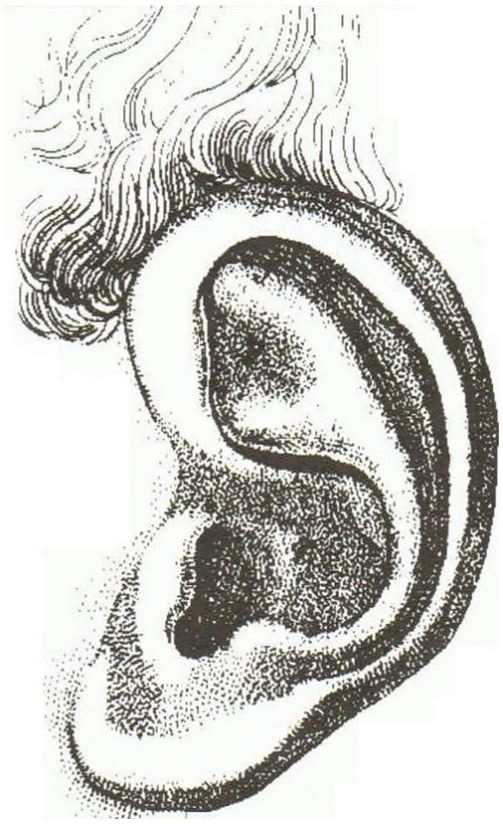
PRIVACY IN THE MILLENNIUM

By Gary T. Marx

Author's note, 2020: Beware of social (or other) scientists bearing predictions! (A few we missed were the emergence of the civil rights movement, the ending of the cold war, global warming plus…!) Yet I take some modest satisfaction from these predictions coming true. The satisfaction is in the predictions' accuracy, not the consequences of their veracity. When written in the early 1990s the internet was in its infancy. The only prediction missed was that rather than seeing the development of a physical card programmed with a person's medical records, we would instead see the records travel to the Cloud. The article even anticipated Alexa and her family of related tools in noting that "smart homes in which data (electricity, communications, temperature) flows into and out of the home could be part of an integrated system available to monitors." We now know that spy portals like Alexa can directly record our habits, preferences and purchases.

The head of a computer database company providing reports on potential tenants to landlords says, "The more you know about somebody else, the better off everybody is." That highly questionable observation ignores the strategic, aesthetic, diplomatic, and self-definitional aspects of personal information. Yet it is increasingly easy to know "more" about others without their knowledge or consent. Whole new industries have emerged, selling surveillance technology and personal information to marketers, employers, insurers, landlords, government, and individuals. The United States, unlike European countries, treats most personal information as if it were just another commodity to be bought and sold like toothpaste.



What new challenges to privacy will the next decade bring? Eight technologies for surveillance are now being developed or advocated:

- DNA screening and monitoring. Beyond identifying persons likely to develop serious illnesses or to have children at risk of illness, this may lead to claims to identify tendencies to alcoholism, homosexuality, and poor work habits.
- A national health insurance system could merge all individual medical data onto a single smart card. Beneficiaries would be required to have the card as a condition of enrollment (of course you won't have to enroll – so this can be defined as voluntary.)
- Vehicle and personal tracking systems could collect tolls or determine location.
- Spy satellites, capable of producing images of objects as small as a baseball, may become commercially available.
- Smart image-recognition system could permit computer scanning of faces in large crowds to locate persons of interest.
- Wireless portable personal communication devices would lend themselves to interception, and to place and time tracking – for billing purposes.
- Smart homes in which data (electricity, communications, temp-erature) flows into and out of the home could be part of an integrated system available to monitors.
- Electronic highways could integrate commercial, entertainment, and communications transactions. Even if much of this is protected by an encryption

system provided by government, one must ask whether the government can be trusted to invade privacy on with an appropriate court order. If the conclusion is no, then government-sponsored encryption, offered as a privacy protection device, becomes a threat to privacy.

Apart from incursions by new technologies, we are likely to see the continued blurring and crossing of the line between public and private places and between work, travel, and home. These have traditionally helped to maintain privacy. "Public" places such as shopping malls, theme parks, university campuses, large apartment and housing complexes, and industrial parks are increasingly legally defined as private places permitting whatever surveillance their owners deem appropriate. Fast-track employees who are given car phones, beepers, and home fax machines and computers by the company are always on the job – evenings, weekends, and vacations – and their communications and location and accessible to their employer.

Finally: if we think of privacy invasion as not only taking something from the individual, but covertly intruding upon the individual, our attention should also be focused on evolving technologies for subliminal communication through radio, television, and computer screens; aromatic engineering that attempts to affect behavior; dietary engineering, which attempts to affect behavior through food combinations and chemical additives; and microwave harassment and mind-control efforts.