

New York Law Journal

Technology Today

Tuesday, August 31, 2004

Keeping Promises

It Is Time to Rethink the Boilerplate on Online Privacy Policies

On the Internet, a promise is a promise. That much was made clear last month after the Federal Trade Commission settled a complaint against the Gateway Learning Corporation, the sellers of "Hooked on Phonics."

The FTC charged Gateway Learning with violating its own Web site privacy policy when it rented consumer information to direct marketers.¹

In its privacy policy, Gateway Learning promised that it would not share personal information about its customers with other entities: "We do not sell, rent, or loan any personally identifiable information regarding our consumers with any third party unless we receive explicit consent."

Another statement assured Gateway Learning customers that "We do not provide any personally identifiable information about children under 13 years of age to any third party for any purpose whatsoever."

Gateway Learning's privacy policy also promised customers that if its information sharing practices changed, then it would give them a chance to "opt-out" of having their information shared.

Yet, despite these explicit promises, Gateway Learning in April 2003 began renting personal information provided by its customers — including their names, addresses, phone numbers, age ranges and genders of their children — to direct marketers for mailings and

INTERNET ISSUES



HARRY A. VALETK

Harry A. Valetk, a former trial attorney with the U.S. Department of Justice and an adjunct assistant professor at the Bernard M. Baruch College, Zicklin School of Business, is the director of privacy online for the Entertainment Software Rating Board.

telemarketing calls.

Two months later, Gateway Learning revised its privacy policy to say that "from time to time" it would provide personal information to "reputable companies" whose products or services its customers may find interesting.

Even after making this revision, Gateway Learning continued to rent the personal information collected under the previous will-not-share privacy policy without contacting those customers to inform them about Gateway Learning's revised policy.

Generally, federal law does not require Web site owners to have or post privacy policies. An exception to this rule applies to sites that target children under 13. Those sites fall under the complex purview of the Children's Online Privacy Protection Act.

However, once a site does post a privacy policy, it must abide by the terms of that policy. This means that if a company's policy explains that it collects consumer information, but promises not to share it, that company can't share unless the consumer agrees. Companies that fail to abide by the terms of their own privacy policy can be charged with deceptive business practices under Section 5 of the FTC Act. So it was for Gateway Learning.

In its settlement with Gateway Learning, the FTC included four provisions to address the company's misdeeds. First, the settlement bars Gateway Learning from making future misrepresentations about how it will use data it collects from consumers. Second, the agreement also prohibits Gateway Learning from sharing any personal information collected from customers on its site under the earlier will-not-share privacy policy, unless it first gets their express affirmative "opt-in" consent. Third, Gateway Learning cannot apply future material changes to its privacy policy retroactively without customers' consent. Finally, the settlement required Gateway Learning to for-

feit the \$4,608 it earned from renting its customers' information.

Privacy Policies Exposed

Although arguably resolved, the Gateway Learning case still raises important questions about the current prevalence of deceptive personal information sharing practices online. Do Web site owners protect customer information as promised in their privacy policies?

The answer is unclear. In a comparative study of privacy policies published in January, Michigan State University Professors Robert LaRose and Nora Rifon found that most Web site privacy policies did not have consumers' best interests at heart.²

To the contrary, most privacy policies often contained soothing assurances about consumer privacy with implicit threats that services will be withheld unless personal information is disclosed. Based on their findings, the researchers concluded that Web site owners were using privacy policies not just to inform the Internet public, but also to persuade visitors to give up personal information and ignore lax privacy protection measures that could harm them later on.

Additionally, studies by the FTC examining content of leading commercial Web sites have also found that only 20 percent met the regulatory agency's standards.

All this comes at a time when consumers remain seriously concerned about their privacy. Fear of undue privacy invasions is the leading cause keeping new users from participating in electronic commerce. Research conducted by the Pew Internet and American Life Project showed that 84 percent of Internet users were concerned about the confidentiality of their information online, and 94 percent

wanted privacy violators punished.³

These figures should serve as a wake-up call. Self-regulation has worked to get us this far. But how many more privacy invasions will consumers tolerate before Congress enacts strict rules regulating the content of online privacy policies?

Regrettably, continued privacy violations by a few irresponsible Web site owners may bring an end to the age of

Regrettably, continued privacy violations by a few irresponsible Web site owners may bring an end to the age of industry self-regulation, and escort a new era of governmentally imposed guidelines.

industry self-regulation, and escort a new era of governmentally imposed guidelines.

All site owners should take consumer privacy seriously. Here are five key ingredients to include in a privacy statement that not only comply with the letter of the law, but with the spirit of consumer protection:

- **Use plain English.** When reviewing a company's privacy policy, consumers expect clear explanations about information sharing practices. This is the first step toward making a conscious decision to participate in a Web site's interactive activities.

- **Respect consumer choice.** Most Web sites make broad assurances that the information they collect will be kept confidential. However, companies that give consumers easy access to the personal data collected, coupled with simple procedures for editing or removing it, can go a long way in earning consumer trust.

- **Go outside.** Use of third-party

compliance verification programs is a good way to catch inadvertent disclosures early, gain valuable expertise and maintain the integrity of existing procedures.

- **Don't advertise.** A surprising number of Web sites post advertising and other distracting graphics on the pages containing privacy statements. Selling merchandise on the same page that a company is trying to inform customers about its information sharing practices may be viewed as tactless, and offer little return for the indiscretion.

- **Post warnings.** Above all, keep consumers informed about the risks. If a privacy policy is drafted in a way that tries to convince consumers to disclose personal information, then it should also include explicit warnings about the threats of identity theft, spam, and credit card fraud when disclosing too much sensitive information online. The challenge for Web site owners here is how to educate consumers without prompting avoidance behavior.

Ultimately, the best way to ensure the Internet reaches its full potential is by balancing privacy protections with sound business practices that bolster consumer confidence.

1. At www.ftc.gov/opa/2004/07/gateway.htm (last visited on Aug. 23, 2004).

2. Robert LaRose and Nora Rifon, "Your Privacy Is Assured — Of Being Invaded: Web Sites With and Without Privacy Seals," at www.msu.edu/~larose/es2003post.htm (last visited on Aug. 23, 2004).

3. Susannah Fox, "Trust and Privacy Online: Why Americans Want to Rewrite the Rules," The Pew Internet and American Life Project, at www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf (last visited on Aug. 23, 2004).