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

Kelly A. DeMarchis
kademarchis@Venable.com
202.344.4722

Tara Sugiyama Potashnik
tspotashnik@Venable.com
202.344.4363

Julia Kernochan Tama
jktama@Venable.com
202.344.4738

Ariel S. Wolf
aswolf@Venable.com
202.344.4464

1.888.VENABLE
www.Venable.com

January 2013

In this Issue:

Heard on the Hill
- Congress Updates the Video Privacy Protection Act
- Congressional Developments in Mobile Privacy

Around the Agencies
- FTC Updates COPPA Rule
- Mobile Privacy Still High on Agencies' Agendas
- New Breach Notification Standards for Health Information

International
- European Parliament Issues Report on Proposed General Data Protection Regulation

Heard on the Hill

Congress Updates the Video Privacy Protection Act

On January 10, 2013, President Obama signed the Video Privacy Protection Act Amendments of 2012 (P.L. 112-258) (the "VPPA Amendments Act"). The new law updates the Video Privacy Protection Act ("VPPA") by allowing consumers to consent to having their video viewing records shared automatically for up to two years. The VPPA Amendments Act also adds requirements for obtaining such consent whether online or offline.

Previously, consumers were required to grant consent for entities to disclose their video viewing records at the time of each intended disclosure. Proponents of the VPPA Amendments Act argued that the development of social media sites and new technologies such as video content platforms made the structure of obtaining consent cumbersome and outmoded.

The VPPA, as amended, now states that consent for disclosure can be obtained in advance and electronically. Thus, for example, a service may now give customers the choice up front to share all of their video viewing choices with their online social networking contacts on a continuous basis.

Whether offline or online, consent will now need to meet three

requirements: (1) must be obtained distinctly and separately from other legal or financial disclosures; (2) may be obtained at the time the disclosure is sought or in advance for a set period of time up to two years (unless consent is withdrawn); and (3) must give consumers a clear opportunity to opt-out of case-by-case or ongoing disclosure.

Other provisions of the VPPA remain in place, such as the ability for entities to disclose consumers' names, addresses, and general subject matter of the viewing material to anyone without affirmative consent, if the disclosure is for marketing purposes and if the video service provider has given consumers the opportunity to opt out of the disclosure.

Congressional Developments in Mobile Privacy

At the close of the last Congress, the Senate Judiciary Committee approved an amended version of location data privacy legislation introduced by Sen. Al Franken (D-MN). However, the bill was not taken up by the full Senate, leaving Sen. Franken to begin the process anew in the 113th Congress. The amended legislation, like the introduced version, would generally require a mobile device user's express authorization prior to collecting geolocation information from a device, subject to narrow exceptions. These restrictions would be enforceable by the Federal Trade Commission ("FTC"), state attorneys general, and private plaintiffs.

Rep. Hank Johnson (D-GA) has also released a discussion draft of legislation on mobile app transparency, titled the Application Privacy, Protection, and Security Act of 2013 ("APPS Act"). The bill would require app developers to provide notice and obtain prior consent to data practices, with the format, timing, and manner of such notice to mobile app be regulated by the FTC. Users would also be able to request that apps stop collecting data from them, and either stop using or delete any data already collected. The legislation would be enforced by the FTC and state attorneys general, but there would be a safe harbor for companies that adhere to a mobile data privacy code of conduct produced through a multistakeholder process convened by the NTIA.

Around the Agencies

FTC Updates COPPA Rule

Following a multi-year review that began in 2010, the Federal Trade Commission ("FTC") has released its updated Children's Online Privacy Protection Rule ("COPPA Rule" or "Rule").[1] Revisions to the COPPA Rule become effective July 1, 2013. Between now and that effective date, the FTC is expected to refine its Frequently Asked Questions to help businesses comply with new aspects of the Rule.

[1] Federal Trade Commission, Final Rule Amendments, Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972 (Jan. 17, 2013).

The COPPA Rule continues to apply to operators of commercial websites and online services directed to children under age 13 that collect, use, or disclose personal information from children, and operators of general audience websites or online services that have actual knowledge that they are collecting, using, or disclosing personal information from children under the age of 13. Now, however, instead of focusing on first parties, the Rule has expanded to cover third parties such as social plug-ins and ad networks as well when they have actual knowledge that they are collecting personal information from a first-party site or service that is directed to children. At the same time, first-party operators of websites and online services will now be strictly liable for the actions of such third parties.

Additional changes to the Rule include an expansion of data considered to be personal information. The COPPA Rule now covers information such as: persistent identifiers that can be used to recognize a user over time and across different websites or online services (e.g., IP addresses and mobile device IDs); screen names that function as online contact information; photos, videos, and audio files containing a child's image or voice; and geolocation information.

Providing notice and obtaining verifiable consent from parents prior to the collection of such personal information from children continues to be a core requirement of the COPPA Rule. Operators of websites and online services also now have data security obligations when working with service providers and third parties, including receiving assurances about how these entities will treat the data. Additionally, personal information may only be maintained as long as reasonably necessary to fulfill the purpose for which it was collected, after which time the data must be deleted.

Mobile Privacy Still High on Agencies' Agendas

Mobile privacy continues to be a topic of interest at key agencies. The Federal Trade Commission ("FTC") released a new report on children's mobile applications in December 2012, shortly before publishing its amended children's online privacy regulation. Entitled "Mobile Apps for Kids: Disclosures Still Not Making the Grade," the report follows up on the FTC's earlier study on children's apps.

