VENABLE LLP

the download

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

MAY 2009

E-COMMERCE, PRIVACY, AND MARKETING ATTORNEYS

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

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

Recognized in the 2008 United States editions of *Chambers USA* and *Legal 500* 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 M. Sugiyama
tmsugiyama@Venable.com
202.344.4363

Julia Kernochan Tama
jktama@Venable.com
202.344.4738

In this Issue:

As Congress continues to move presidential nominations and legislative priorities forward, key committees and legislators have begun proposing and debating a host of initiatives in the privacy and data security arena. Several bills from previous sessions have been reintroduced, and merit monitoring as legislators look for opportunities to pass measures ahead of the August recess. In the agencies, the Federal Communications Commission remains short two commissioners as the president's nominee for chairman, Julius Genachowski, awaits a Senate hearing. At the Federal Trade Commission, newly appointed Chairman Jon Leibowitz has taken strong positions on consumer protection issues and has selected several new managers to carry out the Commission's agenda.

This issue of the *Download* discusses recent activity in the House of Representatives related to online privacy, including hearings and new legislation. Another article reports that federal legislators and regulatory agencies are showing an active interest in mobile marketing issues. Additionally, this issue includes summaries of recent agency developments, such as the release of a Red Flag Rule compliance tool and a proposed rule on health data breach notification, as well as upcoming deadlines for public comments on Internet governance and the proposed national broadband plan.

Heard on the Hill

Developments in Online Privacy

Congress has begun considering issues that implicate online privacy. On April 23, 2009, the House Energy and Commerce Subcommittee on Communications, Technology and the Internet held a hearing to consider the impact on consumer privacy of using certain online technologies, including deep packet inspection technology, for advertising purposes. The hearing covered the privacy implications arising from advertising practices and addressed issues of transparency, informed consent, and the appropriate regulatory approach to privacy concerns. Then, on May 5, 2009, the House Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection held a hearing to consider H.R. 2221, the Data Accountability and Trust Act, and H.R. 1319, the Informed P2P User Act. This hearing focused on securing consumer data. H.R. 2221 would create a federal standard for data breach notification and would require companies that possess electronic data containing personal information to take steps to secure it. H.R. 1319 would require peer-to-peer software providers to disclose that an installed program could make a consumer's files available to others. A stated purpose of H.R. 1319 is to prevent inadvertent disclosure of information on a computer.

I. House Subcommittee Hearings

Rep. Boucher (D-VA), during the April 23rd hearing, and Rep. Rush (D-IL), during the May 5th hearing, both pledged to hold a joint subcommittee hearing on online privacy in mid-June, which they indicated will be the first in a series of hearings to consider consumer privacy issues. The June hearing will likely focus on online privacy issues.

II. Privacy Legislation

Rep. Boucher is expected to introduce privacy legislation based on a bill he previously introduced with Rep. Stearns (R-FL) during the 109th Congress. In a May 6, 2009, speech to the Computer & Communications Industry Association, Rep. Boucher indicated that the new bill is likely to cover offline as well as online data collection and transfers. Rep. Boucher also stated that the bill will require companies to allow consumers to "opt-out" of first party information uses, and to obtain a consumer's "opt-in" consent for transfers of information to third parties. The Stearns-Boucher privacy bill introduced in the 109th Congress contained, among other provisions, requirements for data collection organizations to adopt a privacy policy statement to be made available to consumers, and to deliver an initial privacy notice at the point of collecting personally identifiable information for a purpose other than the transaction at hand.

Around the Agencies

Comments Due to FCC on National Broadband Plan

On April 8, 2009, the Federal Communications Commission ("FCC" or "Commission") released a Notice of Inquiry regarding a national broadband plan.[1] Congress has directed the FCC, through the American

Recovery and Reinvestment Act, to develop a national broadband plan that will enable the build-out and utilization of high-speed broadband infrastructure.[2] The FCC must provide its plan to Congress by February 17, 2010.

To assist the FCC in the development of its national broadband plan, the Commission is seeking public comments by June 8, 2009, on a variety of issues, including: (1) effective and efficient ways to ensure broadband access for all Americans; (2) strategies for affordability and maximum utilization of broadband; (3) evaluation of broadband deployment; and (4) how to use broadband to advance a number of national purposes. Regarding privacy specifically, the Commission has indicated that it intends to evaluate the role that consumer privacy plays in the deployment and adoption of broadband services and technology. The Commission has focused on behavioral advertising and the use of deep packet inspection ("DPI") technologies to deliver advertisements relevant to consumers' web use. The FCC is considering the appropriate approach to address such privacy issues, and has asked whether it should recommend specific mechanisms or if industry self-regulation could sufficiently address privacy concerns.

In examining these privacy issues, the Commission has asked how it should approach issues such as DPI and behavioral advertising when crafting the national broadband plan. The FCC has queried whether such practices hinder consumer adoption of broadband services or discourage consumers from accessing lawful content due to a fear that the access may be tracked or revealed. To better understand how privacy issues impact broadband deployment, the Commission is seeking comments on the following broad privacy-related issues:

- What are consumers' expectations of privacy when using broadband services or technology?
- What impact do privacy concerns have on broadband adoption and use?
- Should the Commission address issues unique to the Internet, such as potential privacy and security concerns associated with cloud computing?
- Can application providers encourage use of broadband-enabled services (*e.g.*, photo sharing, online bill payment, social networking, and remote data storage) by offering privacy protection?
- What effect do data storage policies have on the use of broadband technologies?
- How do innovation and technological advancements impact consumer welfare?
- How should the Commission account for security issues in its plan?

