are in our homes. Our information is in financial institutions, credit Bureaus, medical complexes, insurance companies, various data bases in educational institutions, commercial retail companies, and of course in various government data bases, from the IRS, to perhaps the FBI (depending on our politics and what we were up to when were young and idealistic).

Trading in information is big business. Retailers want to target their markets, so they want information on your buying habits, income, and education level. Insurance Companies want medical and genetic information so that they will know who not to sell insurance to. There are many others who want your medical information: researchers, public health agencies, pharmaceutical companies etc.

With all this information now in computer data bases that can be called up with the flick of a finger, the next step, of course, is linking the data. The idea is to give everyone a number or some unique identifier that will make it possible to easily link data ... we can bring together financial, medical, criminal histories, education, political affiliation and other pertinent information. We can build profiles and try to predict what people will do. We can get a profile of potential terrorists, drug- traffickers, sex offenders, after all we want security, right? We can also profile potential high spenders and what they will spend their money on because we can profile their buying habits, based upon their street address, and the car they drive (which reveals their buying power).

Or better yet, perhaps we should have national identity cards so employers can make sure they are only hiring people who are citizens or have the proper immigration clearance to work. National identity cards would certainly help control crime ... it would give police a means to fix identities in their criminal investigations, and would be a legitimate request for a police stop. "Let me see your ID card," or as some call it, your domestic passport.

Retailers could require the use of identity cards to make purchases with credit cards. All the better if the identity cards are "smart cards" that contain on their magnetic strip all kinds of information about the card's holder. Since the holder will probably not have the equipment to read the smart card, that person may not know the scope of information on the card that is easily accessible to merchants, police, or any one else who wants to use the smart card for identification.

You get the idea. It's the society that craves law and order, that places security above liberty that this all makes sense to. There have been and are such societies ... We like to think we are not one of them. We do not have a unique identifier yet, nor identity cards, but we are damn close, and moving closer. The social security number, which was created for the sole use of the Social Security Agency (SSA) for the administration of a federal benefits program, has become sort of a unique identifier**.** Think how often you are asked for your social security number in both the public and private sector. In most instances those requesting it have no authority to do so, yet most of us blithely give it. How secure is your social security number?... not very. Senator Dianne Feinstein testified before Congress that it took her less than 3 minutes on her computer to search and call up her own Social Security number (SSN) from the internet.[13]

At several points government agencies, from the SSA itself, to the Justice Department and the old Department of Health, Education and Welfare have studied the issue of a unique national identifier and in each instance have rejected it as anathema to our liberty interests. Congress even passed the Privacy Act of 1974, which prohibits new uses of the number unless Congress itself authorizes it. Congress specifically declared its opposition to the use of SSN as a unique identifier. Yet we march ahead in a kind of unofficial way, linking data to the SSN, and the federal government is one of the greatest culprits in expanding the use of the SSN as a national identifier. For instance, they now require children to be given SSN for use on IRS forms.

Further, the government also shares its information on individuals with the private sector. In fact private sector entities have access to at least 79 of the largest federal data

[13] United States. Senate. *Testimony of Dianne Feinstein*. Washington: GPO, 8 August 1997.

bases, and those are just the ones we know about. The FBI's criminal history records system, which initially was limited to law enforcement purposes, is now being freely used by employer and licensing boards. In fact half of the requests the FBI receives for criminal histories today are from private sector employers.

Sometimes there is a rebellion that puts the brakes on the march toward a national identifier. Several years ago, you may recall, Equifax and Lotus Corp. announced the development of a product called "Lotus Marketplace". It was advertised as containing personal information about 120 million Americans including age, address, income, gender, marital status, and spending habits. Through inquiries about the product a computer privacy organization discovered that the information provided by Equifax to Lotus was keyed to the SSN. Public outcry convinced Equifax and Lotus to abandon the project. The same thing happened to TRW's [credit bureau] plan to market a similar product called "Social Search." But you know that similar databases must exist even it they are not available as a commercial commodity.

