Current Privacy Issues Facing Marketers

ROBERT J. DRISCOLL

This article discusses marketing-related privacy and security issues. The author believes that adware, tracking devices, "buzz marketing," children's online privacy, and data collection and security concerns will be hot button issues for privacy advocates in the future.

Recent years have seen an explosion of new media and entertainment platforms and an erosion of the primacy of traditional broadcast and print media. Marketers have followed closely each new technological and marketplace development, rapidly creating new methods to reach consumers via those new platforms and to present marketing messages that can break through media clutter. These new marketing methods—often involving increased customization and use of consumer information—have in many instances given rise to concerns about privacy and data security. Here are five marketing-related privacy and security issues likely to cause headlines in the coming months:

ADWARE

Virtually all Internet users at some point have confronted adware—software applications that once placed on a user's computer serve marketing messages, including pop-up ads, usually triggered by the user's Internet browsing habits. Adware often is bundled with and loaded onto the user's computer along with some other downloadable software application. The fact that the adware program is included in the download

---

Robert J. Driscoll is a partner in Davis Wright Tremaine's New York office and a member of the firm's Advertising and Marketing and Privacy and Security practice groups. He may be reached at robertdriscoll@dwt.com.

This article appeared in Vol. 1, No. 9 (August 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006.

often is stated in the terms and conditions that accompany the download, although whether consumers actually read those terms and conditions is another story. In the worst cases, adware is distributed via "drive-by downloading," i.e., the program loads automatically when the user visits a particular Web site or opens an e-mail message, through a security hole in the user's Web browser or e-mail software.

In the last year, adware distribution practices drew substantial attention from the Federal Trade Commission (FTC). In August 2005, the FTC entered into an agreement with online advertising firm Advertising.com settling FTC charges that the company had violated the Federal Trade Commission Act (FTC Act), which bars unfair and deceptive commercial acts and practices, by failing to adequately disclose that adware was included in a free anti-spyware software download it offered to consumers. The FTC alleged that Advertising.com had distributed online advertisements warning computer users of potential security risks and offering a free download of the software, which was named SpyBlast. The ads included a link to a licensing agreement that disclosed the inclusion of the adware program in the SpyBlast bundle, but consumers were not required to view the license agreement prior to downloading the program. According to the FTC, this means of disclosing to consumers the adware component of the software bundle was inadequate, and the download offer therefore constituted a deceptive trade practice. The FTC may have regarded Advertising.com's activities as particularly egregious because the adware was included as part of a download promoted as a security tool. However, the FTC's analysis made clear that it would regard as unlawful any adware download that does not involve appropriate notice and consent.

State regulators also have cracked down on adware companies. In April 2006, the office of New York State Attorney General Elliot Spitzer announced that it had filed a lawsuit against Direct Revenue, a marketing firm that, according to prosecutors, was responsible for the installation of millions of copies of adware programs on consumers' computers without adequate disclosure. News reports have indicated that among documents secured by the Attorney General in his investigation of Direct Revenue are damning e-mails exchanged by company executives, including one

This article appeared in Vol. 1, No. 9 (August 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006.

in which an executive boasted of his company's "very stealthy" adware program that would "not be caught."

This is not the first time New York's Attorney General has gone after adware companies. In June 2005, the office entered into a settlement with Internet marketing firm Intermix Media, creator of the MySpace.com social networking site, relating to that company's involvement in distributing adware programs. Without admitting any liability, the company agreed to pay $7.5 million to the State of New York as part of the settlement.

