Privacy and Data Security Law Update

MARY ELLEN CALLAHAN, TULASI LEONARD, AND DANIEL MEADE

BEHAVIORAL ADVERTISING UNDER ATTACK: *WILL LEGISLATIVE AND POLICY INITIATIVES AFFECT ONLINE PROGRAMS AND ACCESS TO CONTENT?*

The area of online "behavioral advertising" — often ill-defined and perhaps misunderstood — is being criticized as anticonsumer on several fronts. Recently, the Federal Trade Commission released draft staff Privacy Principles on behavioral advertising. Behavioral advertising is defined by the FTC to be the tracking of a consumer's activities online — including the searches the consumer has conducted, the web pages visited, and the content viewed — in order to deliver advertising targeted to the individual consumer's interests. Behavioral advertising may be performed by a third-party ad server that has relationships with many publisher web sites to serve ads across the publishers' sites; behavioral advertising can also be performed by the site itself, either on its site or related sites.

Advertisers have become increasingly interested in being more effective in reaching audiences that would be interested in their message,

Mary Ellen Callahan is a partner and Tulasi Leonard and Daniel Meade are associates in the Washington, D.C., office of Hogan & Hartson LLP. The authors can be reached at mecallahan@hhlaw.com, taleonard@hhlaw.com, and dsmeade@hhlaw.com, respectively. Michael F. Mason, Thomas Zeggane, Wim Nauwelaerts, and Mark Brennan assisted in the preparation of this Update.

Published in the May 2008 Privacy & Data Security Law Journal.

while technology has allowed for more granular delineation of inferred interests. Of course, publishers and advertisers note that advertising fuels the vast majority of content available online, therefore the effectiveness of the advertising message is something that should be relevant to the discussion of the value of behavioral advertising. In addition to the FTC's attention on behavioral advertising, as noted below the European Union's Article 29 Working Party has identified behavioral advertising as one of its priorities for 2008-2009.

Following the release of the draft FTC principles, recent attention also has been focused on two state bills in Connecticut and New York that purport to regulate third-party ad servers. Both bills use the Network Advertising Initiative's principles as an initial basis. The Network Advertising Initiative ("NAI") is a self-regulatory group of third-party ad servers that requires the ad servers to work with publisher sites to provide notice of any behavioral advertising on the publisher site and to have the publisher site provide a link to NAI's web site to allow consumers to opt out of behavioral advertising. In addition to the NAI requirements, the state bills would require notice and choice on the third-party ad server site, more consumer control over what and when behavioral advertising occurs, access (within reason) to the data collected, and a moratorium on targeting ads based on "sensitive data" generally. In addition to the legislation, Connecticut Attorney General Richard Blumenthal is endorsing the consideration of a "do not track" list based on the federal do not call list for telemarketing. Civil penalties are proposed in each bill. The New York bill is expected to be amended; therefore its text is in flux.

The questions on everyone's minds are: will these initiatives affect online programs and innovation, and relatedly, would legislation or regulation in this area affect consumer access to free content? With regard to the pending bills, it is unlikely either will pass the legislature this year, although the New York bill in particular appears to be getting increasing attention as part of a competitive squabble among industry leaders in online advertising. If the bill becomes a strategic pawn between several competitors, its language — and its likelihood of passage — will change. Regardless, it is not clear any state law would survive Commerce Clause constitutional scrutiny if challenged.

Even if no law is passed and no final FTC principles are released, the NAI is planning to modify its principles and increase membership. The widespread support for increased education, notice, and choice with regard to behavioral advertising will likely continue. Although consumers are uncomfortable in the abstract with the concept of behavioral advertising, as evidenced by the recent survey that consumer privacy organization TRUSTe commissioned, consumers do embrace free or ad-supported content, as well as receiving information that is of interest to them according to the same survey.

Third-party ad servers and publisher sites in the near future will likely need to improve consumer education efforts and notice about behavioral advertising and its values, and will likely provide more conspicuous choice. At the same time, the concept of ad-supported content is so ingrained in the consumer online experience that efforts such as the state legislative initiatives that may directly or indirectly affect that access may eventually fail if industry can demonstrate the effect legislation may have on access to online content. Companies should continue to improve communications and education on behavioral advertising in order to better educate consumers and legislators about its virtues.