Further, the SSN is a notoriously unreliable identifier. Of the over 210 million SSN's in use today, about 75 % were issued before evidence of age, identity, and citizenship or alien status were required. Only 76 million of the initial and replacement social security cards have been issued using the new counterfeit and tamper-resistant paper, so that most cards in use are easy to alter or forge. And, there is no method to positively assure that any person presenting a social security card is the person to whom it was issued since all that the card contains is a name, an SSN, and a signature. So, we

have a Congress that says it does not want a national identity card but is creating one in the SSN which is rife with false data and is fairly unreliable.

One marvelous illustration of how the system became so polluted is the true story of the company that marketed pocketbooks and wallets. The company placed a replica of a Social Security number card in each of its products. Thousands of people bought the wallets and pocketbooks, but not understanding that the SSN card was a replica used to illustrate how such cards would fit in the product, used that SSN as their own number on their IRS forms. Although this happened over a decade ago the number still shows up each year on countless IRS forms.

The private sector has latched onto the SSN because so much data is already linked it. Its not all that perfect but its all they've got. We are all facilitating this process by adding information to our SSN dossier, and great amounts of money are being made trafficking in this information. If you really want to understand how to work the system to find data through the use of the SSN talk to a private investigator. They are masters at using the SSN to track people, gather data and conduct surveillance. They will also document how SSN crime is increasing in the US. The stories are legion of how criminals are using SSN to control other peoples' credit cards, collect their benefits, and literally take over their identity.

Now we have the specter of the creation of a new unique identifier by the health care industry to track medical records ... should administrative simplification become a reality. That could supersede the SSN as a universal identifier because virtually everyone will have a number, and it will be a more reliable identifier. What can we do about all

this? Before the horse is completely out of the barn, we have to find ways to shut the door.

If we define privacy as the ability of an individual to control the dispersal of his/her information, we must have the protection in law to accomplish that. It will take more than the sweeping language of the Fourth Amendment to protect our privacy interests ... it will take more specific statutory language. ACLU has started what it calls a "Take back your data campaign." It smacks a bit of trying to get the horse back into the barn, but we have to try. It is a call for the development in law of privacy rights based on the following principles:

> 1. Your personal information should never be collected or disseminated without your knowledge and permission.
> 2. Organizations must let you know why they're collecting your information; and they can't use it for other reasons than the one you granted permission for (unless they get a second permission from you).
> 3. Organizations must ensure the privacy of the personal information they collect or maintain on you, retaining only what is necessary information and only for as long as it is needed.
> 4. You should have the right to examine, copy, and correct your own personal information.
> 5. There must be no national ID system - either in law or in practice.
> 6. Unrelated databases must be kept strictly separate so information can't be cross-referenced.
> 7. Personal "biometrics" data - your fingerprints, DNA, retina or iris scans, etc. -must not be involuntarily captured or used (except for fingerprinting criminals).
> 8. The government must not prohibit or interfere with the development of technologies that protect privacy (such as encryption).
> 9. These principles should be enforceable by law. Furthermore, no service, benefit or transaction should be conditioned on waiving your privacy rights.[14]

The military gave us one of the great illustrations of the possible abuses of smart cards. Following the Vietnam War, people had various grades of discharges, honorable, general, less than honorable, whatever. And tied to those discharges, unbeknownst to the GIs, unbeknownst to the people who sort of owned those discharges, were codes, I think they were called "spin codes," which employers knew about and insurance companies knew about, and all kinds of people knew about, codes which indicated that if it was less than honorable, say general discharge, what the problem was, whether there was psychiatric problems. They even had bed wetting as one of the sort of spin codes. And when that, it was a huge hew and cry on that when that was found out. It was one of the great illustrations about privacy is that somehow employers and everyone else knew about information about you that you didn't even know about. And this is the problem with the smart card and the military. Thank the military for giving us a wonderful illustration of the abuse.

