VENABLE LLP

the download

DEVELOPMENTS IN E-COMMERCE, PRIVACY, INTERNET ADVERTISING, MARKETING AND INFORMATION SERVICES LAW AND POLICY

ISSUE EDITORS

Stuart P. Ingis
singis@Venable.com
202.344.4613

Michael A. Signorelli
masignorelli@Venable.com
202.344.8050

ADDITIONAL CONTRIBUTORS

Emilio W. Cividanes
ecividanes@Venable.com
202.344.4414

Tara Sugiyama Potashnik
tspotashnik@Venable.com
202.344.4363

Julia Kernochan Tama
jktama@Venable.com
202.344.4738

Kelly A. DeMarchis
kademarchis@Venable.com
202.344.4722

1.888.VENABLE
www.Venable.com

August 2012

In this Issue:

Heard on the Hill

Senate Commerce Ponders Self-Regulation

Under the Chairmanship of Sen. Rockefeller (D-WV), the Committee on Commerce, Science, and Transportation (the "Committee") continues to examine issues of data privacy and consumer protection. On June 28, 2012, the Committee held a hearing titled "The Need for Privacy Protections: Is Industry Self-Regulation Adequate?" This hearing followed up on the Committee's May 9th hearing to review privacy frameworks set forth by the Obama Administration and the Federal Trade Commission ("FTC").

The June hearing focused on efforts by industry to address privacy concerns via the Digital Advertising Alliance's ("DAA") self-regulatory program. The DAA is a coalition of the nation's leading media and marketing trade associations, including the Association of National Advertisers, the American Advertising Federation, the American Association of Advertising Agencies, the Direct Marketing Association, the Interactive Advertising Bureau, and the Network Advertising Initiative. The DAA administers a self-regulatory program that calls for entities engaged in collection of web viewing data to provide enhanced transparency and consumer control.

At the hearing, Chairman Rockefeller expressed his skepticism about self-regulation and pledged to continue supporting legislation and holding hearings to promote adequate consumer protection. In May 2011, he introduced S. 913, the Do-Not-Track Online Act, but the bill has not yet been formally considered in the Committee. During her opening remarks, Senator Ayotte (R-NH) cautioned against rushing toward legislation. She stated that consumers and the market, rather than Congress, are best suited to address concerns.

Mr. Bob Liodice, President and CEO, Association of National Advertisers, speaking on behalf of the DAA, reported on the evolution and progress of the DAA's Self-Regulatory Program for online data collection. He explained that the DAA Program has evolved with the FTC's encouragement, represents industry consensus on an opt-out standard, and is already being expanded to the mobile ecosystem. He emphasized the value realized for consumers through data collection and use, and explained that data collection is critical to the operation and functionality of the Internet.

Senate Examines Facial Recognition Technology

On July 18, 2012, the Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, held a hearing titled "What Facial Recognition Technology Means for Privacy and Civil Liberties" to consider the implications of facial recognition technology in law enforcement and civil applications.

Subcommittee Chairman Al Franken (D-MN) said he called the hearing to raise awareness that facial recognition technology is in widespread use today. He explained that facial recognition raises acute privacy concerns, and that he believes in the fundamental right to control biometric information because it is permanent and inalterable.

Maneesha Mithal, of the Bureau of Consumer Protection, Federal Trade Commission ("FTC"), testified to a number of examples of both beneficial and more invasive commercial uses of facial recognition technology. Ms. Mithal highlighted the FTC's December 2011 workshop on the topic, where participants discussed the increased use of facial recognition technologies due to recent developments such as better cameras and the rapid growth of online photo sharing. She recommended that companies that employ facial recognition technology should provide clear, simple, concise notice of the practice. She also revealed that the FTC plans to issue a report later this year recommending best practices for using facial recognition technologies.

Congress and the States Consider Legislation on Employer Access to Social Media Accounts

Lawmakers in the Senate and House of Representatives have introduced legislation (S. 3074, H.R. 5684) that would amend the Computer Fraud and Abuse Act to make it a federal crime, punishable

by fines, for employers to knowingly and intentionally "compel or coerce" a person to authorize access (such as by providing a password) to a computer that is not the employer's computer, for hiring, promotion or firing purposes, and thereby to obtain information from the computer. The bills would therefore leave room for employers to compel employees to grant access to computers that belong to such employers. However, the bills would also criminalize retaliation against whistleblowers and employees who refuse to provide access to computers that are not an employer's computers. The restrictions on employers would not apply in certain cases: (1) if employees are disciplined or fired for other good cause; (2) if a State wishes to waive the federal law for its own employees or for individuals who work with children; or (3) if federal agencies waive the law for classes of employees who access classified information.

