PUBLIC IMAGE

by Larry Hunter

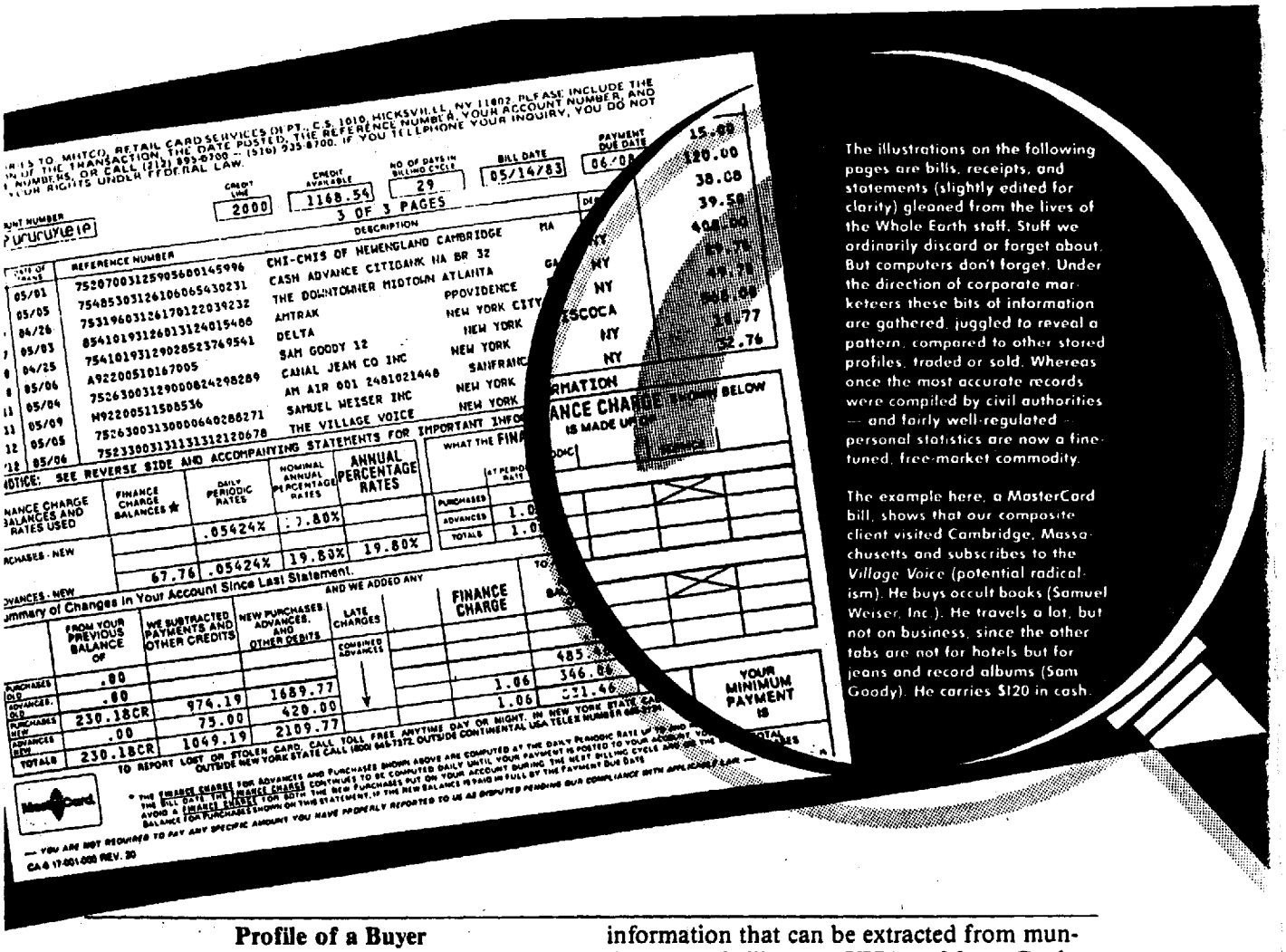
Every day you give out evidence about yourself. Computers can merge these clues into a remarkably complete image of your habits, identity, and thoughts.