Finally we have to learn how to be privacy guerrillas. We have to learn how not to cooperate with those who seek our personal information, how to say no when asked our SSN, and not to fill our every questionnaire given to us when we purchase a new refrigerator, or TV set. Be careful of information you put out about yourself over the phone or on the internet or even email. Be careful about giving out your credit card number over the telephone or through the internet. Don't cooperate, fight Administrative Simplification. Be an obstructionist. It's the least we can do until we get more protection in law.

---

[14] American Civil Liberties Union. “ACLU Take Back Your Data Campaign.” February 1998. 12 February 2004 http://archive.aclu.org/action/tbyd.html.

VII. Molly Shaffer van Houweling, “Learning from a Cyber Course on Privacy”

Molly Shaffer Van Houweling graduated from Harvard Law School in June 1998. She came from the University of Michigan where she was a political science major. Between college and law school, she worked with the U.S. Department of Commerce in technology administration. At Harvard Law, she was articles editor for The Journal of Law and Technology and the head teaching fellow for the Berkman Center's cyber course "Privacy In Cyberspace."

My brief remarks on the subject of privacy and government databanks reflect what I learned as head teaching fellow for the Berkman Center’s inaugural online lecture and discussion series--"Privacy in Cyberspace," taught by Harvard Law School professor Arthur Miller. In this Internet experiment, over 1000 participants from all over the world and all walks of life engaged in online discussions with each other, with Professor Miller, and with guest experts. The cyber course was organized around a series of hypothetical questions that the students have been talking about in online discussions with professor Arthur Miller and teaching fellows at Harvard Law School. Much of what I've learned about privacy and Internet privacy issues occurred during the cyber course discussions with students online about general issues of government and other databases.

As we discussed Website privacy policies, online data collections, electronic medical records privacy, and other Internet privacy topics, several themes emerged that strike me as relevant to today's discussion of government databanks and to the specific issue of national identification numbers for medical records. First, the discussions revealed many participants' willingness to share some personal information in exchange for expected benefits. For example, most participants were comfortable revealing their

email addresses, names, and occupations with the Berkman Center in exchange for participation in "Privacy in Cyberspace." Many people thought that the information we asked for was pretty innocuous. In fact, the e-mail address is the only piece of information we required, because it was what we needed to communicate with the students. Other students who did have misgivings about giving even their e-mail address, their occupation or their hometown, were willing to trade off that information for what they thought they'd get in return, a chance to participate in this experimental course. They mentioned that they would be more concerned about information like Social Security numbers or medical information, which they've learned to be more careful about sharing.

In the first week, we started not with a hypothetical , but with a real life question, asking people what they thought Harvard Law School would do with the data that they had submitted when they signed up to become members of the course, including their names, occupations, and e-mail addresses. We thought that maybe we'd get people scared about the awful things we might do with their information. However, there were a variety of not so scared responses to this scary scenario that we posed. And they broke down along a couple of themes.

At the same time, many participants were uncomfortable with the prospect that the many individual pieces of personal information that they had shared with organizations like the Berkman Center might be compiled together into more complete personal profiles and then sold or given away to third parties. Many were disturbed to discover how much information is currently available online about themselves and others.

During the second week, in fact, students looked at some more complete databases of information to see what they could discover about themselves and others on the Internet. This is where things got a little more interesting, because people discovered that the seemingly innocuous information that they had entered when they registered for a television warrantees, when they logged into other places on the Internet, actually was being compiled by people with the profit motive to put these little pieces of information together into megadatabases of information. This? presents a surprisingly complete portrait of people who've just given little bits of information at different points.

And as students explored these databases of information about themselves and thought about the implications of freely giving information to institutions like Harvard, one thing that emerged was that it's pretty hard to take their data back. After that session, students took a little more pause about seemingly innocuous pieces of information.