PASSPORT SCANDAL HIGHLIGHTS PRIVACY ACT RISKS

Recent press accounts indicating that government contractor employees may have accessed the passport files of presidential candidates may signal increased scrutiny for contractors and other entities that handle sensitive data for the U.S. federal government.

The passport controversy, which the State Department has suggested involves possible violations of the Privacy Act of 1974, comes on the heels of a highly publicized Government Accountability Office report finding that most government agencies failed to employ adequate controls to protect against the unauthorized access to and disclosure, modification, or destruction of sensitive information. It also comes less than a year after the Department of Homeland Security and the Office of

Management and Budget identified government contracts and data sharing agreements as one of the highest risk areas impeding the adequate protection of government information.

The Privacy Act of 1974 and its implementing regulations constitute some of the government's longest standing data security requirements applicable to companies that do business with the government. The Act regulates the collection, maintenance, use, and dissemination of personal information by government agencies or those working on its behalf. The Act prohibits, subject to certain exceptions, the disclosure of any record contained in a "system of records" without the prior written consent of the individual to whom the record pertains.

Pursuant to the Act, government agencies are required to impose the Act's requirements and prohibitions on government contractors. The Act goes so far as to indicate that a contractor or contractor employee involved in the operation of a system of records would be deemed a government employee for purposes of the Act's criminal provisions.

The implementing regulations require that any contract for the design, development, or operation of a system of records using commercial information technology services or information technology support services must also include certain additional requirements. These include making the contractor's personnel subject to the agency's rules of conduct, listing specific safeguards and controls the contractor must employ, providing for government access to the contractor's facilities and records, and requiring that the contractor contractually bind its subcontractors to the Act.

The consequences for a violation of the Act or the provisions imposed to implement the Act can be severe. In addition to potential criminal and civil liability under the Act, a contractor could see its contract terminated for cause; face third-party litigation; be saddled with adverse performance ratings that negatively impact the contractor's ability to obtain future government contracts; and suffer adverse publicity.

In cases where a contractor has certified or otherwise represented that certain controls or procedures would be employed, a violation could result in allegations under the civil provisions of the False Claims Act. Damages under the False Claims Act include treble damages and up to $11,000 per false claim, which the government might claim under a

fraud-in-the-inducement theory of False Claims Act liability to equate to $11,000 per invoice submitted under the contract.

The recent publicity surrounding government contractors' access to and use of personal information maintained by the government highlights the level of scrutiny the Privacy Act mandates. As a result, government contractors should anticipate that they may encounter increased scrutiny when handling sensitive data, including personal information for the government.

NEW EU GUIDANCE ON PROCESSING CHILDREN'S PERSONAL INFORMATION

PRIORITIES FOR 2008 INCLUDE SOCIAL NETWORKING AND BEHAVIORAL ADVERTISING

On February 18, 2008, the Article 29 Working Party adopted a working document on the protection of children's personal data, extending an invitation to those who handle children's personal data — especially teachers and school authorities — to provide comments on the document.

The working document aims to offer guidance on the general principles relevant to the protection of children's personal data and on how these principles should be applied in the specific context of schools. For the purposes of the working document, a child is any person under the age of 18, unless that person has acquired legal adulthood before that age.

The guidance in the working document is based on the fundamental assumption that children have not yet achieved physical and psychological maturity and thus need more protection than adults. According to the Article 29 Working Party, children's immaturity makes them particularly vulnerable, and this must be compensated by adequate protection and care.

Against this background, the Article 29 Working Party has issued a set of data protection guidelines, which include the following:

- When informing children about their privacy rights, layered notices should be given based on the use of simple, concise, and educational language that can be easily understood by children. A shorter notice including basic information about the data processing should be provided, as well as a more detailed notice providing explanations or additional information that may be relevant.
- Consent to data processing given by a child's representative or guardian loses its validity as soon as the child reaches legal adulthood.
- Children require legal representation to exercise most of their rights, including the right to privacy. However, children have the right to be consulted about how their data privacy rights are exercised, and their own opinions should be taken into account.
- If children are mature enough to detect a breach of their right to privacy, they should have the right to be heard by data protection authorities — in some cases without having to involve their guardians.
- As children are constantly developing, data controllers should pay particular attention to the duty to keep children's personal data up-to-date.