Headed for a PhD in computer science, Larry Hunter has been playing with computers since he was ten. He uses a powerful, state-of-the-art workstation at Yale and telecommunicates to it from home on an itsy-bitsy lap computer. The encompassing reach of computers which he describes in this article has made two differences in his own life. It has granted him computer expertise to assist his favored local politicians in their campaign strategies, and it has frightened him into the habit of keeping his paper-life to a minimum, and withholding his ID and Social Security numbers from anyone who does not legally require them.

—Kevin Kelly

I LIVE IN YOUR FUTURE. As a graduate student in Artificial Intelligence at Yale University, I am now using computer equipment that will be commonplace five years from now. I have a powerful workstation on my desk, connected in a high-speed network to more than one hundred other such machines, and, through other networks, to thousands of other computers and their users. I use these machines not only for research, but to keep my schedule, to write letters and articles, to read nationwide electronic "bulletin boards," to send electronic mail, and sometimes just to play games. I make constant use of fancy graphics, text formatters, laser printers — you name it. My gadgets are both my desk and my window on the world. I'm quite lucky to have access to all these machines.

But with this privilege comes a certain sobriety: I've begun to contemplate some of the effects the computer will have on society. It is impossible to predict what our interconnected, information-oriented society will look like in detail, but some of the outlines are becoming clearer. The ubiquity and power of the computer blur the distinction between public and private information. Our revolution will not be in gathering data — don't look for TV cameras in your bedroom — but in analyzing the information that is already willingly shared. Without any conspiratorial snooping or Big Brother antics, we may find our actions, our lifestyles, and even our beliefs under increasing public scrutiny as we move into the information age.



The illustrations on the following pages are bills, receipts, and statements (slightly edited for clarity) gleaned from the lives of the Whole Earth staff. Stuff we ordinarily discard or forget about. But computers don't forget. Under the direction of corporate marketeers these bits of information are gathered, juggled to reveal a pattern, compared to other stored profiles, traded or sold. Whereas once the most accurate records were compiled by civil authorities — and fairly well-regulated — personal statistics are now a fine-tuned, free-market commodity.

The example here, a MasterCard bill, shows that our composite client visited Cambridge, Massachusetts and subscribes to the *Village Voice* (potential radicalism). He buys occult books (Samuel Weiser, Inc.). He travels a lot, but not on business, since the other tabs are not for hotels but for jeans and record albums (Sam Goody). He carries $120 in cash.

Profile of a Buyer

Shoppers who think they are only vague entries on some company's list might lose that anonymity if they hold Mastercard or Visa credit cards. A new service by Citicorp Credit Services, a Citicorp subsidiary, will provide businesses that accept Mastercard and Visa credit cards with a detailed profile of their customers. The data will come close to pinpointing the bank card shoppers' income, education, family, housing type and value, age, vocation, even "lifestyle."

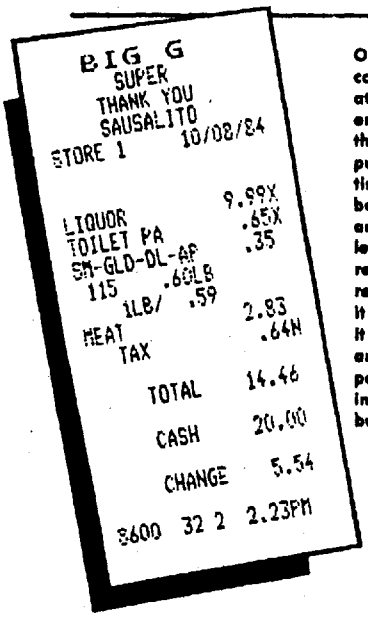
Alan Newman, vice president and marketing director for Citicorp Credit Services, said that until now, businesses that subscribed to bank cards have only been able to get generalized demographic profiles of those who use the cards. But an arrangement with Donnelley Marketing Information Services, a Dun & Bradstreet subsidiary, will allow Citicorp to combine Donnelley demographic data with Citicorp's own cardholder data, he says, "even to the very block of a community." —*New York Times*, 18 March 1984

How does Citicorp know what your lifestyle is? How can they sell such information without your permission? The answer is simple: You've been giving out clues about yourself for years. Buying, working, socializing, and travelling are acts you do in public. Your lifestyle, income, education, home, and family are all deducible from existing records. The information that can be extracted from mundane records like your VISA or MasterCard receipts, phone bill, and credit record is all that's needed to put together a remarkably complete picture of who you are, what you do, and even what you think.