Other concerns that were raised when looking at these more comprehensive databases of information were not just that the information there may be potentially damaging to people's privacy. But there is also the concern that the information could be inaccurate. This was especially so given the strategy that some people have of protecting their privacy of giving inaccurate information when they're asked for it. Some students wondered whether this might destroy the profit motive and therefore would be ultimately a protection of our privacy. But other students were concerned about having access to databases about them, so they could correct inaccuracies and make sure that if information was being used against them, that at least the information was accurate.

Later we looked at medical records, which from the beginning of the course people had indicated was something that they were particularly concerned about. Again,

people were concerned that the information about them residing in these databases might be inaccurate. In the medical records context, they were especially concerned that decisions by doctors, and insurance companies might be made on the basis of information to which the patients didn't have access to and didn't have any assurance it was accurate.

Again in the medical records context the theme emerged of the tradeoff that people expect when they give information. In the medical records area, this is especially troubling. Feeling pressure to sign a form that waives secondary uses of your information that not only lets your medical records be passed on to your insurance company, but also to the employer who's providing that insurance-- raises questions about whether the tradeoffs that we feel we have to make are actually fair and actually necessary. Aren't there are instances when we should be able to say no to those tradeoffs?

Students were also concerned about the possibility of human error. After discussing encryption and other technological means for securing privacy and electronic information, students were skeptical that electronic means would protect privacy. Combining the human database operators and health care professionals who don't have experience with the technology with others who claim to need access to information as it goes from health care provider to insurer to employer, technological protections won't necessarily protect us.

A recent forum that Harvard Journal of Law & Technology hosted about "Privacy, Property and the Family in the Age of Genetic Testing," touched on these issues.[15] A panel then on the uses of genetic testing information raised a concern that, once genetic screening is required for various purposes, it will be difficult to resist its use

for other purposes in the future. And I think that the potential danger of a national unique identifier is that once we have this tool, it's hard to predict how it will be used. Many actors, public and private, have the incentive to abuse such a system, and rules against such abuse will be difficult to enforce.

Another theme that emerged during the cybercourse was that it's difficult to tell, once your information is released, who among the various people who have access to your information is the culprit. That makes it all the harder to enforce laws that we might make about secondary uses of information. And in the privacy area, this is especially difficult, because a violation of privacy can happen even if you never find out, even if the information wasn't used to discriminate against you. People were troubled when they found out the various actors that had access to their information, and were troubled about not knowing about all the people who do.

The two observations--that people are willing to reveal personal information in exchange for perceived benefits, but that they are not comfortable with unlimited subsequent use and compilation of that information--highlight a key concern with national medical identification numbers: These could facilitate compilation of personal information and hinder individuals' efforts to control exactly how much of that information is shared with their internists, their psychiatrists, their insurers, their employers and their families. All of this is in a context in which the benefits at issue are crucial, and the incentive to share information despite misgivings about privacy commensurately great.

---

[15] *Symposium* "Privacy, Property, and the Family in the Age of Genetic Testing." *Harvard Journal of Law & Technology*. 11. 3 (1998).

Because the other panelists have described the possible abuses of national medical identification numbers, I would like to focus on another issue that arose during the cybercourse "Privacy in Cyberspace," the so-called state action doctrine. This is the idea that the Constitution generally applies only to the government--that your neighbor doesn't violate the First Amendment when she refuses to let you give a speech from her front porch, that you can't sue her under the Fourth Amendment when she peeks with binoculars into your bedroom. When we discussed this concept in "Privacy in Cyberspace," several participants were surprised and dismayed to learn that there is so little protection, constitutional or statutory, against collection and release of their personal information by private actors--privacy invasions that they considered just as worrisome as invasions by government actors.

A contentious issue in this area of the law is the degree to which the government should be held constitutionally responsible for establishing legal regimes--based, for example, on property or contract law--that facilitate censorship and invasion of privacy by private actors. My neighbor doesn't violate the First Amendment when she kicks me off of her porch, but can I bring a First Amendment challenge to the government-imposed trespass law that backs up her action? The Supreme Court has generally, but not unequivocally, answered such questions in the negative.

