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

Ariel S. Wolf
awolf@Venable.com
202.344.4464

Robert L. Hartwell
rlhartwell@Venable.com
202.344.4663

November 2013

In this Issue:

Heard on the Hill

Senator Markey and Representative Barton Reintroduce Do Not Track Kids Act

On November 14, 2013, the Do Not Track Kids Act (S. 1700 and H.R. 3481) was introduced in both chambers of Congress by Sen. Edward Markey (D-MA), Sen. Mark Kirk (R-IL), Rep. Joe Barton (R-TX), and Rep. Bobby Rush (D-IL). The bill's authors have cited increased use of the Internet by kids and teens as creating a need for the legislation. In 2011, Sen. Markey, who was then in the House, and Rep. Barton first introduced the bill in the House, where it stalled. Although now serving in separate chambers, these original sponsors have enlisted new co-sponsors from across the aisle to introduce a bipartisan bill in both the House and the Senate. The purpose of the bill is to amend the Children's Online Privacy Protection Act of 1998 ("COPPA") to include further restrictions for Internet companies seeking to collect and disclose children's and teens' personal and location information.

Unlike COPPA's current coverage, which applies to children age 12 and under, the Do Not Track Kids Act would expand the law to cover teens age 15 and under. The bill would prohibit Internet companies from collecting and disclosing personal information from kids (without parental consent) and from teens (without their consent). Consent from parents (on behalf of their children) and teens would also be required before online behavioral advertisements could be displayed. Additionally, the bill would create a "Digital Marketing Bill of Rights for Teens" limiting the collection of certain personal information. Another provision would create an "Eraser Button," which is a tool that parents and children could use to eliminate personal information made publicly available on the Internet.

House Bipartisan Working Group Continues Discussion on Privacy

On November 14, 2013, the Bipartisan Privacy Working Group of the House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade ("Working Group") held a second meeting to discuss the growing information-sharing capabilities and connectivity of consumer devices, known as the Internet of Things ("IoT"). The Working Group heard from representatives from industry and a former top official

from the Federal Trade Commission. During this meeting, the Working Group participants discussed how the IoT could affect the average consumer through the integration of their household appliances, medical devices, and other "smart" items for everyday use. Participants also examined the extent to which any existing or proposed privacy laws could impact innovation within the IoT space.

On November 20, 2013, the Working Group held its third meeting on consumer privacy issues. The Working Group heard from the Direct Marketing Association ("DMA"), consumer interest groups, and a representative of the academic community. At this meeting, the DMA discussed the results of a new academic study that demonstrated the value of data to the U.S. economy. The DMA reported that data-driven marketing generates an estimated $156 billion annually and fueled more than 675,000 new jobs in 2012.

Around the Agencies

Federal Trade Commission Holds Workshop on "Internet of Things"

On November 19, 2013, the Federal Trade Commission ("FTC") hosted "the Internet of Things" ("IoT") Workshop to explore potential consumer privacy and security concerns involving the flow of data across new technologies. "IoT" is a term that describes the exchange of data enabled by everyday devices. Industry stakeholders and consumer advocates came together to discuss both the impact increased connectivity will continue to have on privacy and lifestyles and ways to ensure personal data is protected. Panel topics included "The Smart Home," "Connected Health and Fitness," "Connected Cars," and "Privacy and Security in a Connected World."

Chairwoman Edith Ramirez began the workshop with opening remarks that highlighted the benefits and ramifications that the IoT can have for consumers. She noted that while the workshop would shed light on benefits and risks associated with increased connectivity of everyday devices, the FTC's ultimate goal was to address how to allow for continued use of devices in a manner that overcomes privacy and security issues. She identified three core elements of the FTC guidelines for privacy in the collection of data: (1) privacy by design; (2) simplified consumer choice; and (3) transparency. Chairwoman Ramirez concluded by encouraging companies to follow these guidelines when dealing with the collection of

data to ensure consumers are informed and protected.