The principal focus of regulators and prosecutors so far has been on the adware companies. However, there is some indication that the advertisers whose ads are served to consumers via adware programs may soon find themselves in the spotlight as well. Advertisers typically rely on advertising agencies and media buying firms to create and disseminate advertisements. It is not uncommon for those agencies in turn to look to specialized shops to deal with non-traditional advertising methods, such as online ad distribution. For that reason, advertisers are very frequently several steps removed from the adware companies that distribute the programs that result in the ads' appearance on consumers' computer screens. Recently, however, FTC Commissioner Jon Liebowitz suggested, at an event hosted by the Anti-Spyware Commission, that the FTC might seek to "shame" advertisers whose marketing messages are distributed via adware programs by publicly identifying them and publicizing their involvement with adware. It is not clear whether other FTC commissioners would endorse this approach, or whether direct legal action against advertisers is in the offing. At a minimum, it would be prudent for advertisers to closely monitor all aspects of their online advertising initiatives to ensure their advertisements are being disseminated in a manner that includes appropriate consumer disclosure. Advertisers should also consider including in their agreements with advertising agencies restrictions concerning the use of subcontractors and requirements that agencies adhere to industry "best practices"—including, for example, compliance with the proposed adware guidelines promulgated by TRUSTe—with respect to online advertising programs.

This article appeared in Vol. 1, No. 9 (August 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006.

USE OF TRACKING DEVICES

Another area where new technologies have been adopted in marketing programs is the use of mobile tracking devices such as Radio Frequency Identification (RFID) tags. It has been reported that several major manufacturers have begun using RFID tags to track shipments of products to retailers. For example, according to news reports, the launch early in 2006 of Gillette's new Fusion razor was facilitated by the placement of RFID tags on all cases and pallets of the razors that were shipped to several hundred RFID-enabled store locations of two particular retailers, as well as on promotional displays sent to the stores. According to Gillette, this enabled the company to track the shipments precisely at each step of the distribution chain, with the products reaching those store shelves about 90 percent faster than usual.

In many cases, the use of tracking devices in connection with commercial transactions has led to little public outcry. In others, however, privacy advocates have expressed concern that the next step may be to place RFID tags directly on products that would be purchased by consumers and brought home, with the tags intact. In late 2005, for example, a consumer privacy group objected to plans by Walgreens stores to use RFID technology to track promotional displays in 5,000 stores. As described in news reports, the program would allow packaged-goods manufacturers to monitor the movements of displays and determine when and where the displays actually are placed in stores, making oversight of marketing programs involving placement of materials in multiple geographically dispersed stores much easier. Walgreens disavowed any current intention to place the RFID tags on products consumers could purchase and bring home, or to embed them in customer loyalty cards, but consumer advocates expressed concern that this could represent a movement by Walgreens toward using RFID technology to actually track customers' movements.

Although the Walgreens proposal drew a fair amount of attention, there have already been a few reported instances in which RFID tags have been placed directly on products intended for purchase by consumers. These have included the embedding of tags in packaging for certain Gillette Mach 3 razor blades (as an anti-shoplifting measure) and in

This article appeared in Vol. 1, No. 9 (August 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006.

children's pajamas (as a security measure to combat child abductions), and the placement of tags in a small number of special Coca-Cola cans distributed by the manufacturer as part of a consumer promotion. It has even been reported that a theme park in England intends to start distributing RFID-tagged wristbands to each visitor, apparently to enable them to be tracked and filmed for the purpose of producing a personalized DVD to be made available for purchase at the conclusion of the visit.

So far, these marketing-related uses of tracking technology have not prompted significant legal action. However, laws that would restrict the use of RFID technology (with a particular focus on its use in driver's licenses and identification cards) have been proposed in a number of states in the last two years, although none have yet been enacted.

"BUZZ" MARKETING

Another hot button issue for privacy advocates in recent years has been the increasing prevalence of "buzz" marketing initiatives. Buzz marketing—also known as "word-of-mouth" marketing—in broad terms is the practice of involving ordinary consumers in the creation of goodwill for a product. Marketers have long recognized that the most compelling pitch for a product may be the genuine recommendation of an ordinary consumer to his or her friends or family, and have sought to create marketing programs intended to encourage that honest "buzz" about a product. With the development in recent years of blogging and other newer media formats that facilitate communication among consumers, as well as increasing concerns about consumer "ad fatigue," buzz marketing has become even more widespread in recent years.

