# Privacy in a World of Electronic Data: Whom Should You Trust?

We live in an electronic world, one that has transformed mathematics and mathematical communication. More then ever we are accustomed to sharing what we know and communicating about our work in an open and uninhibited fashion. But our personal data also appear online and in data banks wherever and whenever we act or are acted upon. Many express concerns about the theft of our personal information, but we do little to protect ourselves. Unlike the old world of physical banks where we once placed our money both for security and interest, the new world of electronic data banks holds something much more valuable—our very lives—and our personal information moves in ways that our money never did.

Mobile telephone operators track our every movement, whom we call, and who calls us. Electronic medical records that describe our ailments and treatments, including our hospital billing records, is accessible to a variety of others, such as government agencies overseeing Medicare and Medicaid. Credit card companies and banks record and store the details of financial transactions. Local authorities post information on the value of the property we own. Data warehouses amass personal information on us, details of what we buy, to whom we owe money, for whom we work, what we earn, etc. States and local authorities gather considerable information on us as part of voter registration—such as name, address, telephone number, date of birth, gender, and party affiliation—and voter lists are widely available in electronic form.

We voluntarily share our personal information, our pictures, and our links to our friends and family with social networking sites such as Facebook. That information and more—all the pages you subscribe to—is shared with other vendors and, more often than not, is searchable by others on the Web. Google and other search engine companies track the pages we visit and many of our online activities. Even the words we write—whether in email or in our professional papers—are available and searchable online. Many of the specialized online services we use draw on these data.

There are formal methods for linking data across many of these seemingly separate electronic spheres, using Social Security numbers and other personal identifiers, although often with substantial error. It is no wonder that many ask, "Is privacy dead?'' My answer is, "not quite'', but you will have to be vigilant if you want to protect your information.

In almost every sphere there are rules, supposedly to allow us to protect our data from misuse. But as with Facebook, these are ever-changing and usually too complicated for most people to bother with. Unfortunately, once others have our data, whether they be individuals, private businesses, or even government agencies, we cannot retract the information or restrict how it will be used. Whom should you trust? What can you and should you do to protect your privacy?

Many laws and regulations require businesses and organizations to share their privacy policies with you. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which sets standards for the protection of electronic medical records, also has rules requiring disclosure by doctors and other medical organizations regarding how your information can be used and with whom it can be shared. Read their documents!

It is important to post your research papers online, but think before you post personal information online, whether on Facebook or in some other forum. Do you want your photos and other images tagged and linked to other databases? What would your employer or a future employer think about information posted in your blog? Read the privacy rules and invoke the options they offer for restricting how your data can be used. Make a conscious choice to surrender your privacy, because the decision is irrevocable.

Some government agencies can request our data from other entities, and there are laws to regulate what happens when such data may be disclosed. For example, the Right to Financial Privacy Act of 1978 requires United States federal government agencies to provide individuals with a notice and an opportunity to object before a bank or other specified institution can disclose personal financial information. There are many exceptions to this stricture, however, including for the Internal Revenue Service (IRS) and for cases in which individuals are suspected of illegal behavior, especially terrorist activities.

There are many government agencies whom you can trust with your data and who go to great lengths to prevent the disclosure of your information, both to those inside government and to those outside. For example, the IRS and the U.S. Census Bureau have strict rules to protect the information they gather, and they may release individual information only in nonidentifiable form. Other government agencies, in the United States and abroad, gather data required by law and go to similar lengths before releasing public-use microdata files for research use. How to protect individuals' information has become a major area of research in different parts of the mathematical sciences.

The data deluge has opened up many new avenues for research in mathematics and statistics, including research into methods for protecting individuals' personal information. Proving guarantees of formal privacy requires serious mathematics, and getting methods to scale for databases in our new electronic online world involves innovative mathematical computation. Along with the pursuit of such research, the mathematical and statistical communities should raise awareness of the need to protect other people's privacy. Perhaps the place to begin is with our own data, with ourselves.

*—Stephen E. Fienberg*
*Carnegie Mellon University*
fienberg@stat.cmu.edu

DOI: http://dx.doi.org/10.1090/noti830