


PAUL, WEISS, RIFKIND, WHARTON & GARRISON

COLLECTING, STORING, USING AND SELLING
CONSUMER DATA: KNOW HOW FAR YOU CAN GO

LESLEY SZANTO FRIEDMAN

PUBLISHED IN *THE BUSINESS RECORD*

MAY 1, 2001



What can smart executives do to reduce their company's exposure to privacy lawsuits and public-relations disasters? Here are some practical suggestions, gleaned from a busy law practice servicing technology-savvy companies.

Some of the features of the Web that attract businesses — personalizing marketing and transactions while cutting costs — are provoking unprecedented concern about personal privacy. Protection of personally identifiable information has become Public Issue No. 1 for many. Internet companies such as Yahoo, Real Networks, Amazon.com and Toysmart.com have recently found themselves in hot water over privacy.

The next victims are likely to be more traditional companies that have recently made the move to the Web. Regulators — the Federal Trade Commission, Attorneys General from each of the states and U.S. possessions, and foreign law enforcement authorities — are eager to seize the initiative on this hot button issue. Consumers, too, have brought scores of class-action lawsuits alleging wrongful use and dissemination of personal information. The potential exposure can be in the billions.

Without addressing any individual company's specific legal needs, here are some tips that executives of companies with websites should keep in mind:

Develop a Privacy Policy that Works. No overarching laws have yet been passed in the U.S. dictating how companies doing business on the Web should handle personal data. But consumer protection and other laws that have long been on the books are now being applied to enforce online privacy rights. Companies having an adequate privacy policy are much better positioned to defend against charges of misuse of personal data. Privacy policies should disclose, at a minimum:

- the types of information collected
- to whom the information is disclosed
- how site visitors can opt out of having their information collected
- how site visitors can access, correct and/or remove personal information previously collected, and
- how the site treats personal information collected from children.

A set of Self-Regulatory Principles that has been endorsed by the executive and legislative branches of the federal government can be found online at www.networkadvertising.org.

Once your privacy policy is in place, keep the promises you have made. Only undertake modifications with care and after giving notice and a new opportunity to opt out.

**This article was reprinted with permission from the
May 1, 2001 issue of *The Business Record*. ©2001**

Don't Overpromise on Privacy. Occasionally a client, in a misguided effort to wear the white hat on privacy, will ask me to draft a sweeping policy. For example, one client wanted to make a flat promise "never" to share customers' personal data with anyone. Resist this temptation. Companies get sued far more often for violating the privacy commitments they made than for not making strong enough promises in the first place. Better to disclose every possible dissemination of customer data up front, even if plans are not currently under consideration for such uses. Some examples are outsourcing of fulfillment, promotional, or data mining functions.

The "click-through" rate on privacy policies is minuscule — less than 1% of most sites' visitors actually bother to read them. Thus, a policy that gives your company flexibility is unlikely to scare off many customers. Yet an overly restrictive privacy policy can hamstring major corporate decisions: for example, positioning for a merger with or acquisition by a firm that values your storehouse of customer information, or consideration of a sale of customer data as an asset in a reorganization or bankruptcy. In today's uncertain economic climate, it is better to keep your options open.

Know the Law. There are new privacy regulations for certain sensitive kinds of data, specifically those relating to health, finances and children. The reach of these new regulations is more expansive than many might realize: for example, the privacy regulations covering "financial institutions" apply not only to banks and investment companies, but also to accounting and tax preparation services, appraisers, car dealerships that do long-term leasing, career counselors in the financial area, check printing businesses, retailers offering private label credit cards, and even travel agencies, if they are operated in connection with financial services. And the new rules cover not only the collection of personal information, but even how it must be stored and secured. Check with knowledgeable counsel to see how these new laws might affect your business. Some of these laws are already in effect, and active enforcement starts this summer.

There are also international considerations: if a firm collects or even just processes personal information about citizens of the European Union nations, the company may be subject to European Union privacy laws. EU privacy laws are considerably stricter than those in the United States. The U.S. Commerce Department has recently developed a "safe harbor," a way for U.S. companies to avoid facing prosecution by European authorities under those stricter laws, by certifying that your company provides "adequate" privacy protection. More information is available at www.export.gov/safeharbor.

Know Thyself. Conduct a thorough audit of information obtained from visitors to your company's website. This includes information relating to product purchases, technical support requests, and voluntarily-given personal information, as well as tracking and storing information concerning visitors through use of "cookies." Don't collect or store information that you don't need or use. The privacy audit can be done in-house or through a reputable consulting firm, but it should be an ongoing effort. Some larger companies, including American Express, Citigroup, Prudential Insurance, and AT&T have even appointed a Chief Privacy Officer to oversee these functions.

Remember, too, that privacy is not just an upper-management issue. Make sure that your PR staff, customer relations personnel, and other front-line employees are up to speed on privacy issues.

Companies heeding the principles mentioned here — instituting an adequate privacy policy, keeping it flexible, staying on top of legal developments, and internally tracking privacy procedures — are far less likely to find themselves on the wrong side of a consumer or regulatory action.

The public, the media, and regulators everywhere are eager to sacrifice the next privacy scapegoat. Don't let it be you.

* * *

Lesley Szanto Friedman is a senior associate in the New York office of Paul, Weiss, Rifkind, Wharton & Garrison.