Our Data, Our Selves

by Douglas Neal and Nicholas Morgan

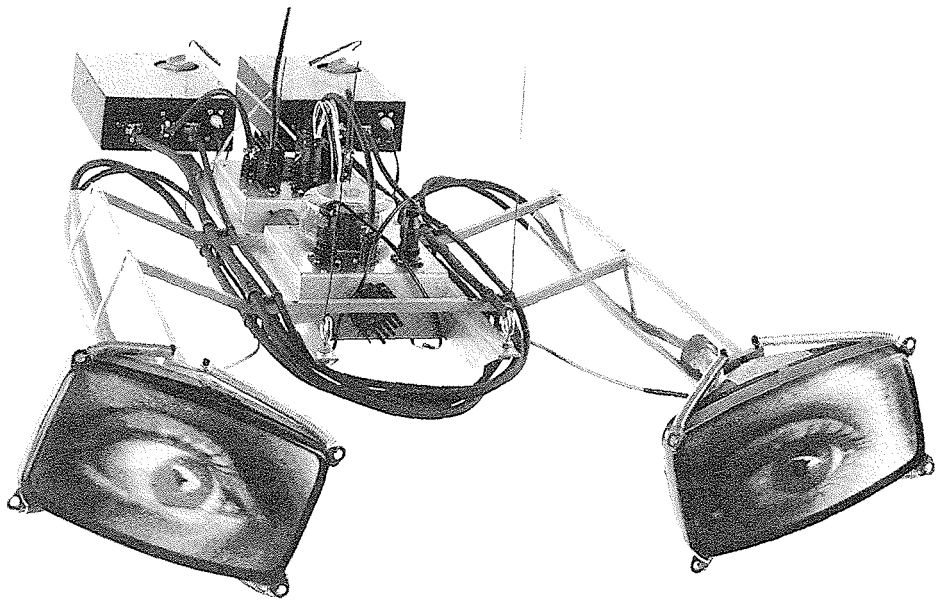
It's Friday night, the end of a tough week. You're ready to relax with your family, and you've enjoyed cooking a meal together. A wonderful aroma of spices and sesame oil fills the kitchen.

Just as you sit down to dinner, the phone rings. A computer half a continent away has turned up your name and telephone number on the screen of a telemarketer. The computer has data about you that suggest you might be interested in purchasing new aluminum siding. "How are you this evening?" comes the telltale telemarketer greeting when you pick up the phone. In a tone that is louder and angrier than you intended, you blurt out, "I was fine, until you called," and then you hang up and stalk back to the table. Once again, your privacy has been invaded.

In this era of rapidly expanding information technologies, telemarketing is only one of the more annoying ways a person's privacy can be breached. There's "junk" mail and e-mail, as well as other intrusions that are less immediately irritating but often more ominous. It is now possible, for example, for companies, governments, and other interested parties to track surreptitiously an individual's virtual travels on the Web and even, by determining his location when he uses his mobile phone, in the nonvirtual world. In London, with its 800 cell phone towers, it will soon be possible to determine a user's location within 50 meters. It is conceivable that in the near future aggressive marketers will be able to use your cell phone to send you advertisements and special offers from stores and restaurants as you pass by.

The list of privacy threats goes on. It's not uncommon for Web site hosts to send out data they have collected for analysis (and thus possible misuse) by another firm. Data that people have allowed others to collect for one purpose may be used for another, unauthorized purpose—a possibility highlighted earlier this year when bankrupt Toysmart.com announced its intention to sell personal information it had gathered about its Web customers. Private information may be disclosed inadvertently in a "data spill" and information about a person's preferences—has she been searching the Web for information about Vivaldi? about new sport-utility vehicles?—can also be released.

For most casual observers, such threats came sharply into focus only last year, when the Web tracking and advertising firm DoubleClick



Soar Eyes *(1994), by Alan Rath*

announced its purchase of a company called Abacus Direct. DoubleClick gathers data that allow it to track the Web browsing of individuals—data linked only to browsers' online identity, but not including their e-mail addresses. Abacus has vast data banks of personal information, including names and addresses, about some 88 million people who have made purchases through mail-order catalogues. DoubleClick's plan was to merge its data with Abacus's, allowing it to compile dossiers on individuals that would link information compiled from the relatively anonymous world of the Web to Abacus's names, addresses, and other data. The reaction from the public and the federal government was swift, loud, and emphatically negative. DoubleClick backed off.