FTC Commissioner Maureen Ohlhausen also addressed the workshop. She commented on the potential the IoT has to benefit consumers and stated that the best approach the FTC can take regarding consumer privacy concerns is "informed action" —namely, (1) conducting policy research and development, (2) educating consumers and businesses, and (3) using traditional enforcement tools.

Jessica Rich, Director of the FTC's Bureau of Consumer Protection, delivered closing remarks, urging industry to take the lead to rethink the framework and to place privacy and data security at the forefront of new products. She concluded by stating that the FTC is not proposing new regulations on this matter, but is preparing a report (that will include some best practices) covering the workshop and related issues.

Federal Trade Commission to Hold Workshop on "Native Advertising"

The Federal Trade Commission's ("FTC") "Native Advertising" Workshop will take place on December 4, 2013. The workshop will serve as a platform to explore possible guidelines for "native advertising." While the FTC has not yet defined native advertising, some examples of the practice include sponsored posts and editorials on websites and social networks.

As advertising increasingly takes on different forms across websites and mobile applications, the FTC is exploring the issue to determine how advertising and publishing companies use disclosure methods to ensure consumers are informed and protected. During the workshop, industry stakeholders, consumer advocates and government regulators are expected to share best practices, regulatory approaches, and research to help develop a framework where native advertising can operate.

Government Accountability Office Report on Information Resellers and the Need for an Enhanced Consumer Privacy Framework

On November 15, the Government Accountability Office ("GAO") released a report to the public on information resellers with regard to the current consumer privacy framework. The report, carried out at the request of Sen. Rockefeller (D-WV), is titled "Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace." The GAO advised

Congress to find a balanced approach by enhancing current privacy laws while ensuring that "any limitations on data collection and sharing do not unduly inhibit the economic and other benefits to industry and consumers that data sharing can accord." [1]

The GAO stated that prescribed federal law altogether and separately, do not address the changes in technology and many do not meet the widely accepted Fair Information Practice Principles ("FIPPs"). The GAO also voiced concerns about new technologies and practices (e.g., mobile devices and online behavioral advertising) used by marketing and other entities that collect personal information, sometimes without the consumer being aware of how the data is being used. The report explained that the GAO's purpose in the study was to address three elements: "(1) privacy laws applicable to consumer information held by resellers, (2) gaps in the law that may exist, and (3) and views on approaches for improving consumer data privacy." [2]

The GAO listed several privacy laws it identified as limited in adequately governing marketing practices with regard to the collection of data and some as not meeting FIPPs, including the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accounting Act (HIPAA), Children's Online Privacy Protection Act (COPPA), Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act (CFAA), Driver's Privacy Protection Act (DPPA), Family Educational Rights and Privacy (FERPA), Video Privacy Protection Act (VPPA), and Section 5 of the Federal Trade Commission Act.

National Institute of Standards and Technology Releases Draft Preliminary Cybersecurity Framework

On October 22, 2013, the National Institute of Standards and Technology ("NIST") released the draft Preliminary Cybersecurity Framework ("Framework") for critical infrastructure. The Framework was developed in accordance with Executive Order 13636 of February 12, 2013 concerning improving critical infrastructure cybersecurity. The Framework seeks to create a voluntary program that could

---

1 U.S. Government Accountability Office, Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace, Report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate, GAO-13-6633, at 46 (September 2013), *available at* http://www.gao.gov/assets/660/658151.pdf

2 *Id*. at GAO Highlights.

supplement existing cybersecurity programs. The voluntary framework may apply to those organizations declared to be part of a critical infrastructure sector. The Executive Order described these sectors as ones that are "so vital to the United States that [their] incapacity or destruction…would have a debilitating impact on security, national economic security, national public health or safety[.]"[3] A few of the sectors that the Department of Homeland Security has identified as critical infrastructure sectors are communications, financial services, energy, and information technology.

