VENABLE LLP

the download

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

Winner of *Chambers* "Award of Excellence" for the top privacy practice in the United States

Winner of *Chambers* "Award of Excellence" for the top advertising practice in United States

Two of the "Top 25 Privacy Experts" by *Computerworld*

"Winning particular plaudits" for "sophisticated enforcement work" – *Chambers and Partners*

Recognized in the *Legal 500* as a top law firm for its outstanding data protection and privacy practice

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

© Venable LLP 2011

JANUARY 2011

In this Issue:

2011 looks to be a busy year for privacy-related matters starting with the upcoming deadlines for comment on the recently released privacy reports by the Federal Trade Commission and the Department of Commerce. In addition, Senators Rockefeller (D-WV) and Kerry (D-MA) are expected to introduce new privacy bills in the coming weeks. It is not yet clear what impact the new Republican majority in the House will have on the timing of the House's consideration of privacy issues, but it is clear that there will be considerable attention to online advertising, data security, cybersecurity, and the commercial uses of data. This issue of the Download includes articles on the Federal Trade Commission's interim report on a proposed framework for how companies could address consumer privacy, the Department of Commerce's report on commercial data privacy, and a newly enacted law that regulates online transactions.

Around the Agencies

Federal Trade Commission's Report on Privacy

The Federal Trade Commission ("FTC" or "Commission") issued its much-anticipated privacy report on December 1, 2010. The report, titled "Protecting Consumer Privacy in an Era of Rapid Change," sets forth the Commission's proposed framework for how companies could address consumer privacy. In addition, Commission staff has expressed support for a universal choice mechanism with respect to online behavioral advertising, sometimes referred to as "Do Not Track." The report

suggests that this mechanism could be achieved either legislatively or through industry self-regulation. Comments on the report are due January 31, 2011. The Commission intends to issue a final report in 2011.

In general, the report provides a detailed, historical context on the evolution of privacy policy. The report calls for best practices, but does not specifically forward any legislative proposals. The report asks numerous questions on how to implement the broader framework, but does not provide much in the way of specific proposals or standards for enforcement at this time. The following is a summary of the key themes from the report.

Privacy by Design. The report calls for companies to promote consumer privacy and security throughout their organizations, business practices, and development of their products and services. This concept includes:

(1) providing reasonable security for consumer data;
(2) collecting only the data needed for a specific business purpose;
(3) retaining such data only as long as necessary to fulfill that purpose;
(4) safely disposing of data when no longer needed; and
(5) implementing reasonable procedures to promote data accuracy.

The report also calls for companies to adopt procedures to promote privacy practices that are scaled to each company's business operations and data practices. These procedures should include appointing personnel to oversee privacy issues, training employees, and conducting privacy reviews when developing new products and services.

Simplified Choice. The report calls for companies to provide simplified, streamlined choice to consumers with respect to their data practices. The Commission's report does not call for universal choice for all collection and use, but instead has developed a bifurcated approach based on the purpose for which data is collected. The Commission suggests that choice is not necessary when collection and use is done for "commonly accepted" practices such as first-party marketing, product fulfillment, fraud prevention, and other internal operations (e.g., improving services offered and legal compliance).

For data practices that are not "commonly accepted," companies should provide consumers with choice. To ensure consumers are able to make informed and meaningful choices, the Commission states that choice should be clearly and conspicuously described and offered when the consumer is making a decision about providing data.

When offering choice is appropriate, the report provides suggestions on where to offer choice in specific contexts including online and offline collection by retailers, social media, and mobile platforms. For instance, the Commission states that for retailers with direct interaction with consumers online, the disclosure and control mechanism should appear on the page on which the consumer types in his or her personal information. For offline retailers, notice and choice should be provided at the point of sale (i.e., the cashier could ask the consumer if they would like to receive offers from the retailer).

The report does not specify whether opt-in or opt-out consent is required for practices that do not fall into "commonly accepted" practices, and invites comment on this issue.

© Venable LLP 2011

Greater Transparency. The report calls for companies to make their data practices more transparent to consumers by providing clearer, shorter, and more standardized privacy statements. The FTC stated that this approach would permit consumers to compare data practices and choices across companies.

Reasonable Access. The report recommends that companies provide reasonable access to data, particularly those companies that collect information but do not directly interact with consumers such as data brokers. The report states that the extent of access should be proportional to both the sensitivity of the data and the intended use.

Material Changes to Data Practices. The Commission reiterated its position that companies should provide robust notice and obtain affirmative consent for material, retroactive changes to data policies.

Education. The Commission has proposed to undertake a broad effort to educate consumers about data collection and the availability of choices.

Department of Commerce Issues Green Paper Concerning Commercial Data Privacy

The Internet Policy Task Force ("Task Force") of the Department of Commerce ("DOC") issued its green paper on commercial data privacy, entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" on December 16, 2010. The report sets forth the Task Force's proposed framework through which to assess current public policy governing commercial privacy. While the report does not express a commitment to specific policy proposals, it is intended to stimulate public discussion with the goal of identifying more specific proposals to be considered in a future white paper. Comments are due on January 28, 2011.