Some of the more aggressive buzz marketing practices have raised ethical and privacy concerns. Critics have focused on reports that marketers have paid consumers to spread "buzz" about their products in casual settings, while encouraging those consumers not to reveal their connection with the company whose product is being touted or in some cases even actively seeking to conceal that connection. News reports have also described instances in which marketers have engaged actors to use or promote products in bars or other public locations while posing as ordinary consumers.

This article appeared in Vol. 1, No. 9 (August 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006.

Major marketers and industry groups engaged in buzz marketing assert that their goal is simply to capitalize on consumer excitement about their products and that they expect consumers to deal with others in an honest and open manner, including disclosing payments or other consideration received from a marketer. These concepts are reflected in an ethics code promulgated by the Word of Mouth Marketing Association, which recommends that "word of mouth advocates . . . disclose their relationship with marketers in their communications with other consumers" and "be open and honest about any relationship with a marketer and about any products or incentives that they may have received." To some critics, however, guidelines such as these are not enough. In October 2005, Commercial Alert, a consumer advocacy group, filed with the FTC a request that it investigate companies involved in buzz marketing to determine whether their activities violate the FTC Act's prohibition on unfair or deceptive acts and practices, in particular by failing to provide disclosure of the connections between the companies and consumers who are paid or provided some other benefit to promote the products. The request was particularly critical of buzz marketing efforts involving children and teenagers, noting that they "tend to be more impressionable and easier to deceive."

It remains to be seen how the FTC will respond to Commercial Alert's request. For many years, a fundamental element of the FTC's approach to advertising and marketing matters has been the principle that when material facts exist concerning a marketing message that would affect the consumer's ability to evaluate that message, those facts must be adequately disclosed. With respect to endorsements and testimonials specifically, the FTC has promulgated guidelines making clear that, among other things, "[w]hen there exists a connection between the endorser and the seller of the advertised product which might materially affect the weight or credibility of the endorsement (i.e., the connection is not reasonably expected by the audience) such connection must be fully disclosed." The FTC has stated publicly its view that this principle is fully applicable to non-traditional marketing activities such as product placements and the appearance of paid celebrity spokespersons in entertainment programming, although so far it has not been active in enforcement efforts in these areas. As buzz marketing becomes more and more prevalent, there likely will be

This article appeared in Vol. 1, No. 9 (August 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006.

increased pressure on the FTC to step up its scrutiny of these activities.

Legislation relating to buzz marketing could be on the horizon as well. A bill was introduced last year in Massachusetts that would have required marketers to obtain parental consent before "employ[ing] a child under 16 years of age in connection with a sales force network that distributes, on the Internet or through an online service, marketing communications designed to encourage the purchase, sale, or use of a commercial product or service." The bill was not enacted into law, but if buzz marketing activities draw unfavorable headlines, particularly with respect to the involvement of children, we can expect to see further proposals like it.

CHILDREN'S ONLINE PRIVACY ISSUES

Online privacy is an issue that continues to draw significant attention, particularly as it pertains to children. It is now almost six years since the federal Children's Online Privacy Protection Act (COPPA) took effect, and virtually all Web site operators are now aware of its requirement that operators of child-directed Web sites obtain parental consent in connection with the collection of personal information from children under 13 years old. Nonetheless, there are still many Web site operators who are just now starting to grapple with the substantive details of COPPA compliance. This may be because, as some industry observers have noted, many Web site operators reacted to the legislation in 2000 by simply ceasing the collection of personal information from children under 13. Those operators may have only recently attained a comfort level with COPPA sufficient to allow them to begin offering online activities that involve the collection of personal information from children. For these Web site operators, many questions that arise under COPPA, such as whether there is a need to periodically update parental permissions, and how specifically permission requests should be worded, are new ones.