The Framework presents a three-part approach to cybersecurity consisting of the "Framework Core," the "Framework Profiles," and the "Framework Implementation Tiers." The Framework Core sets forth details for identifying risks in the context of an organization's business. The Core breaks this task into four elements: Functions, Categories, Subcategories, and Informative References. Functions are meant to organize cybersecurity risks at a high level. The five Functions are:

- **Identify**: This function is where organizational assets and data are identified and risk assessment is done.
- **Protect**: This function is where an organization decides how best to safeguard the identified assets from cyber threats.
- **Detect**: This function is where an organization develops the ability to discover cybersecurity events.
- **Respond**: This function is where an organization decides on plans of action to respond to a cybersecurity event.
- **Recover**: This function is where an organization creates and implements procedures to restore critical infrastructure services after a cybersecurity event.

Within each Function are a set of Categories and Subcategories that cover specific aspects of the function, such as Access Controls and Asset Management. Each category also contains citations to relevant Informative References, such as NIST standards.

The second part of the Framework is the Framework Profiles.

3 Exec. Order No. 13,636, 78 FR 11739 (February 19, 2013).

The Profiles are tools an organization can use to track its progress toward cybersecurity goals. By creating both a current and target profile an organization can see its areas of strength and weakness, and devote resources to where they are most needed. Finally, an organization ranks its progress toward its goals using the Implementation Tiers, ranging from Partial (1) to Adaptive (4), and revises these profiles as time goes on.

One notable addition to the Framework is an appendix discussing privacy and civil liberty protections. Earlier drafts of the Framework had been criticized for lacking details on such protections.

In the Courts

Court Dismisses Class Actions Challenging Use of Third-Party Cookies on Safari Browsers

On October 9, 2013, a federal district court dismissed all of the legal claims raised against four online advertising companies in 25 putative class action cases consolidated as *In Re Google Inc. Cookie Placement Consumer Privacy Litigation*. The cases alleged that consumer plaintiffs' Safari browsers were set to block third-party cookies, but that code embedded in the defendants' advertisements enabled them to place third-party cookies on the plaintiffs' devices. The consolidated complaint charged the defendants with violations of three federal statutes: the Electronic Communications Privacy Act (or "Wiretap Act"), the Stored Communications Act ("SCA"), and the Computer Fraud and Abuse Act ("CFAA"). Plaintiffs also alleged violations of several California state laws against one of the defendants.

The Court, consistent with previous federal decisions involving the use of browser cookies, first held that the plaintiffs lacked standing to bring suit because they failed to allege that they had been injured. The Court found that, even if the defendants had collected plaintiffs' personally identifiable information via cookies, this would not establish that plaintiffs were thereby deprived of the value of the information. The Court went on to reject plaintiffs' arguments that they had standing based on defendants' alleged violations of their privacy rights protected by the Wiretap Act, SCA, CFAA, and California state laws. In a detailed decision, the Court ruled that the defendants' alleged cookie practices did not violate any of these laws.

U.S. District Court Holds Email Address Is Personal Identification Information under Song-Beverly: *Capp v. Nordstrom, Inc.*

On October 21, 2013, the U.S. District Court for the Eastern District of California determined that the California Supreme Court would likely deem an email address "personal identification information" under California's Song-Beverly Credit Card Act ("Song-Beverly," or the "Act"), at Cal. Civ. Code § 1747.08(b). *Capp v. Nordstrom, Inc.,* No. 2:13-cv-00660-MCE-AC, (E.D. Cal. Oct. 21, 2013). The status of email addresses under Song-Beverly was a question of first impression for the court, which made the determination as part of denying defendant Nordstrom's motion to dismiss a class action lawsuit.

The court also concluded that Nordstrom did not meet its burden to show that the plaintiff's Song-Beverly claim is preempted by the federal CAN-SPAM Act.

Section (a) of Song-Beverly prohibits merchants from requiring cardholders to provide "personal identification information" as a condition to accepting a credit card for payment. Section (b) defines "personal identification information" as "information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number" (emphasis added). The plaintiff alleged that Nordstrom, Inc. ("Nordstrom") and other unnamed codefendants asked the plaintiff to provide his email address during a credit card transaction in order to send the plaintiff an electronic receipt, but then the defendants used the e-mail address to send the plaintiff unsolicited marketing materials in violation of the Act.