In general, the report reviews the current status of policy related to commercial data privacy and calls for strengthening the U.S. commercial data privacy framework, especially in the areas of ensuring transparency and informed consent for consumers, while providing guidance to businesses and clarifying the U.S. approach to commercial data privacy. It expresses support for voluntary, enforceable codes of conduct to address emerging technologies and issues not covered by the current application of the Fair Information Practice Principles ("FIPPs"). It also stresses the importance of not hampering the innovation, customer service, and use of new technologies that are a hallmark of online commerce in the U.S. In addition, the report calls for the creation of a Privacy Policy Office within the DOC. The report introduces its proposals as a "Dynamic Privacy Framework." The following is a summary of the key themes from the report.

The framework is organized around five main recommendations:

(1) Adoption of a comprehensive set of FIPPs to protect the privacy of personal information in commercial contexts not covered by existing sectoral law.
(2) Recognize expanding interoperability between U.S. and international data privacy frameworks.

© Venable LLP 2011

(3) Adherence to voluntary industry codes of conduct.
(4) Creation of a new privacy policy office within DOC to focus on commercial data privacy.
(5) Set a national standard for notifications following security breaches involving personal information in the commercial context.
(6) The report sets forth the following policy options for discussion:

Bolstering Consumer Trust Online Through 21st Century Fair Information Practice Principles. The report calls for comprehensive, baseline privacy rules based upon the FIPPs to protect commercial data in areas where it is unregulated by existing sectoral laws—namely, consumer data that is presently largely covered by a notice-and-choice regime. The report expresses no preference for the method of implementation, and mentions legislation, industry self-regulation, greater FTC enforcement of the existing framework, enhanced FTC rulemaking, or some combination of the above as possibilities.

The report pointed to the "enhanced notice" model that has been adopted by the online advertising industry as one example demonstrating that current commercial data privacy policies may be providing adequate incentives to industry to act voluntarily.

Advancing Consumer Privacy Through a Focus on Transparency, Purpose Specification, Use Limitation, and Auditing. The report calls for increased attention to substantive protections, both as part of, and separate from, the FIPPs-based rules it advocates adopting. For transparency, the report calls for privacy policies written in a way that stresses simplicity and clarity. It also suggests the use of privacy impact assessments ("PIAs") in conjunction with privacy notices. PIAs would require organizations to identify and evaluate privacy risks arising from the use of personal information in new technologies or information practices, and to publish this information. They also have the benefit of inducing organizations to think through how their information systems comport with the FIPPs.

The report further seeks increased alignment between consumer expectations and actual information practices, mainly by focusing on two principles—purpose specification and use limitation—which would require an organization to disclose the specific reasons for which it collects information, and then limit the organization to these purposes. The report also calls for increased use of audits of actual data use compared to the stated purposes for which this data will be used.

Maintaining Dynamic Privacy Protections Through Voluntary, Enforceable, FTC-Approved Codes of Conduct. The report expresses concern over privacy practices that do not adapt fast enough, and recommends the adoption of voluntary, enforceable codes of conduct. The report is intentionally ambiguous about who would be writing these codes of conduct, and this ambiguity could be interpreted as calling for the DOC to be the primary author. In that scenario, these codes of conduct would simply amount to regulation by different means. The report cites the Self-Regulatory Code of Conduct adopted by the online behavioral advertising industry as the only positive example of this type of code. The report suggests multiple incentives for developing the codes, including increased encouragement (and enforcement) by the FTC and a safe harbor option for companies who adopt voluntary codes of conduct.

© Venable LLP 2011

The report also sets out a proposal for creating a "Privacy Policy Office" ("PPO") within DOC. It proposes that the PPO work with the FTC to identify areas where new industry privacy codes are needed to implement the FIPPs, and envisions this office as being able to respond quickly to new technologies and to assist industry with developing guidelines for voluntary, enforceable commercial data privacy codes. It envisions that this office will work with the Executive Branch and a number of other government agencies as well as with privacy officers in the private sector.

The report makes clear that the FTC will remain the federal government's primary enforcer of consumer privacy protection for existing and new privacy legislation. But the report leaves the door open for increased enforcement by individual states as well.

Encourage Global Interoperability. In recognition of the obstacles that different international standards for data privacy impose on organizations, the report lists a number of recommendations made by respondents to the DOC Notice of Inquiry for encouraging greater harmony with the laws of other countries in this area. The report stops short of advocating any of these recommendations, and simply encourages greater attention to be paid to identifying and working towards greater international interoperability.

National Security Breach Notification. The report reiterates the frustration that industry feels by having to comply with a patchwork of state data breach notification laws and wants to consider what a national data breach notification law would look like. The report does not make any specific recommendations in this area.

Relationship Between a FIPPs-Based Commercial Data Privacy Framework and Existing Sector-Specific Privacy Regulation. The report also wants further study of what is both good and bad about sector-specific privacy laws, such as HIPAA (health information) and GLB (financial information), and how a comprehensive, FIPPs based framework would interact with these laws.