Just as it is now difficult to get courts to recognize the state action inherent in long-established laws of property and contract, we can imagine a future in which invasions of privacy made possible by national identification schemes now under consideration are similarly dismissed as mere private actions, raising neither constitutional concerns nor claims under statutes like the Privacy Act of 1974. But the

interest that private actors have taken in this debate evinces the increased power over personal information that the schemes being considered would give them--power that they could probably not amass absent government action. The role of government here, and its constitutional implications, should be closely examined. And it is now, when the government's participation is so undeniable, that constitutional concerns are most likely to resonate. That's why today's discussion is so important, and so timely.

Professor Nesson initially noted that cyberspace isn't that much about law at all. And I think that's right. That's something that we talk about here at the law school a lot, about the other things that control cyberspace. Standards are one thing that control cyberspace, and our discussion today is really about a standard, whether we will use a standard way to identify medical information. And we found that we can't always undo the work we do with standards, with laws, because laws respect jurisdictional boundaries. And laws and law enforcers can't always discover the violations of our privacy that we would like to avoid.

The Berkman Center's research philosophy is based in part on the idea that technology is not a neutral platform on which we build pubic policies. The shape of technology is commonly the result--though often unintended--of public policy choices. We need to keep this in mind both when we examine the current state of technology and when we implement policies that might change it. This discussion has been in keeping with that mission.

VIII. Richard Sobel: "Reflections"

Political scientist Richard Sobel moderated the panel discussion about Privacy in Cyberspaces as a Berkman Center Fellow. Previously he was a Fellow at the Shorenstein Center on Press, Politics, and Public Policy in the Kennedy School of Government, and he taught at Princeton University. He is the author of two books and "Not For Identification Purposes," which appeared in the on-line journal of the Berkman Center titled Filter. In the Spring of 1998 he also participated in Professor Arthur Miller's cyber course "Privacy in Cyberspace." He wishes to thank Mark Wasielewski, Bruce Knobe, Evan Hinkle, and the Lincoln Filene Center for assistance on this report.

While this discussion ably focused on the privacy issues around health care information, it extended beyond one government scheme for data collection and identification. Examining health care issues not only raises intimate questions about the essential nature of medical confidentiality, but also, by exemplifying concerns about government databanks and identification schemes, it brings forward more general issues about government intrusions. Each government databank or ID scheme raises fundamental issues about the relationships between government and citizens, real and cyberspaces.

There are three major reasons why government is the central element in the discussions here. First, government has the power to coerce people and to control their lives. In many subtle and not so subtle ways, this is the power that individuals confront when they do or don't do what the government directs. That's the nature of the state and why democratic constitutions are developed to circumscribe that power. Because governments derive their just powers from the consent of the governed in a democratic

system, the proper balance of citizens and state becomes distorted when government bestows and deprives identity through documents, numbers, or places in databanks.

Second, because our Founding Fathers responded to a long train of British government abuses, they developed a Constitution that embodies principles that afford protection against government power. These include the protection of federalism, the familiar principle that power must be divided among different levels of local, state and national government: They also constituted the separation of powers that divides authority among the competing and cooperating legislative, presidential and judicial branches of government. In short, both principles of federalism and separation of powers remind us that centralized power is a danger to a democracy.

Federalism and separate powers are essential because the Founders saw that administrative efficiency and political expediency may endanger democratic government. Powers should be divided and controlled. Because centralized databanks create problems with centralized information for a federal system, examining these databanks means addressing issues of concentrated power. Trying to justify a "unique health identifier" as "administrative simplification" raises exactly the concerns for centralization of power that the Founders feared. Similar concerns appear in the recent reports of the Chief Justice of the Supreme Court and of the American Bar Association Judiciary Committee that federalization of criminal laws is centralizing power and distorting the political system.[16] These fundamental constitutional issues explain, in part, why this panel emphasizes government databanks.