Since the DoubleClick scare, new controversies—including one sparked by the revelation that the U.S. National Office of Drug Control Policy was secretly tracking the Web surfing of people who had visited its Web sites—have helped create a national debate about the protection of personal information in the electronic world.

The United States has long relied on industry self-regulation in this area, but that may be changing. In May, Robert Pitofsky, chairman of the U.S. Federal Trade Commission, describing industry efforts at self-regulation as inadequate, called for new federal legislation to establish "basic standards of practice for the collection of information online." Dozens of separate privacy-related measures are now pending on Capitol Hill, and threaten to create a patchwork national privacy policy. A number of new laws are already in place. The 1999 Gramm, Leach, Bliley

>DOUGLAS NEAL *is director of global networking at CSC Research Services.* NICHOLAS MORGAN *is the editor of the* Harvard Management Communication Letter *and* CSC Foundation Research Journal. *He is the founder of Public Words, a communications consulting firm.*

Act, for example, requires all financial services firms to provide annual notices about their data-use policies to all of their customers, and also to provide mechanisms for customers to "opt out"—to decide that they no longer want information about them to be used in certain ways. In order to comply with the act, these companies will need to send their customers some 2.5 billion pieces of mail by November 12 of this year—a boon to the U.S. Postal Service, perhaps, but for consumers and businesses alike a costly (and probably ineffective) measure.

In Europe, the predisposition has been to deal with the issue through legislation. There are now strict prohibitions on what information may be recorded and how, if at all, it may be used. For example, under Britain's 1998 Data Protection Act (which only comes into full effect in October of this year) firms typically are required to provide notice and gain explicit permission before they can make use of any personal data. The European Union is putting similar policies in place. All of these policies affect American companies doing business in Europe, and while the U.S. government is negotiating an agreement with the EU to avoid the need for similar laws in this country, the potential restrictions are still significant. The Marriott hotel chain, for example, recently had to seek clarification to see if it was permissible to do something as simple and useful as keep track of its customers' preferences for nonsmoking rooms and king-size beds.

RATHER THAN TRYING TO SET ABSTRACT STANDARDS FOR PRIVACY IN THE MARKETPLACE, WE CAN BEGIN TO THINK ABOUT PERSONAL INFORMATION AS PERSONAL PROPERTY.

Who will draw the privacy line, and where will they draw it? If governments do it, then in all likelihood it will be a stark line, one that errs on the side of restricting the availability of information and lacks the flexibility to adapt to changing economic circumstances and individual preferences. But what is the alternative? Few Americans would be comfortable allowing businesses to make all the privacy decisions.

There is a third option. Rather than trying to set abstract standards for privacy in the marketplace, we can begin to think about personal information as personal property. A large part of the threat to privacy today arises from the fact that in an increasingly networked world, data about individuals—everything from their age and sex to their buying habits—have increasing monetary value. Corporations, as well as charities, advocacy groups, and other organizations, want such information because they think they can use it to make money. So why not make them pay for it? More important, why

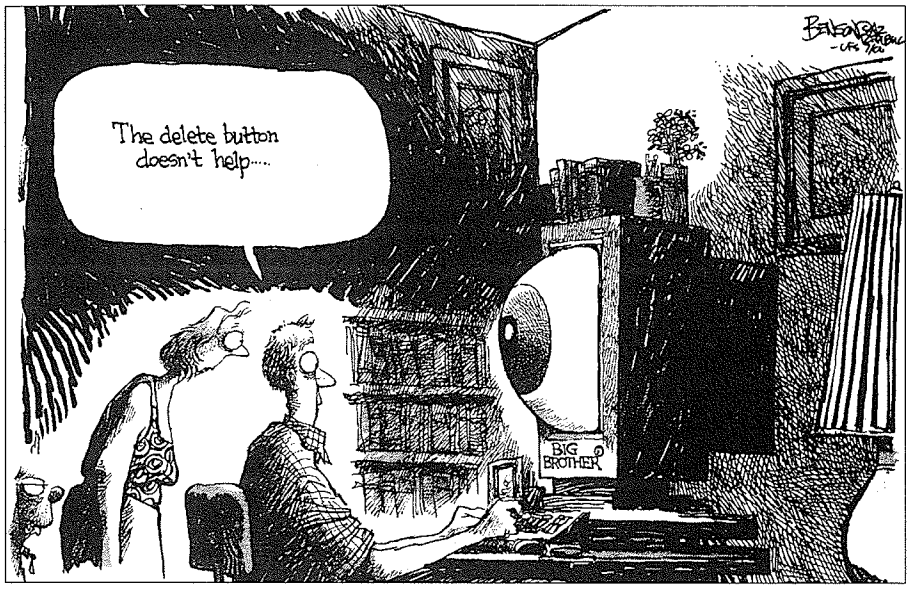
not use the system to allow every individual to draw his or her own privacy line?

