

SOLITUDE: SCARCE RESOURCE OF THE 1990s

When famed actor Klaus Kinski died late last year, his passing received barely a mention in San Francisco newspapers because few people realized that he lived on a small ranch just north of the city. Kinski's search for anonymity and solitude was so complete that he caught even the local news hounds by surprise. In fact, Kinski's isolation was so total that as one magazine reported, he knew nothing about the Gulf War until months after it broke out.

Kinski's lifestyle seems light-years apart from the interrupt-driven nature of everyday business life, yet it is an important indicator of an issue likely to come to the fore in the decade ahead. We fret over a loss of privacy in the face of steady advances in computing and personal communications, but the impact of this trend will be felt as a deprivation of solitude. In fact, solitude may come to be perceived as the scarcest of resources for consumers, obtainable only at considerable personal and financial cost. Kinski's admittedly eccentric lifestyle may become a longed-for option.

Hints of this trend can be seen in the current debate over ensuring citizen privacy in the face of ever more powerful credit databases, telephone caller identification and the like. Daily life for average consumers seems like nothing so much as a string of transactions. From credit card purchases to phone calls, each of these transactions is mediated by computers and recorded in remote databases. Each transaction contributes to a spreading electronic wake that we leave behind us as we go through life. A few bits of matched data can tell volumes about us all, a conclusion implicit in the informal motto of the direct marketing industry—"we know more about you than your mother." Buy a new house, and you will be deluged with solicitations from contractors and financial services companies. Register your pregnancy at a hospital, and word of the event is flashed across a national baby care industry faster than your relatives receive the happy news.

Privacy erosion is a much-debated topic, but it is a driving force and not an issue, for the erosion is irresistible and unstoppable. Despite our privacy jitters, we will never slow, much less reverse the growth of this electronic marketplace, for our society runs on information. Consumer products companies depend on "consumer preference information"—aggregated masses of information about individual habits and tastes. Health care providers routinely record and share intimate personal details that individuals might be reluctant to mention to anyone outside of immediate family.

Our society is becoming ever more complex and interdependent, and personal information is essential to its efficient operation. The health care system would come to a dead stop without a steady diet of patient information, and government couldn't function without a rich flow of taxpayer data. This decade will see a dramatic increase in information

Paul Saffo
Research Fellow

ポール L. サフォ

 Institute for the Future

2744 Sand Hill Road
Menlo Park, CA 94025-7020
Telephone: 415-854-6322
Fax: 415-854-7850
MCI Mail: PSAFFO

collection and use in three ways—analysis/matching, dissemination, and automated capture. Beneath it all will be an argument that efficiency demands the consequent erosion in privacy, and ultimately, solitude.

ANALYSIS AND MATCHING OF DATA

Governments and business have been collecting data for some time, but for the most part, this data was stored in stand-alone computer data islands. Now these islands are being joined. Businesses routinely create views of specific consumer populations (by overlaying data from multiple sources). Combine government census information with credit bureau-collected information on marital status and income, and one can easily gain a good view of lifestyle and preferences down to the detail of a single household. Add a telephone/address database, and the researcher can contact the target household directly.

On the government front, data matching emerged as a trend during the Reagan Administration, touted as a means to track down “welfare cheats” and collect unpaid taxes. More recently, the practice has gained favor as a vehicle for hunting down fathers who fail to pay child support. Recent history in California is particularly instructive. Several years ago, a psychopath murdered actress Rebecca Shaffer in her home after allegedly purchasing her DMV address data from an out of state vendor. Much was made of the need to protect individual privacy in the debate that followed. However, a bill making Social Security numbers part of every driver’s Department of Motor Vehicle record received overwhelming approval despite its potential for abuse because it makes tracking delinquent fathers so “time-efficient” in the words of an aide to the sponsoring Senator. This and similar legislation contemplates an environment where enforcing agencies and others will be able to hunt their quarry by looking for matches in electric and telephone utility records, as well as trade association and union records.

DATA PUBLISHING AND “DESKTOP MARKETING”

Despite worries about “Big Brother,” large corporations have had relatively little impact on the privacy of individual citizens for the simple reason that there is little economic benefit to dig down to the level of individual households. However, the same data that once were available only to large corporations is being repackaged on optical disks for use by local small businesses. For example, one product called “Marketplace” contained a database of names, addresses, and marketing information for 120 million U.S. consumers. Priced under \$1,000, it promised to deliver “desktop marketing” to everyone from local car dealers and stereo dealers to private investigators. Marketplace was withdrawn after a storm of public protest, but several similar products are slated for release within the year.

DATA COLLECTION AND “INFOBOTS”

The third dimension to this driving force is automation of the data collection process by information robots—“infobots.” Credit card “scanners” at checkout counters are a familiar example in the business world, and supermarkets are beginning to combine scanner-gathered information on purchases with purchaser data in order to create a new revenue stream from selling this data to product makers. In the government sector, automated capture has come to the fore in areas such as health care and highway toll collection. Automatic Vehicle Identification (AVI) contemplates a transponder device in every car that beams data to roadside sensors tied to remote toll-taking computers. Several such systems are operational in the United States, and California is contemplating AVI for use on bridges and several planned toll roads.