A competing measure introduced by Representatives Engel (D-NY) and Schakowsky (D-IL) (H.R. 5050), titled the Social Networking Online Protection Act, would prohibit employers from requiring or requesting that an employee or applicant provide access to private email or social networking accounts regardless of the computer used. "Social networking websites" are defined to include any site for managing user-generated content, a definition not limited to sites with social sharing features. The legislation also protects whistleblowers and employees who refuse to provide such access. These restrictions would be enforceable by the Secretary of Labor through civil penalties and injunctive relief. The same restrictions would apply to schools and universities that receive federal funding, with respect to the accounts of students and applicants.

These federal legislative proposals echo bills introduced in over a dozen states that would similarly prevent entities from seeking access to individuals' personal online accounts. In May, Maryland became the first state to enact such legislation. Maryland's law, which will take effect on October 1, 2012, prohibits employers from requesting or requiring access to certain personal accounts of employees or applicants and from retaliating against employees or applicants who refuse to provide access. The law specifies that employees may not download certain unauthorized data to their personal accounts, and that employers are not prevented from conducting certain internal investigations. Delaware has enacted password protection legislation that applies to higher educational institutions. Other state measures remain under consideration.

Around the Agencies

FTC and Spokeo Settle Fair Credit Reporting Act Allegations

The Federal Trade Commission ("FTC") settled allegations against consumer data provider Spokeo in what the agency described as its

first case on the sale of Internet and social media data in the employment screening context.1 The case followed several warning letters that the FTC sent earlier this year to mobile application ("app") marketers warning that their background screening apps may be subject to the Fair Credit Reporting Act ("FCRA").2

The federal complaint filed against Spokeo by the U.S. Justice Department, litigating on behalf of the FTC, stated that Spokeo provides "consumer reports" subject to the FCRA because the company assembled consumer information from sources including social networking sites, provided access to individually identifiable data profiles through paid subscriptions, and offered and marketed its data for use in hiring and recruiting job candidates.3 The complaint alleges that Spokeo failed to comply with applicable requirements of the FCRA.

The FTC further alleged that Spokeo employees endorsed company products in online forums without revealing their connection to the company, thereby engaging in deceptive advertising in violation of the FTC Act. In 2009, the FTC issued an update to its guidance on endorsements in advertising, which clarified the agency's views that online commenters should disclose material connections to companies they endorse.4

In addition to paying $800,000 in civil penalties, Spokeo agreed in the settlement to comply with the FCRA, to rectify its advertising endorsement practices, and to comply with reporting and recordkeeping provisions similar to those of other FTC consent agreements.

FTC Requests Further Comment on Its COPPA Rule

On August 1, 2012, the Federal Trade Commission ("FTC") issued its supplemental Notice of Proposed Rulemaking ("NPRM") in connection with its Children's Online Privacy Protection Rule ("COPPA Rule") review.5 The NPRM proposes additional modifications to the COPPA Rule's definitions of terms: "operator," "personal information," "screen name," "support for internal operations," and "website or online service directed to children." The FTC will be taking comments until September 10, 2012.

This NPRM follows and modifies the FTC's earlier proposed rule ("Proposed Rule"), issued in September 2011, to amend the FTC's

---

1 FTC Press Release, "Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA" (June 12, 2012), available at http://www.ftc.gov/opa/2012/06/spokeo.shtm.

2 FTC Press Release, "FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act" (February 7, 2012), available at http://www.ftc.gov/opa/2012/02/mobileapps.shtm.

3 Complaint, *United States v. Spokeo*, CV-12-05001 (C.D.Cal., filed June 7, 2012).

4 16 C.F.R. Part 255.

5 FTC NPM, available at http://www.ftc.gov/opa/2012/08/coppa.shtm.

current COPPA Rule. The COPPA Rule applies to operators of commercial websites and online services directed to children under age 13 that collect, use, or disclose personal information This NPRM follows and modifies the FTC's earlier proposed rule ("Proposed Rule"), issued in September 2011, to amend the FTC's current COPPA Rule. The COPPA Rule applies to operators of commercial websites and online services directed to children under age 13 that collect, use, or disclose personal information from children, and to operators of general audience websites that have actual knowledge that they are collecting, using, or disclosing personal information from children under age 13. The COPPA Rule provides parents with tools to control how personal information about their children is collected online.

