

Where the public draws the line

Consumers are learning they can say 'no' to invasions of privacy

JANLORI GOLDMAN



A targeted mailing arrives at your door: "Congratulations, Ms. Jones, on your new raise. You'll be needing it since you've just bought a new home and a car and had a baby last year. Wondering how you'll afford your third trip to Barbados? Or how you're going to pay that huge mortgage? Have we got a deal for you."

The core principle of privacy laws is that information collected for one purpose may not be used for another purpose without the individual's consent. Thus, a detailed financial history you provide to obtain a mortgage should not be used later by a marketer unless you give your permission. However, in areas not yet regulated by privacy law, such as most marketing activities, personal information obtained in one transaction is routinely sold for a second profit without the person's knowledge or permission. The information travels from database to database, eventually making up what one commentator dubbed "a womb-to-tomb dossier."

Catching the fever

Everyone's catching database fever, and the consequences can be severe.

Employers are running credit and criminal history checks of employees to assess trustworthiness. Landlords can now access a database to learn if a tenant has ever filed a complaint against a former landlord. Doctors can check to see if a patient

has brought a malpractice suit against another doctor.

Although these databases are notoriously inaccurate, they are used to make decisions affecting people at critical junctures in their lives. And in the near future, genetic testing will make it possible for insurance companies and employers to weed out people who seem likely to develop a physical or mental illness.

The good news is that consumers are catching on. They're learning that information about them is being bought, sold and exchanged by the private sector and the government, and they're beginning to insist on the opportunity to say "no" to secondary disclosures.

Recently, for example, the Social Security Administration was forced to stop matching and verifying millions of social security numbers for TRW, Inc. after the practice was made public.

Consumers are demanding privacy protection in the development of information products and services, and the industry is responding. Privacy is emerging as a critical factor that can determine the rise or fall of certain products.

The recent decision by Equifax and Lotus to abandon Lotus Marketplace was in direct response to intense and widespread opposition to the product, a database that would have contained names, addresses,

buying habits and income levels of 80 million households. Much of the information came from Equifax's consumer reporting databases. Outraged that such a vast amount of personal information was to be available without their permission, thousands of people insisted that their names be removed from Lotus Marketplace.



James Turek

In withdrawing the product, the companies conceded that the privacy problems could not be fixed. This session, Congress will consider a sweeping reform of the outdated law that regulates the credit reporting industry.

Digging deep

Caller ID is another product that taps people's deeply rooted sense of privacy and another area where public response has altered industry policy.

Early on, a number of telephone companies decided to market Caller ID to automatically display the number from which a call is placed, regardless of the privacy concerns of the

person making the call.

These telephone companies soon realized, after intense public pressure, that people want control on both ends of a telephone call — people on the receiving end want to see who's calling before they pick up the telephone, and callers want to decide when and to whom to give their number. Legislation is pending to require that, where Caller ID is offered, telephone companies must give callers the ability to block the display of their number on the receiving end. In the meantime, however, the public is demanding blocking and, with the exception of a few hold-outs, they are getting it.

Blocking actually serves the privacy interests of both callers and call recipients, who are often the same people. It actually provides more information for call recipients. For instance, people who are on the receiving end of abusive or harassing telephone calls may decide never to answer a call from a blocked number.

People who care about their privacy are a powerful constituency. In the past few years, a number of companies and trade associations have actively supported federal privacy legislation as a good way to assure the public that personal information is safe with them.

After the disclosure of ex-judge Robert Bork's video rental list, Erol's video stores, the Video Software Dealers Association and the Direct Marketing Association came forward to press for a tough law prohibiting video stores from releasing rental information without a person's

consent. The resulting Video Privacy Act of 1988 won the unanimous approval of Congress.

The Bork bill, as it is known, is not about having something to hide. It is about the freedom to view movies in the privacy of your own home, shielded from the prying eye.

Right to decide

The right to decide what people know about you strikes at the heart of our constitutional values of liberty, autonomy and freedom. Without the ability to retreat into our private world, we will lose our freedom to step boldly into public life. Privacy protection allows people to actively and openly participate in our society.

Unfortunately, in its recent decisions, the Supreme Court has lowered constitutional privacy protection to fit what is technically possible. For example, the court has ruled that since high-tech helicopters can hover over backyards, we should expect the Feds to be there. The court has also decided that, since cordless telephones operate on a radio-based, easy-to-overhear frequency, we should expect all of our conversations on them to be public. As a result, privacy advocates have learned that we must turn to Congress to write privacy expectations into the law.

Privacy advocates are not Luddites who are trying to smash the computer state. We are insisting that progress be measured by technology's ability to preserve privacy. In this area, progress must be defined by new technologies designed to meet — not undercut — society's legitimate expectations of privacy.

Goldman is director of the American Civil Liberties Union Project on Privacy and Technology.

Mainframe programmers and the V-8 mentality

MARC S. SOKOL



A recurring scene in the Danny DeVito/Richard Dreyfuss movie *Tin Men* says a lot about what's happening in information technology today. DeVito and Dreyfuss play two aluminum siding salesmen in the early 1960s. They drive around Baltimore in huge Cadillacs, but Dreyfuss starts noticing Volkswagen bugs zipping around all over the place.

By the end of the movie, he realizes that those peppy little cars represent the future and that the lumbering hulks he and

his colleagues drive are headed for near-extinction.

Today, something similar is going on in IS shops around the country. Not only have personal computers become more powerful, but a whole range of PC-based application development tools now exist — Cobol compilers, CICS emulators, debuggers, compression utilities, screen editors and programming shells.

Machine machismo

These products do more than enable PCs to build full-scale mainframe applications. In many ways, they do a better job of building those applications than mainframes do. Yet there remains a strong degree of resis-

tance to using PC workstations this way.

There are hard-core mainframe programmers determined to hold their ground against the incursion of smaller systems. They seem to feel that PCs just don't have "the necessities" — the capacity, the sophistication, the power — to perform mainframe programming and maintenance.

Much of this reflects the unique mainframe programmer mentality. It's well known that many of us who come from a mainframe programming background view ourselves as a kind of high-tech elite. We often distinguish ourselves by our language, style of dress and eccentric working hours. But most of all, some mainframe programmers pride themselves on the sheer size and power of the machines at their command. Within this group, the idea of programming on a PC is demeaning —

like asking Mario Andretti to drive a Ford Escort in the Indy 500.

The user has a choice today: Work the graveyard shift to get development time on the mainframe or work normal hours on the PC.

IS managers also have a choice: Let programmers hog mainframe resources to build applications at the expense of current operations and end users, or let them use separate, less costly and nondisruptive PCs to perform the same job.

Get the message?

The message for the mainframe programmer is clear: Adapt, or go the way of black-and-white television and monaural recordings.

Today's hard-core mainframe loyalists are like American carmakers in the 1960s. They too firmly believed that nothing would replace their hulking, su-

percharged monsters.

In a sense, the carmakers were right — there is nothing like the size and power of those big cars. There is also nothing like their gas guzzling, their jack-rabbit starts, their lack of maneuverability or their inability to get into small parking spaces.

Mainframes are already being used differently in the new IS environment, more as information repositories and large-scale batch processors. It is the less progressive, less realistic IS shops that will continue to buck the trend toward using PCs for these programming tasks. Such shops will pay a high price in the form of relatively low productivity, less effective applications and continued unresponsiveness to end-user needs.

Sokol is executive vice president at Retalia, Inc., a Chicago-based producer of Cobol compilers and other application development tools for PCs.