The working document provides further guidance on how to apply general data privacy principles in the specific context of processing of children's personal data at school. Student files, for example, should only contain personal data that are really needed — according to the Article 29 Working Party, data about guardians' academic achievements or occupation may not always be necessary. Processing of personal data that might lead to discrimination (e.g., a child's race or immigrant status) requires proper security: the Article 29 Working Party recommends that such data be kept in separate files that can only be accessed by qualified and designated school personnel.

The transfer of children's personal data to third parties for marketing purposes should always require prior consent of the children's guardians (and of the children themselves, depending on their level of maturity).

The same principle applies to the publication of children's pictures in the press or on a school's web site.

Disseminating personal data via a school's web site should be subject to restricted access mechanisms that require, for instance, prior login via user ID and password. More and more schools are using children's biometric data for access systems (e.g., to enter school premises or cafeterias). The Article 29 Working Party is of the opinion that children's legal representatives should be able to object to such use. If the right to object is exercised, children should be provided with access cards or other access means instead.

The overriding theme in this working document is that for effective protection of children's privacy, the child's best interest should always prevail. The EU Data Privacy Directive (95/46/EC) as well as the E-Privacy Directive (2002/58/EC) should be interpreted and applied accordingly, taking into account the specific situation of children and their representatives.

Following the release of this report on children and data protection, the Article 29 Working Party released its priorities for 2008-2009. For the first time, the Working Party identified Internet-related data protection issues generally and social networking sites and behavioral targeting specifically to be priorities. The themes raised in the protection of children working document will undoubtedly be discussed as the Article 29 Working Party examines the issues of social networking. Furthermore, the Article 29's statements on IP addresses and search engines will likely inform its investigation into behavioral advertising.

WEB SITE FOR GRADING TEACHERS ORDERED TO REMOVE FRENCH TEACHERS' PERSONAL INFORMATION

Note2be.com is a French Web site, launched on January 30, 2008, that purports to provide a collaborative social networking platform for students and parents to "grade" and critique teachers anonymously.

Teachers' unions protested almost immediately.

After receiving several hundred complaints, the French data protection authority ("CNIL") launched on February 13 an emergency investigation of Note2be to assess the site's compliance with French data protection law.

On February 14, several teachers' unions brought a summary judgment action before the Paris First Instance Court, arguing that Note2be's processing of the teachers' personal data constituted a violation of privacy, and seeking the suspension of the processing and removal of personal data from the web site.

On March 3, the court ordered the purging of the personal data of the teachers on the web site as well as on the interactive forum. It also ordered the web site to implement prior review of the forum postings.

The court based its decision on French data protection law, highlighting the requirements that the purpose of the processing of personal data must be defined, explicit, and legitimate while the data collected must be adequate, relevant, and not excessive. Given the lack of prior consent of the teachers, the processing would have been permissible only to the extent the interest pursued by the data controller was legitimate, and not incompatible with the interests or the fundamental rights and liberties of the data subject. The judge held that Note2be's reasons for collection did not outweigh the rights and liberties of the teachers who were data subjects on the web site.

Incidentally, the court noted that the registration of minor students was not subject to prior parental consent.

The decision is noteworthy in light of the speed in which the court and the CNIL reacted to order the modification of a site that allegedly violated French data protection law. Furthermore, the requirement to review all forum comments prior to posting creates a very high standard on which to operate a user-generated content site. It is unclear whether this case is unique given the sensitivity of the circumstances, or whether this is the first indication of the CNIL's desire to increase administrative burdens on user-generated content web sites.

Finally, the dicta as to whether registration of minor students is subject to prior parental consent is inconsistent with the standards set forth in

the Article 29 Working Party's 2008/1 working document on children discussed above. This inconsistency may indicate that the issues associated with collecting personal data from children is far from resolved in the European Union at this time, particularly given the fact that the head of the CNIL, Alex Turk, is the chair of the Article 29 Working Party for 2008.