When the Commission released the Proposed Rule, it explained that it was seeking to update the regulation to help ensure that it continues to protect children's privacy online as technologies evolve. In its proposal, the FTC explained that the COPPA Rule would continue to apply to children under age 13. Additionally, the Commission noted that the regulation would still only apply to general audience websites and online services when operators have actual knowledge that they are collecting personal information from children.

The Proposed Rule includes several proposed amendments to the COPPA Rule, including among others the FTC's proposals to:

- Expand the definition of "collection";
- Consider the presence of child celebrities and celebrities who appeal to children as factors when determining if a website or online service is directed to children;
- Modify required online privacy policies and direct parental notices;
- Eliminate the sliding scale approach to obtaining verifiable parental consent;
- Create a Commission approval process for identifying new means of obtaining verifiable parental consent;
- Place data security obligations on service providers;
- Implement new data retention and deletion requirements; and
- Include audit and reporting requirements for self-regulatory safe harbor programs.

The Multistakeholder Process on Mobile Transparency Begins

On July 12, 2012, the National Telecommunications and Information Administration ("NTIA") hosted its first multistakeholder process meeting to examine mobile application transparency. Earlier this year the White House released a privacy blueprint and requested that NTIA convene interested stakeholders to develop enforceable codes of conduct. In response, the NTIA hosted a meeting titled, "Providing Transparency in How Consumer Data Is Handled by Mobile Applications." The meeting kicked off NTIA's effort to develop a code

of conduct for providing transparency for mobile apps and interactive services for mobile devices. The next meetings will be held August 22nd and 29th.

Lawrence Strickling, Assistant Secretary for NTIA, greeted the more than 200 people who attended the meeting in person, with another 100 or more joining online. He said that the discussion is "the first step in a journey to develop codes of conduct for transparency in mobile apps." He reiterated that NTIA will act solely as a facilitator of the process, and it will not impose rules or its judgment on the process. He said the purpose of the first meeting is not to reach any consensus, but instead to identify issues for future meetings.

In line with the Assistant Secretary's message, the NTIA conveners guided the discussion to assist the stakeholders in identifying common ground on issues. This process resulted in the stakeholders identifying over 70 substantive points for consideration. On August 1, 2012, NTIA released a list of discussion elements grouping similar substantive points identified by the group into "working lists."6 NTIA has suggested that stakeholders consider these issues in working groups in advance of the August meetings.

In the States

State Attorneys General to Examine Privacy

In June, Maryland Attorney General Douglas Gansler was elected president of the National Association of Attorneys General ("NAAG") and announced that his year-long presidential initiative will focus on "Privacy in the Digital Age." State attorneys general not only enforce the privacy laws of their own states; they also have authority to enforce certain federal privacy restrictions.

Attorney General Gansler, now in his second term, has been active in using his post to scrutinize privacy issues and often describes state attorneys general as "the Internet police." In announcing his initiative, Attorney General Gansler pledged that NAAG will spend the next year "bringing the energy and legal weight of this organization to investigate, educate and take steps necessary to ensure that the Internet's major players protect online privacy and provide meaningful options for privacy control, while continuing to enhance our lives and our economy."7 As a part of this initiative, NAAG will hold a conference in April 2013 focusing on privacy issues. Although the effects remain to be seen, Attorney General Gansler's initiative may lead to increased awareness, and potentially scrutiny, of Internet

6 See NTIA Working Lists Document, available at http://www.ntia.doc.gov/files/ntia/publications/draftgroupings_08012012.pdf.

7 NAAG Website, "2012-2013 Presidential Initiative: Privacy in the Digital Age," available at http://www.naag.org/privacy-in-the-digital-age.php.

privacy issues among state prosecutors nationwide.

In California, Attorney General Kamala Harris recently announced the creation of a new Privacy Enforcement and Protection Unit within her Justice Department.8 This Privacy Unit will be staffed with six prosecutors dedicated full time to enforcing state and federal privacy laws. Joanne McNabb, who previously headed the California Office of Privacy Protection, will oversee the Privacy Unit's consumer education and outreach efforts. The Privacy Unit is located within California's eCrime Unit, which the Attorney General launched in 2011 to focus on cyber crimes.

****

About Venable

An American Lawyer Global 100 law firm, Venable serves corporate, institutional, governmental, nonprofit and individual clients throughout the U.S. and around the world. Headquartered in Washington, DC, with offices in California, Maryland, New York and Virginia, Venable LLP lawyers and legislative advisors serve the needs of our domestic and global clients in all areas of corporate and business law, complex litigation, intellectual property, regulatory, and government affairs.

8 California Attorney General's Office Press Release, "Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit" (July 19, 2012).