



Privacy Patchwork

The “anything goes” frontier is becoming more regulated.

By Alan L. Friel

ARE YOUR CORPORATE Web site and online marketing activities a legal liability that may subject your company to lawsuits or regulatory enforcement action? Recent state legislation has created a patchwork of Internet laws regarding privacy, security, and online advertising similar to those in the e-mail arena prior to the federal CAN SPAM Act. These regulations create a maze of obligations for companies that have corporate Web sites or use the Internet to communicate with consumers. Marketing managers need to be aware of recent legal changes in privacy policies, direct marketing, cyber-security, and certain forms of online advertising.

In the early days of the Web, the general rule was that U.S.-based companies (not subject to foreign jurisdiction) disclosed what personally identifiable information (PII) was collected and how it was used within their privacy policies. A company then strictly followed the policies and was in compliance with legal mandates. Most companies are familiar with the requirements that came from the first wave of regulations regarding marketing to children, health-care information, or financial information. More recently, there is a growing trend to require specific disclosures, notifications, and opt-in/opt-out requirements.

Any company that collects PII from California residents must have a privacy policy on its Web site (California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code, § 22575). The policy must (1) identify all forms of PII collected and with whom such information is shared; (2) provide a description of the process for changing such information, if the process exists; (3) describe the policy change notification process; and (4) identify the effective date of the policy. There also must be a prominent hyperlink to the privacy policy that satisfies specific guidelines. Violation of these requirements or of your own privacy policy constitutes a violation of the law.

It also may not be possible to change an enacted

policy without opening your company to potential claims, even with notice to consumers. The U.S. Federal Trade Commission (FTC) has brought lawsuits against companies that have changed their privacy policies to allow disclosures to direct marketers without first giving customers the opportunity to opt out (e.g., *FTC v. Toysmart.com, LLC*, 2000 U.S. Dist. LEXIS 21963 (D. Mass. Aug. 21, 2000)). The FTC adopted standards requiring an opt-in for material changes to privacy policies in 2000, but has not gone so far in its enforcement actions. FTC staffers are, however, suggesting publicly that such enforcement actions will be brought about soon.

Companies should post privacy policies and include the California requirements. They should not

It may not be possible to change an enacted policy without opening your company to potential claims, even with notice to consumers.

change policies, particularly regarding disclosures to third parties, without giving 30 days notice and providing customers with the opportunity to avoid having information used. Opt-in is recommended, or companies can segregate lists so that the users who accepted older policies continue to be governed by those respective policies.

Beginning in 2005, a California statute will allow customers to demand that companies provide information about what PII has been given to direct marketers and which marketers the information was given to in the preceding calendar year (Cal. Civ. Code § 1798.83). The statute also creates general notice provisions, which require placing a “your privacy rights” hyperlink on the home page or keeping

jacobs & clevenger

information on privacy rights available at places of business. It's possible to be exempt from this statute if customers are permitted to either opt in or opt out of direct marketing disclosures and are notified of this option. To some extent, this statute can be viewed primarily as an incentive to provide a direct marketing opt-in or opt-out for consumers.

Cyber Security

The FTC has promulgated guidelines requiring that Web sites maintain and disclose security procedures. Any representation of security (including not mentioning security at all) will be taken to mean that the company has designated personnel to run a security program and complies with the guidelines listed here. A commercial Web site operator should follow FTC/Better Business Bureau guidelines and (1) employ state-of-the-art technology, (2) keep its employees trained in cyber-security, (3) keep patches and security updates up to date, and (4) keep backups of all data. The FTC requires all Web sites to maintain a comprehensive information security policy, and these requirements are enforceable by civil penalties.

California has also passed legislation creating a consumer notification requirement for companies that have suffered electronic security breaches (Cal. Civ. Code § 1798.82). Any business either in California or with California customers must notify its customers of any breach of security that may have resulted in the theft of sensitive personal information. Notification must be direct or, if costs are greater than \$250,000 or to more than 500,000 people, through mass e-mails, Web site posting, and notification through the statewide media.

Spyware and Adware

The Wild West of Internet advertising today is spyware, a difficult-to-describe genre of computer pro-

grams viewed as both an annoyance and a threat to consumer privacy. The narrow definition of spyware applies to any program that is installed on a user's computer without the user's explicit assent and which monitors a user's computer usage (or other personal information) and sends it back to a third party. Adware, which is sometimes included in the definition of spyware, is a program installed on a user's computer without the user's explicit assent, which monitors the user's Internet usage and uses it to pop up context-based ads. Spyware and adware can be difficult to remove and can interfere with the user's computer or Internet usage sometimes making normal use close to impossible. Cookies, small text files that Web sites place in computers to help browsers remember specific information, are generally exempted from current and pending legislation.

A recently passed Utah statute (Utah Code section 13-40, the "Spyware Control Act") sweeps both adware and spyware in its definition of banned programs. The law requires any program that (1) monitors the computer's usage and (2) either sends information about the computer's usage to a remote computer or server or causes advertisements to be displayed, satisfy certain notice, consent, and uninstall guidelines to escape definition as banned "spyware."

Somewhat more disturbing to the software industry, the statute bans outright the use of a "context based triggering mechanism to display an advertisement that partially or wholly covers or obscures paid advertising on an Internet Web site in a way that interferes with a user's ability to view the Internet Web site." This ban applies even if a user has explicitly assented to the download and the program can be easily removed.