BLOC MODELLING

A powerful technique used by managers of large amounts of data is called *bloc modelling*. The goal of bloc modelling is to evaluate how people fit into an organization or group, based on their relations with other members of the group. The primary use of this practice, which was developed more than a decade ago, has been to examine how employees fit into the firm where they work. Bell Labs, ABC, the Wharton School, and even the Institute for Social Management in Bulgaria are among those who have used the technique.

The mathematics and computations behind the process are complicated, but the underlying idea is simple: While the relationship between two people in an organization is rarely very informative by itself, when many pairs of relationships are connected, patterns can be detected. The people being modelled are broken up into groups, or *blocs*. The assumption made by modellers is that people in similar positions


BIG G
SUPER
THANK YOU
SAUSALITO
STORE 1 10/08/84

LIQUOR 9.99X
TOILET PA .65X
SM-GLD-DL-AP .35
115 .60LB
1LB/ .59 2.83
MEAT .64N
TAX
TOTAL 14.46
CASH 20.00
CHANGE 5.54
8600 32 2 2.23PM

Our local supermarket employs computerized laser scanners at the checkout. These generate itemized receipts, like this one which shows a large purchase of liquor and the time of day. Our client might be unjustly accused of having an undisclosed drinking problem. This store does not record customer ID numbers required to cash checks, but if it was one of those which did, it would rapidly accumulate an economic gold mine (and political gas pocket): an individual's extensive buying history.

behave similarly. Blocs aren't tightly knit groups. You may never have heard of someone in your bloc, but because you both share a similar relationship with some third party you are lumped together. Your membership in a bloc might become the basis of a wide variety of judgements, from who gets job perks to who gets investigated by the FBI.

Where does the initial data come from? In the office, it may be who you talk to on the intercom, whose phone calls you return (or don't return), who you eat lunch with, who you send your memos to, even who you play softball with. Fancy telephone systems, electronic mail, and bulletin boards make gathering this relational data even easier. When personal computers are on every desk, routine information about who says what to whom is automatically generated and easily collected. Employers and others can keep track of that mundane information, and save it in a database that can be bloc modelled later.

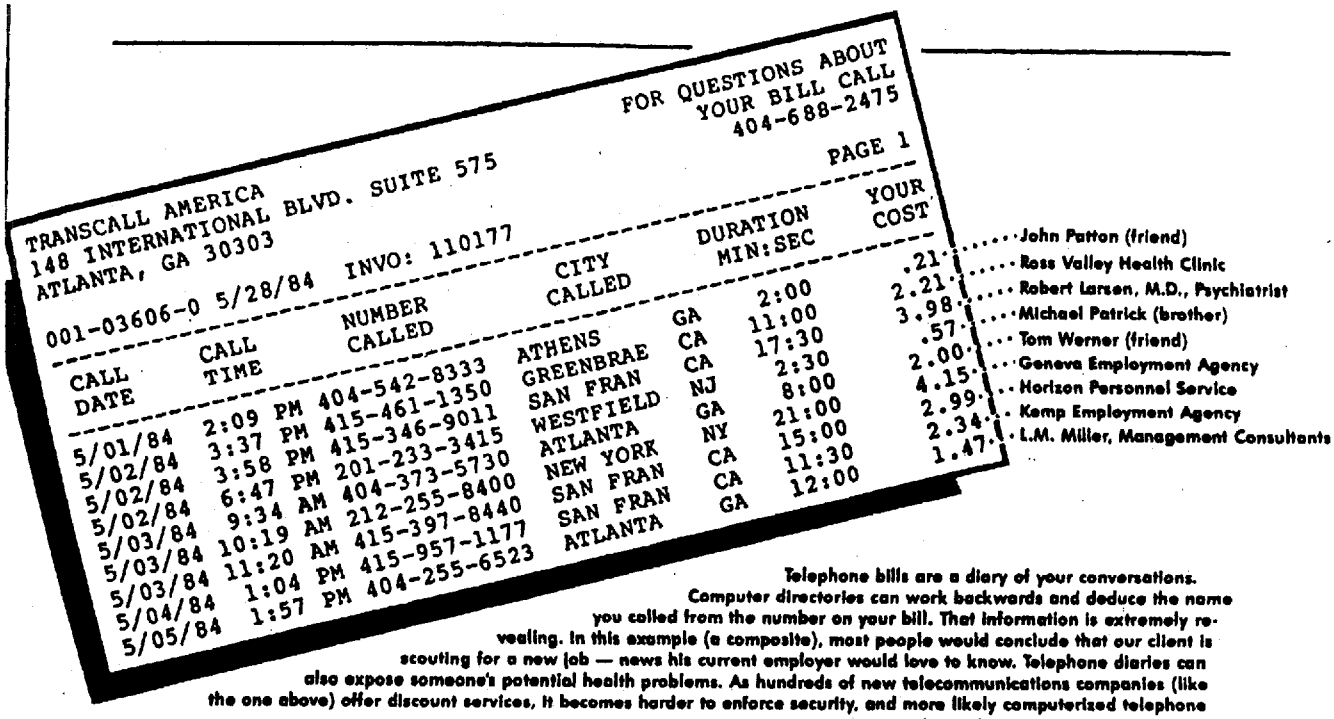
Bloc modelling is used to separate people, cliques, and whole organizations into categories which determine the way the modeller may ultimately treat the groups. While conceptually similar to the more familiar "redlining," it is unlike other kinds of discrimination, since the blocs found are generally inconspicuous, and the members may easily fail to recognize their common fate. Furthermore, the existing laws protecting privacy, such as those that guarantee individuals access to their own files, do not address bloc modelling. It is difficult to imagine what remedies might be devised for this new form of guilt by association.