[16] William H. Rehnquist. "The 1998 Year-End Report of the Federal Judiciary." 1999. 5 February 2004. <www.uscourts.gov/ttb/jan99ttb/january1999.html>

Third, this panel focuses on government because of the constitutional protection provided particularly by the Bill of Rights. There's a lot of privacy in the Constitution: in the Preamble, in the First Amendment, in the Third Amendment, in the Fourth Amendment, in the Fifth Amendment, in the Ninth Amendment, and in the Fourteenth Amendment. The Preamble calls for securing the blessings of liberty; the Bill of Rights promotes free expression, and protects against illegal searches and self-incrimination. Those Ten and the Civil War amendments establish citizens' rights and sustain liberty and property against arbitrary governmental actions.

The course of American History, and particularly the American Revolution, is intimately tied to the securing of these principles, protection and rights. For instance, the American response to colonial rule derived in part from the British use of "Writs of Assistance"—general search warrants authorizing soldiers to go anywhere to search for any contraband. The Fourth Amendment was created to require that any encounter with officials, police or soldiers, may not occur until there is a specific reasons to search a particular person.

The principles in the Fourth Amendment extend to the idea that information about an individual sought by government in a search of personal records should not be available without probable cause and due process. There needs to be particular and compelling governmental reason to invade a particular person's privacy, including informational privacy. Each of the other constitutional principles and protection derives from the lessons of history about protecting individuals against governmental abuses.

Today government data collection extends well beyond medical ID numbers and SSN databanks to other major collections tied to identification schemes. There's a pilot

databank set up by the immigration laws.[17] There's also a new hire databank set up by the welfare reform act.[18] There's even a passenger profiling system set up for airline travel.[19] These keep track of where people live, when they change jobs, and where they travel. The first and last are linked to requirements for governmental identification for permission to work or to fly. The immigration and welfare databanks are keyed to the Social Security Number as a de facto national identity number.

The discussion here of privacy and data collection was neither restricted to the health care nor to government databanks, as the last two panelists reveal. Yet constitutional protections that are essential regarding government data banks typically don't apply to the private sector unless there is an issue of state action.[20] Principles of Fair Information Practices and privacy do, however, apply there.[21] A fundamental principle behind information privacy is that an individual has the right to consent to the collection and use of information about him or her. Questions about accuracy or control once the data are collected neglect the issue of whether the information should be collected in the first place. Preventing the collection of information protects privacy more effectively than restrictions on use or dissemination afterwards. In short, the ability to opt in or opt out is essential to informational fairness and privacy. Cyberspace amplifies the need for both public and private protections because data today travels huge distances at lightening speeds.

---

[17] IIRIRA, Pub.L.No.104-208, 110 Stat. 3009-546 to 3009-724(1996).
[18] United States. Cong. House. Welfare Reform Act of 1996. 104th Cong., 2nd sess. Washington: GPO, 1996.
[19] "CAPPS II Privacy Act Notice." The Department of Homeland Security On-Line. 5 February 2004. <www.dhs.gov/dhspublic/display?content=1115>.
[20] Uniform Trade Secrets Act 18 U.S.C. 1905; Federal Reports Act 44 U.S.C. 3501.
[21] United States. Secretary's Advisory Committee on Automated Personal Data Systems. *Records, Computers, and the Rights of Citizens*. Washington: GPO, 1973.

These discussions of privacy, in short, raise important principles and practical issues. This panel focused on the medical aspect to privacy and touched on further questions about government databanks for thoughtful inquiry. Other forums need to further address these issues and larger questions about the essential nature of privacy, both in the public and private spheres. The debates initiated here will hopefully inspire continuing inquiry and searches for ways to address social problems while protecting, indeed enhancing, our privacy and our constitutional rights.