MANDATORY COMPLIANCE WITH FACT ACT AFFILIATE MARKETING AND RED FLAGS RULES BY THIS FALL

The federal banking agencies (the Federal Reserve Board, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, and National Credit Union Administration) and the Federal Trade Commission issued substantially similar final rules required by the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act") regarding sharing consumer information among affiliates for marketing purposes (Affiliate Marketing Rule), and the prevention of identity theft through the identification of certain "red flags" indicative of identity theft ("Red Flags Rule").

Covered institutions must comply with the Affiliate Marketing Rule by October 1 and with the Red Flags Rule by November 1, 2008. The major portions of these rules generally apply to most corporate users of credit or consumer reports.

Background on Affiliate Marketing Rule

The rule implements the affiliate marketing provisions of Section 624 of the Fair Credit Reporting Act ("FCRA"), which was added by the FACT Act. Though there is substantial overlap with the affiliate sharing provisions of the FCRA, the affiliate marketing provisions implemented by the final rule regulate the use of certain "eligibility information" received by an affiliate, rather than the sharing of certain information by or among affiliates. A consumer's existing right to opt out of the sharing of nontransaction or experience information under the FCRA is not

changed by this rule.

The final rule generally tracks the statutory limitations on the use of "eligibility information," such as consumer-submitted applications, and historical relationship information obtained from an affiliate for marketing purposes; clarifies certain definitions; and provides both examples and certain sample forms that covered entities may (but are not required to) rely upon. The statute and the rule specifically prohibit an affiliate that receives eligibility information from using that information to make a solicitation for marketing purposes unless the consumer (1) receives notice, (2) has a reasonable opportunity and reasonable and simple method to opt out of such solicitations, and (3) does not opt out.

The agencies opted not to adopt special rules regarding pop ads and other Internet-specific marketing, and stated that whether Internet-based marketing is a solicitation will be determined based on the same criteria and facts and circumstances that apply to other marketing media.

Background on Red Flags Rule

The Red Flags Rule was issued pursuant to Sections 114 and 315 of the FACT Act; its primary requirement is for financial institutions and creditors holding consumer or other covered accounts to develop and implement an Identity Theft Prevention Program in connection with both new and existing accounts. The rule specifies that the program must include reasonable policies and procedures for detecting or mitigating identity theft and enabling a financial institution or creditor to:

- Identify relevant "red flags" (patterns, practices, and specific activities that signal possible identity theft) and incorporate those red flags into the program;
- Detect the red flags that have been incorporated into the program;
- Respond appropriately to detected red flags to prevent and mitigate identity theft; and
- Ensure the program is updated periodically to reflect changes in risks.

The rule's other two general provisions require that (1) debit and credit card issuers develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card; and (2) users of consumer reports, such as those issued by credit bureaus, must develop reasonable policies and procedures to apply when they receive notice of an address discrepancy from a consumer reporting agency.

ELECTRONIC HEALTH RECORDS — A STATUS REPORT

When President Bush called in 2004 for the widespread adoption of interoperable electronic health records ("EHR") within 10 years, both public and private efforts to implement a national health information technology plan were set in motion. The Department of Health and Human Services ("HHS") established the American Health Information Community ("AHIC"), a federal advisory body, in 2005 to help advance efforts to meet President Bush's goal.

As AHIC's efforts largely fell short of expectations, HHS Secretary Michael Leavitt announced in January that a $5 million grant had been awarded to establish a public-private successor to AHIC. Known as AHIC 2.0 and recently dubbed "A2," it will be based in the private sector. LMI, a nonprofit government consulting firm, and the Brookings Institution, under a team led by former Centers for Medicare & Medicaid Services Administrator Dr. Mark McClellan, received the grant to spearhead this project. Two million dollars of the grant has been allocated to the LMI-Brookings team, while the remaining $3 million has been earmarked for start-up funding for the new successor organization. Notably, the partnership will also oversee the Healthcare IT Standards Panel ("HITSP") and the Certification Commission for Healthcare IT ("CCHIT"). Additional funding may be allocated to sustain A2 once it is established.