AVI data can tell volumes about drivers. The time of passage and direction is useful information particularly if several sensors are passed. This usefulness is not lost on the California Highway Patrol and California Department of Transportation, which hope for transponders that transmit several hundred characters worth of data at each pass, an aid to everything from stolen car tracking to emissions compliance.

In the business world, Automatic Number Identification—ANI—offers similar benefits for phone calls. ANI systems automatically flash the number of the caller on a screen on the recipient’s end. Just the thing to track down obscene callers, and for telemarketers to capture customers’ phone numbers.

The most that privacy watchdogs can hope to accomplish in this age is ensuring accuracy and confidentiality for certain kinds of information. Each instance cited above can be justified by pleas for efficiency and equity despite their erosive effect on privacy. AVI data could be used to track the comings and goings of private citizens, but such hazards will seem remote because AVI systems also will save commuter time, while fighting car theft and air pollution. Use of Social Security-based data matching amounts to making Social Security a national identification system, but it will save taxpayers millions in child support alone. Finally, ANI systems might make life easier for telemarketers at the expense of individual privacy, but they will also help 911 operators smoke out false alarms and efficiently direct emergency services to the real thing. “Efficiency” will make low-level, automated surveillance of consumers an unavoidable fact of life in the decade ahead.

CONSUMERS WILL RESPOND BY SEEKING NEW KINDS OF PRIVACY

In this environment of rising surveillance, individuals can and will do more—for a price. Today, consumers wanting telephone privacy can opt for an unlisted number. De-listing was free once upon a time, but today, one

must buy anonymity from the phone company. In California, the charge for de-listing is thirty cents a month for “special handling costs.” Transactional anonymity is also possible at the sales counter, but at real cost in inconvenience and hassle—consumers can use cash, which they must remember to carry. Similar strategies can be pursued elsewhere as well. Frequent Flyer programs amount to an economic bargain in which the airline buys brand loyalty and demographic information for ticket discounts. Flyers can opt for some measure of anonymity in their travel, provided they are willing to forego mileage-related travel awards. The same will soon become true for groceries, as more and more supermarkets implement “frequent buyer” programs designed to capture preference information. Consumers will be able to retain their anonymity, but only at the cost of lost discounts.

PRIVACY AND SOLITUDE WILL BECOME STATUS ITEMS

As privacy and anonymity become more costly luxuries, they will become a badge of status, and being connected a sign of social inferiority. For example, a decade ago, phone beepers were status symbols carried by cardiac surgeons and captains of industry. Today, they are required wear for repair persons and maids. Tiny cellular phones are the current executive perk, but by decade’s end, they will be heading the way of the beeper, replaced by more sophisticated devices with built-in call screening.

As connectivity becomes the inexpensive norm, anonymity and “disconnectivity” is certain to gain in status. Telecommuting has been pushed as a solution to our commuting woes, but the same tools will enable a new elite of nomadic executives to run businesses from distant Shangri-las while their employees are talking on cellular phones in traffic jams. Delightful places like Santa Fe and Aspen already are seeing the first such executives move into the neighborhood. Anonymity behind gated drives is the norm. The less wealthy will seek out their solitude in the form of holidays to resorts that offer packaged isolation in the same way that resorts like Club Med offer relaxation today.

IMPLICATIONS

As data collection, analysis, and dissemination continue to grow, the consumer search for anonymity and solitude will swell into an activity that will complicate the process and even spawn new industries. A few of the more interesting implications follow:

- *Passive resistance to data collection and analysis.* The days of blindly filling out applications are numbered. Consumers are increasingly likely to question the need for certain information when applying for credit cards and the like. And they will also ask about the uses of information provided and the security it is afforded. A minority will take things a step further, actively confusing the process with false or misleading information—guerilla data-tage.

- *Privacy and anonymity consultants emerge.* Currently several private consumer groups offer advice on how to tailor one's data profile and seek out anonymity. As perceptions about privacy and anonymity sharpen, look for a growing number of consultants to offer similar services for a fee.
- *Costs of collecting data rise after the fact.* New technologies will make actual collection and analysis cheaper and more effective than ever, but upstream costs occasioned by legal restrictions and security obligations will make the data business more expensive than ever. One wild card is that certain kinds of data become the information equivalent of hazardous waste, so dangerous that no one wants to collect or keep it.
- *Solitude will become a status symbol.* The ultra-rich will also be envied as the ultra-private, their wealth buying them anonymity and privacy. Instead of "lifestyles of the rich and famous," it will be "lifestyles of the rich and invisible."
- *Technologies will be used to enhance solitude.* Unlike Kinski, the ultra-private will seek a special kind of one-way solitude, using computers and communications to stay on top of outside events even as they jealously guard their privacy. Mail filters and automated call screening will be sure bets in the decade ahead, helping the elite create solitude-preserving information "black holes" that provide them with broad world views while preserving privacy and anonymity. These same tools will gradually filter down to ordinary consumers, as we all seek one-way filters between us and the outside world.
- *Consumers will invade one another's privacy.* Fears over personal privacy and solitude will lead to increased desires to peek over the neighbor's fence. Suspicious spouses will record their mates' phone conversations, managers will eavesdrop on employee conversations and electronic mail and private detectives will be busier than ever.

—Paul Saffo