WHEN IS PRIVATE INFORMATION PUBIC?

We live in a world of private and public acts. We consider what we do in our own bedrooms to be our own business; what we do on the street or in the supermarket is open for everyone to see. In the information age, our public acts disclose our private dispositions, even more than a camera in the bedroom would. This doesn't necessarily mean we should bring a veil of secrecy over public acts. The vast amount of public information both serves and endangers us.

To make this idea clear, I'd like to use an example invented by Jerry Samet, Professor of Philosophy at Bentley College. He suggests that, although we consider it a violation of privacy to look in somebody's window and notice what they are doing, we have no problem with the reverse: someone sitting in his living room looking *out* his window. If I'm looking out my window and I notice you walking down my street, I may notice that you are wearing a red sweater, holding hands with someone else, or heading towards the local bar. If I wanted to, I might write down what I saw out my window. Consider what happens if I write down everything I see out my window, and all my neighbors do, too. Suppose we shared notes and compiled the data we got just by looking out our own windows. When we sorted it all out, we would have detailed personal profiles of everyone we saw. If every move anyone made in public were recorded, correlated, and analyzed, the veil of anonymity protecting us from constant scrutiny would be torn away. Even if that record were never *used*, its very existence would certainly change the way we act in public. The idea that someone is always watching is no less threatening when the watching goes on in the supermarket, in the department store, and in the workplace than when it goes on in our homes.

The harmful consequences of just keeping personal profiles pale in comparison with the problems associated with their use. We don't have to look far into the future to imagine how such files could be used. There is a pressing example already apparent in two proposed additions to the National Crime Information Computer. The computer, or NCIC as it is commonly called, was set up to track wanted criminals and stolen property across state lines. When a policeman makes a routine traffic stop or otherwise confronts a stranger, the first thing he does is check the name through NCIC. If his name is in NCIC, the officer can search or arrest him, or take other discretionary action. The FBI now wants to add people to the database who have been accused of nothing, but are *suspected* of organized crime connections, terrorism, or narcotics possession, or are "known associates" of drug traffickers. Their avowed goal is to keep track of the whereabouts of such people. The FBI claims that this rep-



