Ethics Guide

SECURING PRIVACY

Some organizations have legal requirements to protect the customer data they collect and store, but the laws may be more limited than you think. The **Gramm-Leach-Bliley (GLB) Act**, passed by Congress in 1999, protects consumer financial data stored by financial institutions, which are defined as banks, securities firms, insurance companies, and organizations that supply financial advice, prepare tax returns, and provide similar financial services.

The **Privacy Act of 1974** provides protections to individuals regarding records maintained by the U.S. government, and the privacy provisions of the **Health Insurance Portability and Accountability Act (HIPAA)** of 1996 give individuals the right to access health data created by doctors and other healthcare providers. HIPAA also sets rules and limits on who can read and receive your health information.

The law is stronger in other countries. In Australia, for example, the Privacy Principles of the Australian Privacy Act of 1988 govern not only government and healthcare data, but also records maintained by businesses with revenues in excess of AU$3 million.

Most consumers would say, however, that online retailers have an ethical requirement to protect a customer's credit card and other data, and most online retailers would agree. Or at least the retailers would agree that they have a strong business reason to protect that data. A substantial loss of credit card data by any large online retailer would have detrimental effects on both sales and brand reputation.

Data aggregators like Acxiom Corporation further complicate the risk to individuals because they develop a complete profile of households and individuals. And no federal law prohibits the U.S. government from buying information products from the data accumulators.

But let's bring the discussion closer to home. What requirements does your university have on the data it maintains about you? State law or university policy may govern those records, but no federal law does. Most universities consider it their responsibility to provide public access to graduation records. Anyone can determine when you graduated, your degree, and your major. (Keep this service in mind when you write your resume.)

Most professors endeavor to publish grades by student number and not by name, and there may be state law that requires that separation. But what about your work? What about the papers you write, the answers you give on exams? What about the emails you send to your professor? The data are not protected by federal law, and they are probably not protected by state law. If your professor chooses to cite your

Source: ktsdesign/Shutterstock

work in research, she will be subject to copyright law, but not privacy law. What you write is no longer your personal property; it belongs to the academic community. You can ask your professor what she intends to do with your coursework, emails, and office conversations, but none of these data are protected by law.

The bottom line is this: Be careful where you put your personal data. Large, reputable organizations are likely to endorse ethical privacy policy and to have strong and effective safeguards to effectuate that policy. But individuals and small organizations might not. If in doubt, don't give the data.

DISCUSSION QUESTIONS

1. As stated in the case, when you order from an online retailer, the data you provide is not protected by U.S. privacy law. Does this fact cause you to reconsider setting up an account with a stored credit card number? What is the advantage of storing the credit card number? Do you think the advantage is worth the risk? Are you more willing to take the risk with some companies than with others? If so, state the criteria you use for choosing to take the risk.
2. Suppose you are the treasurer of a student club and you store records of club members' payments in a database. In the past, members have disputed payment amounts; therefore, when you receive a payment, you scan an image of the check or credit card invoice and store the scanned image in a database. Unfortunately, you have placed that database into a shared folder. (See the Security Guide in Chapter 10, pages 414–415.)

   One day, you are using your computer in a local coffee shop. A malicious student watches you sign in. Your name is visible, and your password is very short so it's easy for that student to see what it is. While you're enjoying your coffee, the malicious student learns the name of your computer from the coffee shop's wireless device, uses your login and password to connect to your shared folder, and then copies the club database. You know nothing about this until the next day, when a club member complains that a popular student Web site has published the names, bank names, and bank account numbers for everyone who has given you a check.

   What liability do you have in this matter? Could you be classified as a financial institution because you are taking students' money? (You can find the GLB at *www.ftc.gov/privacy/privacyinitiatives/glbact.html.*) If so, what liability do you have? If not, do you have any other liability? Does the coffee shop have liability?

   Even if you have no legal liability, was your behavior ethical? Explain your answer. In this and in questions 3, 4, and 5, use either the categorical imperative or utilitarianism in your answer.
3. Suppose you are asked to fill out a study questionnaire that requires you to enter identifying data, as well as answers to personal questions. You hesitate to provide the data, but the top part of the questionnaire states, "All responses will be strictly confidential." So, you fill out the questionnaire.

   Unfortunately, the person who is managing the study visits that same wireless coffee shop that you visited (in question 2), but this time the malicious student is sniffing packets to see what might turn up.

   The study manager joins the coffee shop's wireless network and starts her email. Her first message is from a small online Web store at which she has just opened an account. The email says, in part, "Welcome! Your account name is *Emily100* and your password is Jd5478IaE$%$55."

   "Eureka!" says the packet-sniffing, malicious student to himself as the packets carrying that email appear on his screen. "That looks like a pretty good password. Well, Emily100, I'll bet you use it on other accounts, like maybe your email?" The malicious student signs into email using Emily100 and password Jd5478IaE$%$55 and, sure enough, he's in. First thing he reads are emails to the study monitors, emails that contain attachments containing all of the study results. The next day, your name and all of your "confidential" responses appear on the public student Web site.

   Did the person conducting the study violate a law? Did she do anything unethical? What mistake(s) did she make?
4. In question 3, does the online Web site that sent the email have any legal liability for this loss? Did it do anything unethical?
5. In question 2, did the malicious student do anything illegal? Unethical? In question 3, did the malicious student do anything illegal? Unethical?
6. Given these two scenarios, describe good practice for computer use at public wireless facilities.
7. Considering your answers to the above questions, state three to five general principles to guide your actions as you disseminate and store data.