These things become possible in a world where personal information is treated as property that individuals have the right to control, just as they control their household possessions. In a way, such a scheme takes us back to the 19th century, before changing cultural mores and technology (e.g., the telephone and the wiretap) vastly complicated the definition of privacy. In that era, before inquisitive media began regularly peering into private lives, one could largely protect privacy by protecting tangible property, such as personal papers and diaries. In the marketplace, and perhaps in other realms of existence, we may be able to recover some of that simplicity.

The advantages of such an approach are considerable. Calling upon government to draw what would inevitably be an overly restrictive privacy line would undermine the information revolution that is driving the new economy. The cost in lost jobs, income, and choices would be high, the blow to America's competitive advantages in the world marketplace severe. As Federal Reserve Chairman Alan Greenspan said last year, America's economic surge since the early 1990s has largely been a consequence of bringing more and better information to bear on economic life. Companies that don't know who their customers are, what they want, or when they want it, he noted, invariably do a number of things to hedge against uncertainty. These hedges lead to costly mistakes: excessive stockpiling, flawed decisions about what products to produce, and inappropriate delivery times. By contrast, the near real-time nature of the Internet enables manufacturers to respond to real "pull" signals rather than someone's guesses. The key to the future, Greenspan continued, lies in using information "to detect and to respond to finely calibrated nuances in consumer demand."

THE LINE DIVIDING WHAT YOU WANT TO SHARE FROM WHAT YOU DON'T CAN BE VERY SHARP AT SOME TIMES—AND ALMOST INVISIBLE AT OTHERS.

Rigid rules governing information would also deprive consumers of many of the choices and efficiencies that the information economy is beginning to offer. While one's instinctive response might be that, given a choice, people will elect never to release any personal information, experience shows that this is not the case. A sense of urgency surrounds the privacy debate precisely because vast quantities of personal information are already in circulation. Look, for example, at all the people who are willing to share information about themselves and their buying habits with Internet companies that offer discounts or free merchandise in exchange. A recent survey by the Pew Internet and American Life Project found that while most of those polled said they were concerned about online privacy, two-thirds said they had given out personal information online or would be willing to do so.



Many Web users express concern about online privacy, but only 10 percent set their browser software to reject the "cookies" used to monitor Web travels.

Eighty-one percent of those polled favored stricter privacy rules, but only 24 percent wanted the federal government to formulate them. Most said Internet users should make the rules.

There is enormous variation in the privacy preferences of individuals. Just as there are certain details you would like your co-workers to know about you and others you prefer to keep confidential, so there is some information you would like the world to know about you and other information that you want to keep to yourself. The line dividing what you want to share from what you don't can be very sharp at some times—and almost invisible at others. Your personality, ethnic background, and stage of life, among many other factors, all play a role in determining whether you believe a certain piece of information should be kept private. Equally important are the purposes for which the information is to be used and who will use it—as well as the compensation you will receive for granting access to it.

In the future, marketing will be only one of many valuable uses of personal information. Ohio-based Progressive Auto Insurance, for example, is now testing a system that will closely tie the cost of its customers' insurance premiums to their actual use of their cars. Progressive installs in the customer's car a mobile telephone that is tied into the Global Positioning System. Every six minutes the device records the car's location in its database; once a month the company computer connects to the onboard telephone and downloads information about when and where the car has been driven. The company can then send a custom-tailored bill based on a variety of pricing factors, including distance and time of day driven. For example, since actuarial studies show that accident rates at 2:00 A.M. are four to five times higher than at 7:00 A.M., drivers who stay off the roads during the wee

hours will pay less. Prudent drivers will reap big rewards. With this technology, insurers would no longer need to group drivers into large pools, with the good drivers subsidizing the bad.