In the new study, the FTC compared popular apps' privacy notices to the apps' data collection practices, and raised concerns that many of the examined apps were not providing privacy notices before download and/or were not disclosing certain practices that the FTC views as relevant to parents: in-app purchasing features, data sharing practices, interactive advertising, and links to social media. While the report did not find that any laws were violated, the FTC stated that it will be conducting nonpublic investigations to determine whether certain apps have violated the Children's Online Privacy Protection Act ("COPPA") or Section 5 of the FTC Act. The FTC additionally pledged to develop consumer education on mobile privacy, stated that it will conduct a third study of children's mobile apps in the future,

and encouraged the industry to develop mobile privacy best practices.

The National Telecommunications and Information Administration ("NTIA"), a division of the Commerce Department, is also proceeding with its multistakeholder process focusing on transparency practices for mobile apps. Launched in July 2012, this is the Administration's first multistakeholder effort to implement the White House's "Privacy Bill of Rights" principles through a voluntary industry code of conduct. NTIA has convened numerous meetings attended by industry representatives and consumer interest groups. While several draft codes have been circulated, consensus on key issues remains elusive. NTIA has scheduled additional meetings through the spring of 2013.

In California, Attorney General Kamala Harris recently issued new mobile privacy recommendations that go beyond what current law requires. The report, entitled "Privacy on the Go," is aimed at mobile app developers, app market providers, mobile ad networks, and other entities operating in the mobile app ecosystem. Among other recommendations, Attorney General Harris encourages app developers to use "special notices" or other techniques to alert consumers to data practices that may be unexpected. Trade groups have raised concerns that the recommendations were not adequately vetted before release and will harm innovation and economic growth.

New Breach Notification Standards for Health Information

The Department of Health and Human Services ("HHS") issued final omnibus HITECH Regulations on January 17, 2013.[2] The HITECH Act was signed into law in February 2009 and significantly modified the Health Insurance Portability and Accountability Act ("HIPAA"). One of the key features of the HITECH Act was the establishment of a breach notification rule that imposed a nationwide notification requirement for breaches of protected health information. This rule has been enforced in interim status since 2009.

The new HITECH Regulations, which go into effect on March 26, 2013, will require covered entities and their business associates to comply with the new breach notification rule starting September 23, 2013. This new breach notification rule features significant differences from the interim rule, and could make many more incidents regarding protected health information reportable.

Under the interim rule, the trigger to notify HHS and affected individuals of a data breach was based upon an assessment that a breach must be reported only if it poses a "significant risk of financial, reputational, or other harm to the individual." This trigger has been changed to eliminate the "risk of … harm" threshold, and instead, imposes a threshold that presumes that any "unauthorized acquisition, access, use, or disclosure" of protected health information is a data breach, unless the covered entity or its business associate

[2] The final regulations are available here: http://www.ofr.gov/OFRUpload/OFRData/2013-01073_PI.pdf.

can demonstrate that there is a "low probability" that the protected health information was compromised. The entity must also maintain documentation sufficient to meet that burden of proof, such as by conducting and retaining a written risk assessment. The final rule also identifies some objective factors that must be considered when conducting a risk assessment. These factors include the following:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

According to the new regulation, any probability of harm that is greater than "low" will mean that notification is required for the breach, even if there is no reasonable likelihood of harm to the affected individuals. This new standard could result in more reportable incidents, and increase the burden on companies to perform more formal risk assessments of data security incidents involving protected health information.

International

European Parliament Issues Report on Proposed General Data Protection Regulation

On January 8, 2013, the European Parliament issued two reports prepared by the Parliament's committee of Civil Liberties, Justice and Home Affairs (the "LIBE") on the European Union Proposed General Data Protection Regulation (the "Proposed Regulation") and its draft Directive for law enforcement. Both reports were based on proposals that were released by the European Commission in January 2012. While the law enforcement report is of limited interest to most sectors of the business community, the draft report on the "processing of personal data and the free movement of such data" would – if finalized by the European Parliament – impose significant burdens on the international business community in its dealings with residents of the EU.[3]

The author of the report on the Proposed Regulation, Jan Philipp Albrecht, is a member of the European Parliament from Germany, and has long advocated for more stringent privacy restrictions. Against

[3] The Albrecht Report is available here: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

this background, the Albrecht Report proposed 350 separate amendments to the Proposed Regulation, which itself proposes 91 separate articles and leaves open a number of places for further "delegated" and "implementing acts" in the future. The amendments in the Albrecht Report would significantly lengthen the existing Proposed Regulation, as well as eliminate many of the mandates for delegated and implementing acts, instead replacing them with provisions built into the Regulation.

The Albrecht Report's amendments would strengthen and expand many of the individual consumer rights in the Proposed Regulation. For example, the much discussed "right to be forgotten" in the Proposed Regulation would be amended to be a "right to erasure and to be forgotten." This would expand the data subject's right to have his or her data erased, and impose erasure requirements on data controllers, including requiring them to take certain steps to have data erased even after it has been disseminated to third parties. Another example comes from the proposed right to data portability. As written, the Proposed Regulation would require consumer data to be provided in a "commonly used format" upon consumer request. The Albrecht Report would expand this right to require the data to be provided in an open source format, free of charge.

Despite the extensive proposed changes, the Albrecht Report fully supports the structure of the Proposed Regulation as a "one stop shop" for enforcement across the EU. The European Commission hailed the Report's support for "strong and uniform" regulation. The Proposed Regulation would replace the 1995 EU Data Protection Directive in its entirety.

It remains to be seen how influential the Albrecht Report is in further shaping the Proposed Regulation. At present time, the Albrecht Report remains in draft form; a final version will be voted on by the Parliament later this year.

****

About Venable

An *American Lawyer* 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.