TRANSCALL AMERICA
148 INTERNATIONAL BLVD. SUITE 575
ATLANTA, GA 30303

FOR QUESTIONS ABOUT YOUR BILL CALL 404-688-2475

PAGE 1

001-03606-0 5/28/84 INVO: 110177

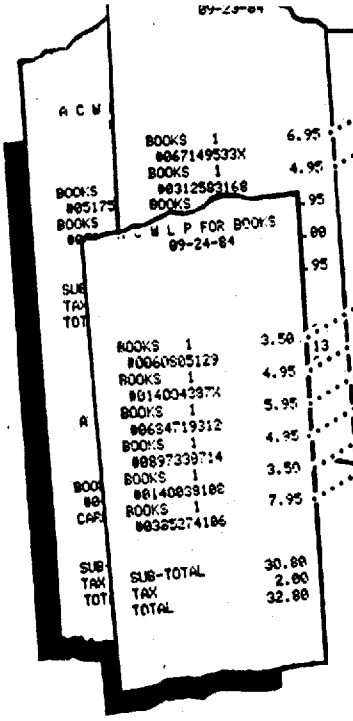
CALL DATE	CALL TIME	NUMBER CALLED	CITY CALLED		DURATION MIN:SEC	YOUR COST	
5/01/84	2:09 PM	404-542-8333	ATHENS	GA	2:00	.21	John Patton (friend)
5/02/84	3:37 PM	415-461-1350	GREENBRAE	CA	11:00	2.21	Ross Valley Health Clinic
5/02/84	3:58 PM	415-346-9011	SAN FRAN	CA	17:30	3.98	Robert Larsen, M.D., Psychiatrist
5/02/84	6:47 PM	201-233-3415	WESTFIELD	NJ	2:30	.57	Michael Patrick (brother)
5/03/84	9:34 AM	404-373-5730	ATLANTA	GA	8:00	2.00	Tom Werner (friend)
5/03/84	10:19 AM	212-255-8400	NEW YORK	NY	21:00	4.15	Geneva Employment Agency
5/03/84	11:20 AM	415-397-8440	SAN FRAN	CA	15:00	2.99	Horizon Personnel Service
5/04/84	1:04 PM	415-957-1177	SAN FRAN	CA	11:30	2.34	Kemp Employment Agency
5/05/84	1:57 PM	404-255-6523	ATLANTA	GA	12:00	1.47	L.M. Miller, Management Consultants

Telephone bills are a diary of your conversations. Computer directories can work backwards and deduce the name you called from the number on your bill. That information is extremely revealing. In this example (a composite), most people would conclude that our client is scouting for a new job — news his current employer would love to know. Telephone diaries can also expose someone's potential health problems. As hundreds of new telecommunications companies (like the one above) offer discount services, it becomes harder to enforce security, and more likely computerized telephone records will become an item of trade.

resents a "logical progression" of the crime center's efforts. The idea that associating with someone who gets arrested could get your name into the national crime database is scary enough. Worse yet, the Secret Service wants to get into the act. They want to sidestep the judicial process by directly entering the names of people they consider to be dangerous to the President or other high officials into NCIC without obtaining warrants. If the FBI and the Secret Service get their way, having tne wrong friends or being on the wrong side of the Executive Branch could get your name into the computer, subjecting you to police harassment, surveillance, even detention. Since just adding a name to NCIC doesn't legally deprive anyone of liberty or property, constitutional due process constraints do not apply.

Why not make gathering this information against the law? Think of Samet's metaphor: do we really want to ban looking out the window? The information about groups and individuals that *is* public is public for a reason. Being able to write down what I see is fundamental to freedom of expression and belief, the freedoms we are trying to protect. Furthermore, public records serve us in very specific, important ways. We can have and use credit because credit records are kept. We can prevent the sale of handguns to convicted felons because criminal records are kept. Supermarkets must keep track of their inventories, and since their customers prefer that they accept checks, they keep information on the financial status of people who shop in their store. In short, keeping and using the kind of data that can be turned into personal profiles is fundamental to our way of life — we cannot stop *gathering* this information.

What we have to do is find a way to control its *use*. We need to make it possible to draw distinctions between the kinds of information processing, dissemination, and use we want to allow and the kinds we want to prohibit. Some uses of personal information are quite reasonable. Using conviction records to avoid selling guns to criminals is a legitimate use of personal data. Keeping track of who I call on the telephone and for how long is legitimate if the purpose is to bill me for those calls. Writing down what books I buy is fine, so long as the intent is to maintain the inventory at my local bookstore. There are a variety of traditional, necessary, and nonthreatening uses of personal information. Ideally, any use of information outside the scope of these traditional ones should require the knowledge and consent of the person the information is about. Marketing and direct advertising are not traditional uses of personal information, and should not be thought of as such. I should be able to choose whether or not I want my local bookstore to keep a list of the books I buy, even if they just want to mail me ads for new books they think I'd like. I should be able to prevent a company from selling my name and address to someone else without my permission. I don't want the FBI to be able to look at my consumer records and decide that my lifestyle fits their model of a subversive or a drug user. I certainly do not want employers to use bloc modelling to fire people on the basis of who they associate with, or politicians to use it to identify their "enemies." →



Cash register receipts from a bookstore that has computerized its inventory. Each book is itemized by its industry code ISBN number. We used a software program called IN-SEARCH (*WESC*, p. 152) to quickly access Dialog's database "Books in Print" in order to decode the ISBN numbers into book titles. If customers shop with credit cards their account numbers can be linked to the reading history of an individual. Even emotion can be tallied. From the book titles we have a clue that our client may be quite angry.