The law is currently being challenged before the Utah Supreme Court by WhenU.com, a desktop global advertising network, on numerous federal and state statutory and constitutional grounds. Assuming the statute is upheld, any Internet businesses or advertisers that have any contact with Utah (including programs being downloaded there, or potential pop ups blocking a company based there) will be faced with numerous obligations. For companies like WhenU.com and Clarion (another purveyor of pop-up ads), with entire business models based on installation and distribution of context-based triggering mechanisms, their business models are essentially prohibited by Utah law if it is upheld.

California appears likely to be the next state to enter the spyware regulation field with a recent bill passing the Senate (S.B. 1436). The California bill takes a somewhat different approach to the spyware problem than that taken in Utah. First, its definition of spy-

Custom reprints

Custom article reprints offer information at a glance at trade shows, conferences, and seminars. They can also be a great way to share with your colleagues some of the cutting-edge research, opinions, and insights featured in *Marketing Management*.

To order reprints of any article in *Marketing Management*, contact Reprint Services at 800-217-7874. For subscription information or to order single copies, call 800-262-1150.

ware is narrower and focuses more on harm to the user or the Internet than on harm to the advertiser. Its notice requirement is less detailed than (but consistent with) Utah's, and there is no mention of an uninstall procedure. There is no general ban on "context-based triggering devices." Liability extends to those who "select and place online . . . or directly to cause placement on a computer" spyware, so advertisers themselves may not be liable under the bill. Causes of action are available only to users, as opposed to in Utah, where they are available only to Web site owners and advertisers. The California law would not prohibit the advertising campaigns of companies that are not themselves installing spyware; it would apply to context-based ad networks, but not to one of their clients. Furthermore, companies like Clarion and WhenU would be able to operate under this law as long as they satisfied the consent requirements.

Finally, there is a risk of trademark litigation against advertisers who use adware providers to advertise online using pop-ups and against the adware disseminators. In *1-800 Contacts v. WhenU.com*, 309 F.Supp.2d 467 (S.D.N.Y. 2003), 1-800 Contacts successfully sued both WhenU.com and

Vision Direct for trademark infringement. Vision Direct used WhenU's software to cause its advertisements to "pop-up" in front of a 1-800 Contacts Web site. Although there is a circuit split on the issue (e.g., *Wells Fargo & Co. v. WhenU.com*, 293 F.Supp.2d 734 (E.D. Mich. 2003)), there is a significant risk of adware-based advertising leading to litigation and liability under both Utah law and federal trademark law. For most companies, the cost of defending such a claim will far outweigh the value of adware advertising, especially given consumers' negative reaction to pop-ups. ■

Author's Note: This article is a summary of issues and not legal counsel. Research assistance was provided by Steven Wright, an associate at Kaye Scholer, and Nathan Meyer, a summer associate.

About the Author

Alan L. Friel is counsel in the Los Angeles office of international law firm Kaye Scholer LLP, where he practices in the areas of advertising, entertainment, and technology law. He may be reached at AFriel@KayeScholer.com.

ADVERTORIAL

Marketing Tool Increases Time To Market, Decreases Costs

SPS Product Review

Imagine an automated, digital marketing tool that increases time to market more than 600% and decreases costs as much as 800%. A group of savvy marketers with decades of experience in creative, sales and technology claim to have done just that by inventing a new tool, the Self Publishing System (SPS), which they say is radically improving the way their customers create and distribute customized marketing materials to sales forces and customers.

Like all new and innovative products SPS can be tough to describe, and it is easier to explain what it does rather than how it does it. Medea's CEO Dave Gurney says, "SPS is the only product that allows anyone with basic computer skills to create and distribute sophisticated marketing materials in virtually any format (PDF, html, print on demand, email and fax) without compromising quality or brand". According to Dave, for a small licensing fee users can "create and distribute customized materials fast, which can easily be published to

websites, pushed out as email attachments, faxed or printed".

Easy to use, affordable, adaptable, high ROI, minimal IT involvement, these are the words that pop up over and over again in the company's case studies which feature interviews with customers who are marketers from Fortune 500 companies within the financial, insurance and trade sectors. So I decided to take a test drive through an Internet demo myself to see if SPS is as good as Medea and its customers say.

I was impressed. It seems that one of the great assets of the system is the ability to empower sales forces within controlled parameters. In the words of an exec from a large insurance company: "A lot of the 'brain dead' admin work we had to do is now in control of the agent who determines information to use individually on their promotional materials within our structure". A major financial institution is also using the system because they say:

"Sales people are very inventive. If we don't give them what they need they create it - we end up with 300 versions of things that are embarrassing". SPS has allowed them to give reps materials such as brochures, newsletters and web pages that look customized even though the bank controls the offering, still leaving room for market adaptation.

Not sure how SPS could work for you? Another customer claims "Medea's experience and SPS technology brought new ways of helping us address issues and find solutions...they were able to understand our needs and show us solutions we wouldn't have asked for because we didn't know they existed".

Sound too good to miss? For more information check out their website at www.medeagroup.com, email info@medeagroup.com or call 1-866-341-9993

Nancy Smith,
Product Review Specialist