In collaboration with the efforts of AHIC and A2, the Office of the National Coordinator of Health IT ("ONC") has been coordinating and

overseeing the incorporation of a set of health IT standards. In January, Secretary Leavitt formally recognized technical standards for operability, which were developed by HITSP in 2006 and updated before being finalized early this year. The hope is that if these standards become widely known and accepted, they will further enable interoperability of data between EHR systems. Federal agencies and their government contractors are now required by an executive order to incorporate the HITSP standards into new systems or upgrades, or to buy products that comply with them. The secretary's standards for interoperability are also relevant to qualifying for the exception and safe harbor under the Stark and anti-kickback laws, which protect certain donations of EHR systems to potential referral sources.

CCHIT, a nonprofit body that certifies EHR systems, also is playing a role in the development of standards for EHRs. It has been working for HHS since 2005 to develop certification criteria and create evaluation processes in the areas of: ambulatory EHRs (for the office-based clinician); inpatient EHRs (for hospitals and health systems); health networks (through which EHRs and other health-related systems will share information); components of developing personal health records; and EHRs for specialty practices and special care settings.

Congressional involvement in the development and implementation of EHRs is currently focused on financial incentives and electronic prescribing, or e-prescribing. Although likely not to pass Congress in 2008, current bills include:

- The Wired for Health Care Quality Act (S. 1693), sponsored by Sen. Edward Kennedy (D-Mass.), which would offer grants and other financial incentives to encourage providers to purchase and use EHR systems;
- The Promoting Health Information Technology Act (PHIT Act, H.R. 3800), sponsored by Rep. Anna Eshoo (D-Calif.), which would also offer grants to promote the adoption of HIT on the state and local level, in addition to providing incentives for delivering HIT to rural and underserved areas; and

- The E-MEDs bill (S. 2408) introduced by Sen. John Kerry (D-Mass.), which would target incentives to the adoption and use of e-prescribing systems. Specifically S. 2408 would: (1) provide a one-time incentive of several thousand dollars to qualifying physicians to help them purchase and institute an e-prescribing system; (2) establish bonus payments for Medicare prescriptions written electronically; and (3) beginning in 2011, impose financial penalties for those not e-prescribing.

On the state level, a number of legislatures may enact laws to encourage the use of EHRs. West Virginia and New Jersey are both considering bills that would provide financial incentives for the adoption of EHRs. Bills introduced in West Virginia and New Mexico would establish EHR pilot programs, and several other New Mexico bills seek to promote the use of EHRs more generally.

Such state efforts are inevitably intertwined with the debate over data security and privacy; to that end, Oklahoma, Washington, and West Virginia are considering bills that would establish e-health working groups, task forces, committees, or councils to study electronic medical records issues. Oklahoma Governor Brad Henry issued an executive order on January 30 that established the Health Information Security and Privacy council to address these same concerns.

FACT OR FICTION? FACT ACT ACCOUNT NUMBER TRUNCATION REQUIREMENT APPLIES TO ELECTRONIC RECEIPTS

The U.S. District Court for the Southern District of Florida agreed with a consumer that an online retailer's provision of an electronic receipt that included the full credit card expiration date violated Section 113 of the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"),[1] and thus did not grant the retailer's motion to dismiss.[2] Section 113 provides that "no person that accepts credit cards or debit cards for the trans-

action of business shall print more than the last five digits of the card number or the expiration date upon any receipt provided to the card holder at the point of sale of the transaction."

The district court rejected 1-800-Flowers.com's argument that the FACT Act's truncation requirement applies only to transactions where the seller, not the consumer, "prints" the receipt for the consumer at the seller's location, as well as the retailer's argument of the definition of "print." The court found that the ordinary meaning of the term "print" encompasses information included when a seller transmits a receipt electronically, regardless of whether the consumer prints the receipt onto paper or just views the receipt on the computer monitor.