Relying on the California Supreme Court's ruling in *Pineda v. Williams-Sonoma Stores Inc.,* 54 Cal.4th 524, 246 P.3d 612, (Cal. 2011), that "personal identification information" includes ZIP codes, the district court in *Capp* reasoned that the statutory phrase "concerning the cardholder" encompasses an email address because an email address "pertains to or regards a cardholder in a more specific and personal way than does a ZIP code" by permitting direct contact with and implicating the privacy interests of a cardholder, rather than simply referring to the general area in which a cardholder lives or works. Moreover, the court determined that this interpretation is "consistent with the statute as a whole and

statute's purpose."

Marketplace Developments

Revised Payment Card Industry Data Security Standard Released

Version 3.0 of the Payment Card Industry Data Security Standard (PCI DSS) was published in early November, three years after the previous update to the standard. The new standard is due to take effect on January 1, 2014, but companies will generally have until December 31, 2014, to come into compliance. Some revisions to the standard, which may require more transition time, will not require compliance until July 1, 2015.

Enforced by the major payment card brands, PCI DSS sets detailed mandates for the security of payment card information that apply to all companies that process credit card data. Verification requirements differ depending on the scale of a company's card processing operations. According to the PCI Security Standards Council, the self-regulatory body that administers PCI DSS, Version 3.0 is generally intended to provide covered companies with more flexibility, promote education and training, and make card security a "business as usual" effort rather than one focused on annual assessments. Some changes are aimed at tackling potential causes of data security breaches, such as malware and password weaknesses. At the same time, the changes are intended to provide more specificity about how compliance with the standard should be evaluated.

Of note for smaller businesses, PCI DSS Version 3.0 clarifies that the use of a compliant payment application does not relieve a merchant of its own PCI DSS obligations; rather, the PCI DSS review should include review of the application's configuration and implementation. The revised standard provides guidance on how to assess PCI DSS compliance for companies that use third-party service providers to store and process card data or to provide other security-related services.

International

Article 29 Working Party Weighs In On Cookie Consent Mechanisms

The European Union (EU) Article 29 Working Party recently released an opinion setting forth "practical" guidance for obtaining consent to the use of cookies or similar

technologies across the EU. [4] The amended 2002 ePrivacy Directive, adopted in 2009, required all EU Member States to implement a local law mandating that websites obtain consent prior to placing cookies or other technologies on a user's device. Member States slowly passed these local laws over the past few years, resulting in a range of different obligations for websites operating across the EU.

Now, the Article 29 Working Party has provided guidance intended to set forth requirements to make a website legally compliant across all Member States. This guidance has four elements:

1. **Specific Information**: Consent must be specific and based on appropriate information. The Guidance makes clear that notice should be "clear, comprehensive, and visible" at the time and place where consent is sought, such as the website's homepage. Information must include the purpose(s) of the cookies and, if relevant, details about third party cookies used on the site. Also, the cookie expiration date and any choice mechanism must be explained.

2. **Timing**: By law, consent must be given before cookies are set or read.

3. **Active Behavior**: Websites must present clear and comprehensive information to users on how they may signify consent. This should appear on the page where users start their browsing experience. Different tools to obtain consent could include "splash screens, banners, modal dialog boxes, browser settings etc." Browser settings are appropriate where the website operator is "confident" that the user is fully informed and has actively configured their browser in response. The Guidance also supports use of a positive action or active behavior, such as clicking a button or link, or ticking a box. The Guidance makes clear that any user who enters a website and is shown information on cookies, but does not undertake an active behavior, has likely not consented to the use of cookies.

4. **Real Choice—Freely Given Consent**: Users must have the opportunity to freely choose to accept or decline some or all cookies. Granularity in choice is recommended, and the Guidance recommends that

4 *Available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.

websites refrain from using consent mechanisms that only provide an option to consent without further choice. This choice should extend to "tracking cookies," used for online behavioral advertising, and the website should obtain "unambiguous consent" to this type of cookie.

****

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.