Another increasingly popular marketing practice that has raised privacy concerns is "advergaming," i.e., the provision of marketing-driven interactive games of which products and brands are an integral part. Data collection is not the only purpose of such games; they appeal to marketers for various reasons, including the young demographic they attract, the substantial amounts of time many gamers spend playing the games, and

This article appeared in Vol. 1, No. 9 (August 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006.

the close interactions between consumer and brand that they can facilitate. Indeed, many of the criticisms that interest groups have expressed about advergaming are premised not on privacy issues, but rather on the fact that such games represent a further blurring of the boundary between advertising and editorial content (a boundary that young children typically are presumed to have difficulty identifying even in the clearest cases). That being said, it has not escaped the notice of critics that many games, in addition to their other marketing benefits, also provide an opportunity for marketers to collect consumer data, whether in the aggregate or from particular players who register with the Web site offering the game. For example, the Web site of one advergame developer promises marketers that "[e]very game generates valuable information, user names, mailing address, sex, age, and when they last used your product. If there is information you want to request from players, our tools facilitate it. You can control how the information is collected and we give you the tools to extract it when you need it." We can expect interest groups to continue to monitor this issue closely in the months ahead. It may also receive some attention from the Children's Advertising Review Unit of the Council of Better Business Bureaus (an industry self-regulatory group that oversees child-directed advertising and promotional materials), which is currently in the midst of a review of its guidelines, including a review of advergaming practices.

DATA COLLECTION AND SECURITY

Marketers continue to grapple with data collection and security issues. In recent years, concerns about consumer privacy and the security of personal information have led to several legislative and regulatory developments affecting marketers, including federal "do not call" legislation and Federal Communications Commission crackdowns on violations of its Customary Proprietary Network Information (CPNI) rules that restrict carriers' ability to use or disclose subscribers' personal telephone records, as well as relatively new data breach notification laws in over 20 states. With a number of widely-publicized data breaches in 2005, consumers are more concerned than ever about the security of their personal information. As marketers race to implement ever more personalized marketing

This article appeared in Vol. 1, No. 9 (August 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006.

initiatives that are closely linked to in individual consumers' behavior, the concerns likely will only increase, and will be reflected in further legislative and regulatory activities.

One specific area that will continue to draw further attention is the collection and storage of personal information by Internet portals, search engines and other Web sites. In February 2006, Representative Edward Markey (D-MA) introduced the "Eliminate Warehousing of Consumer Internet Data Act of 2006," which would require Web site owners to "destroy, within a reasonable period of time, any data containing personal information if the information is no longer necessary for the purpose for which it was collected or any other legitimate business purpose." Many observers quickly pointed out that such a requirement could cripple the online marketing activities of companies who rely on such data to deliver targeted ads, and could also be damaging to search engines who may wish to offer advertisers the ability to target their ads based on consumers' personal information and browsing behavior. They also noted that the bill does not specify at what point information would be deemed "no longer necessary" such that the operator would be required to destroy it (is the information considered "necessary" if the Web site operator plans generally to use it in the future?), or what constitutes a "legitimate business purpose." Nonetheless, as data security concerns continue to mount, legislative proposals like this one are likely to garner substantial support from privacy watchdogs.

This article appeared in Vol. 1, No. 9 (August 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006.

MARKETING PRIVACY ISSUES CHECKLIST

- Adware—software applications that once placed on a user's computer serve marketing messages, including pop-up ads, usually triggered by the user's Internet browsing habits.
- Mobile tracking devices such as Radio Frequency Identification (RFID) tags.
- Buzz marketing is the practice of involving ordinary consumers in the creation of goodwill for a product.
- Marketing practices, such as, "advergaming," i.e., the provision of marketing-driven interactive games of which products and brands are an integral part, which may adversely affect children.
- Data collection and storage of personal information by Internet portals, search engines and other Web sites.

This article appeared in Vol. 1, No. 9 (August 2006) of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006.