To hold otherwise, the court reasoned, would undermine Congress's aim in passing this provision of the FACT Act, to reduce the chance that a consumer would fall victim to identity theft by virtue of the inclusion of sensitive information on a credit or debit card receipt. The court's finding that the FACT Act receipt truncation provision applies to electronically provided receipts is consistent with another court that considered this issue.[3]

The district court also rejected 1-800-Flowers.com's argument that Section 113 was unconstitutionally vague given that "point of sale" in an online or telephone transaction could be any number of locations. The court stated that the relevant factor is not where the receipt is provided to the cardholder, but rather that the protected information is unnecessary in providing the customer a receipt, and its inclusion on a receipt, no matter where the customer receives it, can lead to identity theft.

This account truncation requirement has been in effect approximately 18 months, and has led to several class action lawsuits. As evidenced by this decision and the 2007 Stubhub decision, the account truncation requirement is essentially "strict liability." Thus, companies not in compliance with their online or offline activities should modify their receipt processes as soon as possible or face the prospect of class action litigation.

Published in the May 2008 Privacy & Data Security Law Journal.

STATES CONSIDER LIABILITY-SHIFTING DATA BREACH LEGISLATION

The majority of U.S. states have already adopted data breach notification laws, but a new trend is underway through which the financial liability associated with data breaches may be shifted from financial institutions to merchants.

Last year, Minnesota adopted a law that would allow a financial institution with compromised customer data to sue the merchant that experienced the data breach at issue if that merchant retained certain customer payment card transaction information for more than 48 hours. Similar bills were also considered, but not adopted, in Connecticut, Illinois, Massachusetts, and Texas. Currently, however, Alabama, Michigan, and New Jersey are considering legislation similar to the Minnesota law, while retailer liability initiatives in Iowa, Washington, and Wisconsin recently were defeated.

Notably, the proposed New Jersey legislation would expand liability for breach costs to businesses, as well as New Jersey's government agencies. In addition, unlike other states where the law would apply only to sensitive credit card verification data held for longer than the authorized time period, the New Jersey law could potentially impose liability on any business or government agency that experienced a data security breach involving personal information as defined in the data breach notification law.

These legislative efforts are designed to reimburse card-issuing banks for costs associated with reissuing cards and protecting affected consumers by making retailers liable for these costs. Most of the proposed retailer liability bills would require merchants to comply with the Payment Card Industry Data Security Standards ("PCI DSS") — industry self-regulatory data security safeguards — or would exempt merchants from liability if they comply with PCI DSS.

The liability-shifting proposals are not a surprising response to the increase in reported data breaches and to the public outcry over the infamous TJX Companies data breach. Nor is it surprising that there is widespread opposition to the laws by the businesses that would face increased liability.

Published in the May 2008 Privacy & Data Security Law Journal.

Retailers have argued that contractual provisions (including the self-regulatory PCI DSS standards) and associated financial penalties preclude any need for legislation in this area. Another concern is the proposal's requirement that merchants delete transaction records within a very short period of time. This standard, already adopted under the Minnesota law, could hamper fraud investigations.

In spite of these concerns, the continued rise in publicized data breaches and the financial burden of such breaches make it likely that more states will consider, and possibly adopt, liability-shifting legislation.

FEDERAL TRADE COMMISSION REVISES COPPA FAQS

On December 27, 2007, the Federal Trade Commission revised questions 27, 30, and 44 of its FAQs about the Children's Online Privacy Protection Act ("COPPA") and its implementing rule. The rule applies to operators of commercial web sites and online services directed to children under 13 that collect, use, or disclose personal information from children, and to operators of general audience web sites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. Operators covered by the rule must, among other requirements, provide direct notice to parents and obtain verifiable parental consent (with certain limited exceptions) before collecting personal information from children.

The revised question 27 expands on the information that must be included in the direct notice sent to parents to obtain consent. Previously, the FAQs advised simply that the direct notice may include a link to the company's privacy policy and also must include "additional information required by the Rule." FAQ 27 now states that even where a link to the company's privacy policy is included, the direct notice must also state that the company wishes to collect personal information from the child and what types of information it wishes to collect, and must provide certain specific additional disclosures when relying on the "multiple-use"

exception, as described below. This modification makes the FAQs expressly consistent with what is required under the rule.

