

# A Database Nation?

## Security and New Challenges to Privacy

*Minhaj Siddiqui*

---

**W**hen you enter a department store, a camera pointed at the door most likely records your face. Imagine a world in which this surveillance doesn't end there. A computer matches your face to your name using records that the Department of Motor Vehicles sold to commercial interests. It then searches for your name in databases obtained from major credit card companies to see what your consumer preferences are and to check your credit history. Your income bracket can be estimated by searching for your neighborhood of residence in a phone directory. With all this information at hand, salespeople can now decide not only whether it is worth their time to approach you, but what products to push at you. The same system can consult police records to check if you have broken the law in any way, ranging from murder to an unpaid parking ticket. The police can be notified at that point to arrest you.

All this because a camera is pointed at the doorway.

Granted, talk of privacy issues tends to take on a tinge of paranoia, but the scenario may become reality in the near future. The potential for abuse of such invasive technology is great. With so much to gain from increased knowledge of its consumers, commercial interests are sure to take advantage of consumer profile databases as they are compiled. Similarly, other industries such as health care providers and even the government have much to gain from the knowledge found in these databases.

Similar issues are raised by Simson Garfinkel in *Database Nation: The Death of Privacy in the 21st Century*. In this book, Garfinkel, an MIT and Columbia graduate with a strong background in computer privacy issues, illustrates the dangers associated with a society that does not act to control abuses in invasion of privacy. He then calls for action from society to avoid such a future. The concept of privacy is important to define in this discussion. Many will hear talk of protecting privacy and feel as if they need not partake because they have nothing to hide. The privacy being discussed here is of a very broad nature encompassing the characteristics that allow individuals to



distinguish themselves from others. The threat to privacy is not a loss of privacy in the sense that criminals can no longer run illegal drug cartels from inside VCR repair shops; it is the loss of the right to keep any type of knowledge, whether it be a disease or a political thought, away from those who would use that information against the individual. This loss of privacy under the most extreme circumstances would allow HMOs to deny service because the person's complete medical history is an open book. Further, HMOs could access that person's DNA profile, obtained when they donated blood, with its interpretation as to what ailments may later affect the individual.

The threat, as described by Garfinkel, only grows from there. A loss of individual privacy may not only mean others knowing too much, indeed maybe even more than the person knows about him or herself, but as the use of this knowledge becomes more universal, a basic database entry error could destroy a person's lifestyle. Even today there exist a few very central information-gathering services that have the sole purpose of compiling large databases about people. Key examples are the three major credit report bureaus, Equifax, Experian, and Trans Union, all of which maintain extensive databases of credit information (credit cards, bank accounts, loans, etc.) for everyone in the United States. If someone develops a "bad credit rating," these are the companies from which that knowledge is found. In the field of medicine, the Medical Information Bureau (MIB) is in charge of maintaining a database of all major diagnoses that a person has had in his or her lifetime. Each person has a series of codes associated with his or her name, with diagnoses ranging from heart problems or AIDS to codes indicating dangerous lifestyles such as "adverse driving records, hazardous sports, or aviation activity."

Now suppose that some day a person's record, out of the millions that pass through these corporations every day, has an error: instead of "stomachache," the code for HIV was recorded. In a future of no privacy, this person may encounter discrimination, having sudden difficulties obtaining any type of health or life insurance or being harassed in the workplace. Management may refuse a promotion for fear

that he or she will not live much longer and thus would be a poor investment to train. Other companies may refuse to hire the person for similar reasons. If this person's career requires continuous and close interaction with others, those who could now very easily know the medical condition of this individual may stop coming to this person because of the stigma sometimes associated with AIDS. All this because of an inputting error.

To exacerbate the problem, it is very difficult to change negative reports once established, even if caused from a clerical error. In some cases, people do not even have access to their own files, cannot find out what is being said about them, and thus cannot even check whether erroneous data is being recorded.

After presenting the problems that a future without privacy may pose, Garfinkel presents possible ways to combat these problems. Privacy-conscious individuals should avoid volunteering information to data-collecting companies by not participating in random sweepstakes that require them to supply a large amount of personal information for the remote chance of winning a prize. Other proposed solutions to protect consumers involve very large-scale national actions with calls to the government urging careful consideration of the issues and the passing of legislation to protect individuals. For example, laws could be passed forbidding any type of database to withhold information from the individual if other corporations use it to judge the person. Similarly, legislation could establish formalized procedures for fighting data that may be recorded incorrectly in some database.

Loss of privacy does not have to be an inevitable result of technological advances in society. This is not to say that privacy must be maintained at all costs; loss of some privacy can be helpful, such as increased ability of police forces to capture and prosecute real criminals. However, especially in the case of commercial interests amassing information about people, a balance needs to be established. It is important that we are cognizant that our privacy can be infringed upon and that the consequences of uncontrolled invasion are indeed great. Act accordingly. ■