Preemption of State Law. The report also does not make any recommendations regarding state preemption, and suggests that such preemption could range anywhere from being narrowly tailored to broadly sweeping. The report also seeks further input on the role of State Attorneys General to enforce a national FIPPs-based regime.

Electronic Surveillance and Commercial Information Privacy. The report advocates consideration of reform of the 1986 Electronic Communications Privacy Act in light of the rise of cloud computing and location-based services.

New Online Marketing Law

Congress Passes the Restore Online Shoppers' Confidence Act

In a move to combat allegedly deceptive online sales tactics that result in recurring charges for consumers for membership clubs until cancelled by consumers, Congress passed the "Restore Online Shoppers'

© Venable LLP 2011

Confidence Act." The bill, introduced by Senator Rockefeller (D-WV), was signed into law by President Obama on December 29, 2010.

This law is the product of an investigation started in May 2009 by the Senate Commerce Committee. The focus of the investigation was on membership club enrollment offers that are presented as a free trial and convert to a subscription program after the initial free period. These offers were made by "third-party sellers" after the consumer initiated a transaction with another merchant. In November 2009, the Senate Commerce Committee issued a staff report that found: (1) consumers are not aware at the time of accepting the additional offer that their credit card, debit card, bank account, or financial account information are passed through to a "third-party seller" to be used for subsequent billing, and (2) consumers are surprised to be charged once the free trial has ended, without further communication with the seller of the second product or service.

The law will impose three new obligations for online sellers:

1. Prohibition against data pass (Section 3(b)).

The law will prohibit merchants from sharing financial account numbers and "other billing information" used to charge the customer with "third-party sellers" – sellers who market goods and services online through an initial merchant after a consumer has initiated a transaction. The bill does not specify the types of "other billing information" that will be covered by the law, but does limit the scope to data used to bill consumers. This data pass prohibition will not apply to information shared by the initial merchant with its corporate subsidiaries or affiliates.

2. Restrictions on Internet transactions (Section 3(a)).

The law will require a "third-party seller," before it obtains a consumer's billing information, to clearly and conspicuously disclose to the consumer all material terms of the transaction including:

- a description of the goods or services being offered;
- the fact that the third-party seller is not affiliated with the initial merchant; and
- the cost of such goods or services.

In addition, the third-party seller must obtain the consumer's express informed consent for the charge by:

- receiving from the consumer the full account number of the account to be charged and the consumer's name, address and means to contact the consumer; and
- requiring the consumer to perform an additional affirmative action, such as clicking on a confirmation button or checking a box that indicates the consumer's consent to be charged.

We note that corporate subsidiaries and affiliates of the initial merchant are not "third-party sellers" and are not subject to these obligations.

3. Restrictions on online negative option marketing (Section 4).

© Venable LLP 2011

The law will create specific new requirements for negative option marketing. Negative option marketing is defined as an offer or agreement to sell or provide goods or services where the customer's silence or failure to take an affirmative action to reject goods or services or to cancel the agreement is interpreted by the seller as acceptance of the offer. Before charging a consumer in an Internet-based transaction, negative option marketers must:

- clearly and conspicuously disclose all material terms;
- obtain the consumer's express informed consent to be charged; and
- where there is a recurring charge, provide the consumer with a simple mechanism to stop such charges.

Unlike prior drafts that specified the means by which consumers could cancel recurring charges, the passed law is more general and should allow for cancellation via telephone.

Enforcement (Sections 5 and 6)

The Federal Trade Commission and state Attorneys General would be authorized to enforce against violations of the Act. There is no private cause of action or rulemaking authority granted to the Federal Trade Commission.

© Venable LLP 2011

About Venable

One of American Lawyer's top 100 law firms, Venable LLP has attorneys practicing in all areas of corporate and business law, complex litigation, intellectual property and government affairs. Venable serves corporate, institutional, governmental, nonprofit and individual clients throughout the U.S. and around the world from its headquarters in Washington, D.C. and offices in California, Maryland, New York, and Virginia.

Venable's Privacy and Data Security Team serves clients from these office locations:

WASHINGTON, DC
575 SEVENTH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300

NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
TWENTY-FIFTH FLOOR
NEW YORK, NY 10020
t 212.307.5500
f 212.307.5598

TYSONS CORNER, VA
8010 TOWERS CRESCENT DRIVE
SUITE 300
VIENNA, VA 22182
t 703.760.1600
f 703.821.8949

LOS ANGELES, CA
2049 CENTURY PARK EAST
SUITE 2100
LOS ANGELES, CA 90067
t 310.229.9900
f 310.229.9901

BALTIMORE, MD
750 E. PRATT STREET
SUITE 900
BALTIMORE, MD 21202
t 410.244.7400
f 410.244.7742

The *Download* is published by the law firm of Venable LLP. Venable publications are not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations. You are receiving this communication because you are valued client or friend of Venable LLP. Questions and comments concerning information in this newsletter should be directed to Stuart Ingis at singis@Venable.com

© Venable LLP 2011