Question 30 addresses a web site operator availing itself of the "multiple-use" exception (whereby the operator may collect the child's and parent's e-mail addresses only in order to send the child periodic communications, including online newsletters, site updates, or password reminders), and requires the operator to make "reasonable efforts" to contact the parent immediately after sending the initial response to the child and before sending any additional responses. The revised FAQ 30 adds: "Note that a Web site operator will not have satisfied the 'reasonable efforts' requirement where he receives notification that the e-mail sent to the parent has bounced back or delivery failed in some other manner."

Question 44 addresses e-cards and forward-to-a-friend scenarios and states that if a company deletes the e-mail addresses provided by the child immediately after an e-card is sent, the company can rely on the one-time contact exception, whereby the company does not need to notify the child's parent or obtain parental consent. However, if the company retains the e-mail addresses for a period of time, the company must notify the parent and provide an opportunity to opt-out of the company's further use of the child's information.

The revised FAQ 44 notes that keeping the e-mail addresses until the message is opened constitutes retention of the e-mail address. Notably, the revised FAQ 44 also states that if an e-card or forward-to-a-friend message discloses the sender's e-mail address or first and last name in the message, the company must obtain verifiable parental consent before such collection and disclosure. Previously, the FAQ was silent as to whether the collection of the sending child's name for the purpose of disclosing such name to the receiving child constituted collection of personal information under COPPA.

The revised FAQ 44 also requires that the company delete "the email addresses provided by the child," whereas the previous FAQ required deletion of "the child's e-mail address." It appears that all e-mail addresses provided by the child, including a parent's e-mail address and the receiving child's e-mail address, would have to be deleted immediately in order to comply with the revised FAQ.

WIRELESS TRADE ASSOCIATION RELEASES DRAFT PRIVACY GUIDELINES FOR LOCATION-BASED SERVICES

CTIA — The Wireless Association®, a trade association of wireless carriers, equipment manufacturers, and other service and application providers, recently circulated a draft set of industry Best Practices and Guidelines for protecting user privacy and security with regard to location-based services ("LBS"). The voluntary guidelines are designed to cover current and future LBS offerings across nearly all wireless technologies and mobile devices.

As currently drafted, the guidelines would apply to all "LBS Providers," which include carriers and third-party application providers that access and/or provide location information as part of a service offering. The guidelines generally would be triggered in situations where "the LBS user is identified or his or her location information is linked to other personally identifiable information by the LBS Provider." Depending on the specific offering, the carrier or third-party application provider — or both — may be considered LBS Providers for the LBS offering.

The draft guidelines focus on user notice and consent. Thus, under the guidelines, LBS Providers must inform users about how location information will be used, disclosed, and protected. They also must provide users with (1) choices as to when (or whether) location information will be disclosed to third parties, and (2) the ability to modify those choices. The guidelines do not establish a specific format, placement, content, or delivery method for LBS notices, but require that such notices be "in plain language and be understandable" and not "misleading." Moreover, the guidelines give LBS providers the flexibility to obtain informed consent via both express and implicit methods.

One issue the draft guidelines do not confront is the extent to which an LBS Provider can avoid compliance if LBS data is not linked to a subscriber's personally identifiable information. This could occur, for example, where an LBS application is used to generate an advertisement or promotion on a handset based on the subscriber's location without regard to the subscriber's identity. Another issue the draft guidelines do not —

Published in the May 2008 Privacy & Data Security Law Journal.

and, for practical reasons, probably cannot — confront is how the activities of third-party mobile application providers that are not CTIA members or working with such members (and who thus may not comply with the guidelines) will affect the long-term prospects of government regulation in this area. As technology evolves and LBS offerings are put to additional uses, other issues are likely to emerge as well.

The LBS Best Practices and Guidelines were adopted by the CTIA Board of Directors on April 1, 2008.

NOTES

[1] 15 U.S.C. § 1681c(g).

[2] *See Grabien v. 1-800-Flowers.com*, S.D. Fla., No. 07-22235 (Jan. 29, 2008).

[3] *See Vasquez-Torres v. Stubhub Inc*., No 07-1328, C.D. Cal. (July 2, 2007).