INFORMATION AS PROPERTY

People under scrutiny ought to be able to exert some control over what other people do with that personal information. Our society grants individuals control over the activities of others primarily through the idea of property. A reasonable way to give individuals control over information about them is to vest them with a *property interest* in that information. Information about me is, in part, my property. Other people may, of course, also have an interest in that information. Citibank has some legitimate interests in the information about me that it has gathered. When my neighbor writes down that I was wearing a red sweater, both of us should share in the ownership of that information.

What does it mean to own information? To share in such ownership? How can existing laws about property be interpreted to make judgements about the use and control of information? These questions must ultimately be answered by the legislators who draft laws giving information property status, and the courts who interpret those laws. We can begin to imagine some of the implications of such an approach. What makes information different from other kinds of property is that it is intangible: it cannot be touched, held, or seen directly. The same information can be in two places at once. Other than that, information is like other kinds of property: it can have monetary value, it can be produced, improved, or degraded, and one can share, withhold, or transfer it to others.

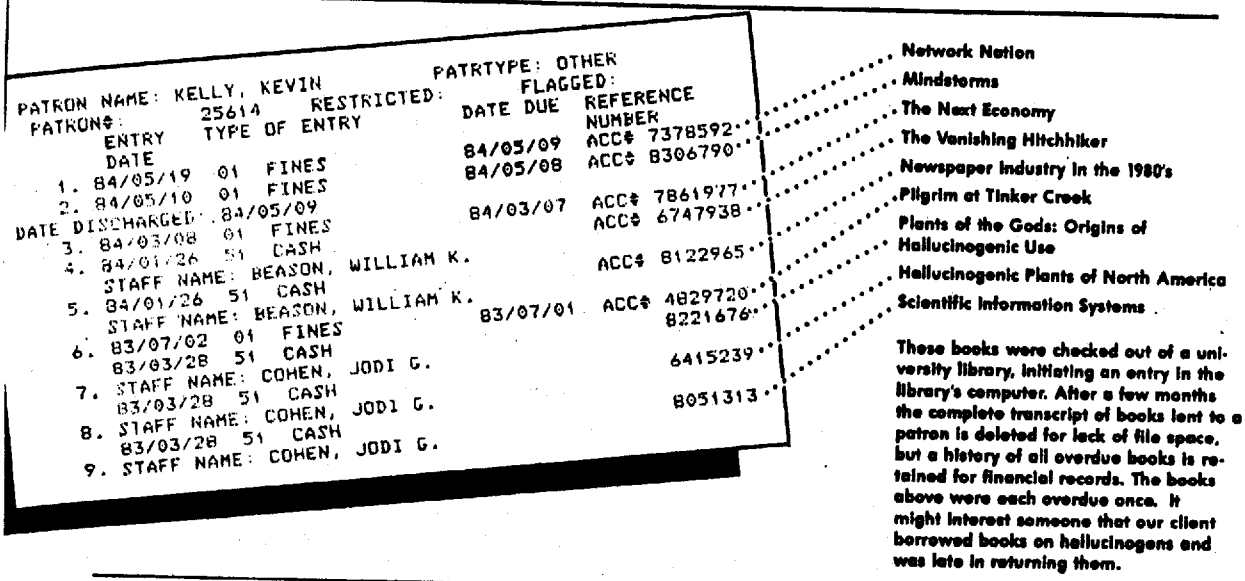
Is information enough like property to be successfully integrated into property law? The process has already begun in many legislatures. Across the country laws are being passed that make unauthorized access, duplication, or tampering with information stored in computers a crime. These laws are deemed necessary because existing burglary statutes don't apply to copying information, or looking at it, especially if the access was by remote computer. When computer data is copied by an unauthorized outsider that action resembles burglary, and it is treated as such in these new laws. If it is like burglary, then something is being stolen. In this context, information is already being implicitly treated as if it were property.