Progressive's plan may prove very attractive, but not if there is any doubt about who owns the information about policyholders' travels. If the policyholder has clear title to it, the plan becomes more palatable. (But anybody engaged in criminal activities or adulterous affairs would be well advised to look elsewhere for auto insurance—there is no guarantee at present that such information could not be used in a legal proceeding.)

In the near future, however, personal information will be most useful in providing Web sites that are highly personalized, based on the site's knowledge of such things as the visitor's interests and buying patterns, and in reaching out more actively to consumers. Instead of receiving a steady deluge of junk mail, for example, you should be able to signal an interest in, say, a new car during that brief period when you really are in the market for one. You, or a software agent that you would program, could stipulate the conditions and prices for which you would provide access to your data (including perhaps your background, demographic characteristics, attitudes, and preferences, as well as specific instructions about how you may be contacted). Many companies would gladly pay for such high-quality information—and would likely provide much more useful information and offers.

INSTEAD OF RECEIVING A STEADY DELUGE OF JUNK MAIL, YOU SHOULD BE ABLE TO SIGNAL AN INTEREST IN, SAY, A NEW CAR DURING THAT BRIEF PERIOD WHEN YOU ARE REALLY IN THE MARKET FOR ONE.

This system would also have the advantage of breaking the current deadlock between business and consumer advocates who call for "opt in" requirements—banning all uses of personal information to which the individual hasn't actively consented. Business responds that such requirements are so costly that many services will become uneconomical. A system in which information is property offers consent *and* efficiency.

To make a system of this kind work, a third party trusted by both consumers and potential purchasers of the information would be needed. Financial services firms are obvious candidates, with their long experience handling sensitive data and complying with privacy regulations, but other institutions might also do the job. Together, the institution and each customer would create a Web page that would function as a secure "storefront" for data about that person. After an initial setup, little would be required of the consumer, since software would infer his or her pref-

erences (about, say, breakfast cereals) from purchases and other behavior; the host institution would have every incentive to keep other information up to date.

To protect privacy, the Web site could issue a digital certificate of authenticity—perhaps in the form of a digitally encoded "watermark"—to those who purchase data. Stipulating where the data were purchased and under what conditions they may be used (including how many times and by whom), the certificate could include the possibility of allowing future information updates. Because the Web sites would be the most authoritative and detailed source of data about each person, organizations would soon come to choose them over other possible sources. Marketing offers arriving via e-mail, telephone, or videophone from companies that failed to carry a digital watermark of authenticity would be blocked by automated filters.

But the system would do a lot more, increasing the flow of information about things in which the person had expressed an interest, from bulk dog food to European travel opportunities. The free flow of more accurate information would have other effects throughout the economy. Consider the fact that the interest rates Americans pay on their home mortgages are from one-half to two percentage points lower than those paid by Europeans. Why? The major reason is that American mortgage lenders are allowed to collect extensive information about their borrowers and pass it on when reselling the mortgage in the secondary market. More information means less risk for the buyer and a more liquid market. Digital certificates would solidify and expand these advantages. If buyers in the secondary market get a digital certificate authenticating the data and permitting them to visit the borrower's Web site for more up-to-date information about, say, the borrower's income and occupation, costs will drop further.

The technological groundwork for such a system is already being laid. Micropayment technologies are making it possible for a person's interest in a new dishwasher, for example, to be sold over the Internet for a few pennies. And Internet markets are being developed in which software "agents" negotiate with other software agents to complete such transactions.

The great benefit of combining market technologies with individual control of personal information is flexibility. Legislation cannot respond to rapid or frequent changes in personal preferences about privacy—but markets can. Yet the privacy line is different for each individual, which is why most people don't want businesses to draw the line for them. So individuals must draw it themselves. Now, with the advent of technologies that are creating new markets for information, it is possible to begin thinking about giving people that opportunity.

In the future, you could have an option when a telemarketer calls on a Friday night. Your "agent" would answer the phone before it rings, saying, "Yes, my client is having dinner. She will be happy to interrupt her dinner to take your call for $200 for the first three minutes. Please deposit the amount on her Web site, *janeqcitizen.com*, now, or disconnect. Thank you." ❑