January 28 2011

www.ober.com

Happy Data Privacy Day 2011 Online Behavioral Advertising and Privacy

By: Cynthia Blake Sanders

Does online behavioral advertising (OBA) invade consumer privacy? Federal regulators claim that it does and threaten to increase regulation of online advertising if the industry does not soon provide consumers with tools to understand and control what personal data is shared with OBA. “Do-not-track” tools will soon be available so consumers can opt-out of OBA on websites they visit. The ad industry finally responded to the regulators’ requests for “baked-in” browsing tools that offer consumers control over what data may be collected by OBA. The ad industry strenuously objects to any mechanism that could interfere with the free flow of information across the Internet. Objections that now seem swept aside by renewed pressure from the Federal Trade Commission (FTC), the Commerce Department and Congress that the industry take steps now to protect consumers from overreaching OBAs. The industry caved. This week saw announcements from browser developers, ad networks and industry groups of new tools, soon to be released, that may allow consumers to better understand and control how their personal data is used and shared by OBA.

Whether or not do-not-track mechanisms will destroy the Internet as we now know it, change is here. Microsoft, Mozilla and Google each plan to offer a tool for their browsers that will help users opt-out or control data sharing by OBA. Two industry groups, the Digital Advertising Alliance (DAA), a coalition of advertising and marketing industry groups, and the Network Advertising Initiative (NAI), a coalition of advertising networks, are now launching programs that will allow consumers to opt-out of data sharing with OBA. The DAA recently launched a program where ads identified by a small blue triangular icon offer consumers a drop-down privacy menu. The “advertising option icon” links consumers to a relevant portion of the advertiser’s privacy policy and offers the consumer a variety of opt-out choices. The NAI’s tool allows consumers to opt-out of behavioral advertising delivered by NAI member networks.

Even if regulators do not issue regulations targeting OBA, online advertisers’ privacy policies and data security practices will continue to be scrutinized by the

FTC. Advertiser's privacy practices, whether online or offline, that fail to live up to the promises made in their privacy policies may be challenged by the FTC as fraudulent, deceptive, and unfair business practices. The FTC recently challenged two website operators whose privacy policies either failed to adequately disclose their information collection practices or were breached by inadequate data security practices. The circumstances behind the two FTC cases illustrate common privacy pitfalls that can easily be avoided but, if not, may be challenged by regulators as deceptive or fraudulent advertising practices. The remedies sought by the FTC provide a primer on how to satisfy FTC disclosure requirements for OBA, and how to provide adequate data security through technology, policies and best practices.

In 2009, the FTC alleged that Sears failed to adequately disclose its tracking and use of sensitive personal information which it collected using tracking software that was "voluntarily" downloaded by certain loyal Sears customers for marketing research. The tracking software monitored and collected information from the users' internet activities, including activities across third party websites and during secure sessions. Information collected included not only the contents of user shopping carts but online banking transactions, drug prescription records, and video rental histories. Only customers who read to the very end of a lengthy user license agreement during a multistep registration process learned the full extent of Sears' collection, use and sharing of their sensitive personal data. Maybe. How often do we consumers actually read lengthy privacy policies?

To settle the FTC charges, Sears agreed to destroy the tracking software, stop collecting data from consumers who had downloaded the tracking software, and destroy all consumer data collected using the tracking software. Sears further agreed that if it uses a tracking software in the future, it will clearly and prominently disclose the types of data the software will monitor, record, or transmit, and whether the data will be used by third parties. This disclosure must be made to the consumer before installing the tracking software, and must be made separately and apart from other user agreements. A pop-up window (don't forget to de-activate your pop-up blocker) notifying the hapless consumer would suffice.

Twitter, the social media service of the moment, agreed to settle FTC charges related to two data security breaches in 2009 caused by hackers. The hackers managed to guess Twitter's all-lowercase dictionary-word administrative

passwords. Then they could hack user accounts, reset user passwords, access nonpublic user information like direct messages, and send phony Tweets. These breaches violated its privacy policy which promised that Twitter uses "administrative, physical, and electronic measures designed to protect your information from unauthorized access." According to the FTC, Twitter was vulnerable to the hackers because it failed to take even the simplest steps to prevent unauthorized administrative control of its system, including reasonable steps such as:

- using hard-to-guess administrative passwords that are not used for other programs, websites, or networks;
- prohibiting employees from storing administrative passwords in plain text within their personal e-mail accounts;
- suspending or disabling administrative passwords after a reasonable number of unsuccessful login attempts;
- providing an administrative login webpage that is made known only to authorized persons and is separate from the login page for users;
- enforcing periodic changes of administrative passwords, for example, by setting them to expire every 90 days;
- restricting access to administrative controls to employees whose jobs required it; and
- imposing other reasonable restrictions on administrative access, such as by restricting access to specified IP addresses.

To settle these charges, Twitter agreed to not to mislead consumers about its level of protection of users' private information for 20 years and to adopt a comprehensive information security program to be assessed by independent auditors every other year for 10 years.

The moral of the Sears and Twitter cases is that it's imperative for all businesses online, whether social media, publishers, advertisers, agencies, or advertising networks review their privacy policies and data security practices to be certain that: (1) the policies sufficiently, prominently, and clearly disclose the actual collection, sharing and uses made from consumer data obtained with OBA; and (2)

companies' data security and data collection and sharing practices comport with their own privacy policies.

How well would your company's privacy policies and practices withstand regulator scrutiny? Review the Sears and Twitter cases and the measures they were forced to adopt by the FTC. Compare those situations to those of your business. Does your website prominently disclose OBA tracking? What information is collected, how is used, is it shared with third parties, and for what purpose? Can consumers easily opt-out? Do your physical data security practices protect your company and customers? Are you complying with other related privacy laws, such as the Children's Online Privacy Protection Act (COPPA), the CANspam Act, sweepstakes and contest laws, and the Telephone Consumer Protection Act? Do you have an online payment system? If so, is your company complying with the correct PCI Security Standard? Do your social media promotions comply with both the host website's policies and rules as well as your company's policies and rules?

Why comply? So consumers remain blithely unaware of the need to protect their private information and still be safe. The consumer will certainly complain about how icons and pop-up warnings mare the Internet landscape, and how do-not-track settings complicate navigation. Let them vent. Our responsibility is to ensure that consumers continue to freely wander the Internet and help them understand their rights when accepting a free coffee from Starbucks® in exchange for sensitive private information.

Kidding aside, new media and advertising technology is developing so rapidly that remedies for related legal problems continue to lag far behind. However, no new laws are needed to halt deceptive and fraudulent online practices. Such practices may be challenged under existing laws. Thus, it is critical that businesses engaged in online advertising not wait for industry and regulators to resolve the OBA privacy issue. Take steps now to determine and meet "best practices" for your industry to protect your customers and the future of your company.