If we are to treat information as property *explicitly*, some of our ideas about property will have to be changed. Information can be stolen by copying it, leaving the original behind. If information is merely what is known, how can it be taken away? How can vesting the individual with the rights associated with property, particularly the right of excluding others from that property, be specifically translated into control over analysis of data? How can we define information so that knowledge in a computer is property that can be controlled, but knowledge inside someone's head is not? Enforcement presents another problem: how can we tell if someone is using personal information illicitly? The example of copyright law suggests that, while finding small abuses of intangible property is difficult, finding major violations is no harder than other law enforcement tasks.

SEARCH AND SEIZURE OF INFORMATION

Treating information as property has an additional benefit. As the law currently stands, information isn't property, but computers are. The owner of the computer has been held to control everything "inside" his computer. That means that if I write a personal note on my office workstation, my employer has the right to read it. By contrast, he has no right to read a note I write on company stationery with a company pen and put in my (company owned) desk. More importantly, my employer can give permission to law enforcement agencies to go on a fishing expedition through my files in his computer, which, metaphorically, gives the police the right to rummage at random through any employee's "desk." This is not hypothetical; a case of just such abuse was reported by Larry Layton, a government employee.

Layton worked in a Defense Department office (DARCOM) which was fully electronic. Most



employees had computers and all used electronic mail to communicate with each other. There were over 3000 users with access to the system, and 500 in-house users of internal workplace computers. All writing and inter-office communication, as well as other office support, was done on a computer. At least three times, the Army Criminal Investigation Division, in conjunction with the FBI, obtained complete dumps of all the workplace automation computers without any type of court order or specification of what they were looking for, other than "wrongful use of government property." A "complete dump" means that every bit of information was printed out and examined. Using the analogy to desks, it is as if the FBI went through every employee's desk looking at every piece of paper, through every address book, reading every memo and every piece of mail. After finding one person who had a recipe in an electronic mail message, and another who had a baby sitter's phone number in a telephone number file, the FBI read each his rights and threatened retribution. The legal staff of the operation advised the managers that the searches were legal since computer files don't fall under any of the same protections that, say, telephone usage does. The searches have resulted in the employees refraining from using the system for communication, electronic mail, filing, and many other applications.

This sort of witch-hunt is only the beginning. Electronic mail typically goes through several computers before reaching its final destination. The owner of each of those computers apparently has the full legal right to read, copy, and disseminate anything contained in his computer, including that mail. Since the U.S. Postal Service, MCI, and a host of other similar entities are operating electronic mail services, one might think that electronic mail had the same protection and privacy as a paper letter or a phone call. It does not. It is, for the time being, completely open to anyone through whose computer it passes. We must extend the special status of the letter and the phone call to all forms of electronic communication. The idea of *information as property* will protect that information with the rules of search and seizure that apply to other kinds of property. It will provide the connection between sending a letter and sending electronic mail necessary to protect the content of our communication.

PUBLIC IMAGES, LIMITED

It is time our legal technicians turned their attention to framing answers in the language of the law. We will need to define many gray areas, and insure that we tread carefully in these sensitive areas of personal information. I think we can specify the uses we consider traditional, and separate those we consider new or threatening. Lawyers, computer scientists, businessmen, and an informed public must work together to bring to our legal system a carefully crafted new framework for thinking about information.

Computers and electronic communication are ushering in a new age. We will be able to talk to more people in more ways than ever before. The dramatic increase in our ability to communicate may be the glue that we need to hold our fragile world together. Computers also help us analyze all the information we can gather and exchange, helping us to understand the world around us. It is precisely those abilities which make computers threatening, too. Soon celebrities and politicians will not be the only ones who have public images but no private lives — it will be all of us. We must take control of the information about ourselves. We should own our personal profiles, not be bought and sold by them. ■

SPECIAL INAUGURAL REPRINT ISSUE: INFORMATION ENVIRONMENT TOOLS AND IDEAS Whole Earth Review Dedicated to the Incoming Administration 20 January 1996 - Link Page

Previous	Six Grave Doubts About Computers (January 1985)
Next	Digital Retouching: The End of Photography as Evidence of Anything (July 1985)

Return to Electronic Index Page