FTC Expected to Act on New Model Privacy Notice for GLBA

According to the Federal Trade Commission's ("FTC" or "Commission") semiannual regulatory agenda, the FTC, banking agencies, and the

Securities and Exchange Commission ("SEC") (collectively hereinafter "agencies") expect to act on the long-anticipated Gramm-Leach-Bliley Act ("GLBA") model privacy form by summer 2009.[3] The privacy rule implementing GLBA requires financial services institutions to provide customers with notice of their privacy practices.

Congress, through the Financial Services Regulatory Relief of Act of 2006, directed the agencies jointly to develop a model financial privacy form as a means to provide required GLBA privacy disclosures. Specifically, Congress required that the model form: (1) be comprehensible to consumers; (2) provide clear and conspicuous disclosures; (3) allow consumers easily to identify financial institutions' sharing practices and to compare privacy practices across financial institutions; and (4) be succinct. Congress also specified that the agencies must accept public comments on their jointly-developed model form. Additionally, Congress stated that use of the model form by financial institutions would constitute a safe harbor from enforcement of the GLBA required privacy disclosures.

Since May 2007, the agencies have been reviewing public comments received on the proposed model form. In April 2009, the SEC reopened the comment period for 30 days, ending on May 20, 2009. With no legal deadline in place, the agencies are not required to meet the projected release date of this summer.

FTC Releases Red Flag Rule Compliance Tool

On May 13, 2009, the Federal Trade Commission ("FTC" or "Commission") released a tool designed to help businesses with a low risk of identity theft to comply with the Red Flags Rule.[4] Pursuant to the Fair and Accurate Credit Transactions Act of 2003, the Red Flags Rule requires many businesses to develop and implement a written Identity Theft Prevention Program to detect warning signs of identity theft and detect persons attempting fraudulently to use the identities of others to gain access to products and services. The FTC guidance explains that the Red Flags Rule provides businesses with flexibility to design programs tailored to the size of the business and the potential risk for identity theft given the nature of the business. For instance, streamlined programs may be sufficient for businesses at low risk for identity theft to comply with the Red Flags Rule.

The FTC's compliance tool contains two parts: the first part helps businesses determine whether they are at low risk for identity theft, and the second part helps businesses falling into the low-risk category to develop their required Identity Theft Prevention Program. Factors to consider when ascertaining whether a business is at low risk include the following:

- Does the business personally know its clients?
- Does the business provide services at its customers' homes?
- Has the business ever experienced an incident of identity theft?
- Is the business in an industry where identity theft is uncommon?

Once a business determines that it is at low risk for identity theft, the

compliance tool provides businesses with the following four basic steps to develop an Identity Theft Prevention Program: (1) identify relevant red flags; (2) detect red flags; (3) respond to red flags; and (4) administer the program.

FTC Issues Proposed Rule on Health Data Breach Notification

As required by the federal economic stimulus legislation, the Federal Trade Commission ("FTC") has issued a proposed rule requiring notification for security breaches of health data. The rule is directed at the growing industry of online health-related services. It will apply to vendors of personal health records; entities that advertise on the websites of such vendors or of health plans, health care providers, and health care clearinghouses; entities that access or send information to personal health records; and third party service providers. Under the proposed rule, the breach notification obligations are triggered when an entity knows, or reasonably should have known, about the breach. At that time, immediate notification is required to the FTC, and notification within 60 days and "without unreasonable delay" to individuals whose "unsecured" personal health record information is acquired without authorization. Information is considered "unsecured" unless it is encrypted or destroyed in accordance with guidance issued by the Department of Health and Human Services. Comments on the FTC proposed rule are due by June 1, 2009, and the final rule will go into effect on September 18, 2009.

NTIA Requests Comments on Expiration of Joint Project Agreement with ICANN

A presidential directive in 1997 instructed the U.S. Commerce Department to privatize the Internet's domain name and addressing system ("DNS"), with the goal of increasing competition and international involvement in its management. Accordingly, since 1998, the DNS has been managed by the private Internet Corporation for Assigned Names and Numbers ("ICANN") through a Memorandum of Understanding with the Commerce Department ("Memorandum"). This Memorandum has been amended and extended on several occasions. The Joint Project Agreement ("JPA") is the current iteration of the arrangement between U.S. government and ICANN. The JPA is set to expire on September 30, 2009.

The Commerce Department has issued a Notice of Inquiry seeking public comments by June 8, 2009, on the upcoming expiration of the JPA.[5] A 2008 review of progress concluded that further work was needed in key areas to boost institutional confidence in ICANN's ability to manage the DNS. The Commerce Department has requested a new round of comments on progress in transitioning technical activities to the private sector, as well as the appropriateness of the general model of private sector leadership and bottom-up policy development. The Commerce Department has set out several specific questions for public comment, including whether ICANN has adequately responded to issues identified in the 2008 review. Senators Snowe (R-ME) and Nelson (D-FL) have taken an interest in the matter, and wrote to Commerce Secretary Gary Locke on May 19, 2009, to urge him to become involved in finding a "permanent accountability mechanism" to replace Commerce Department oversight.

Trend Spotter

Mobile Marketing Draws Attention of Policymakers and Regulators

Interest in mobile marketing issues has lately been high in Congress and the agencies. Currently, Federal Communications Commission ("FCC") rules under the Telephone Consumer Protection Act ("TCPA") prohibit the use of automatic dialing systems to make any non-emergency call, including a text message, to a mobile telephone number without prior express authorization. Commercial email messages transmitted to wireless devices are also generally banned, with certain exceptions, under the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act.

The FCC reported in January 2009 that consumer complaints under the TCPA increased by about 65 percent from 2007 to 2008. In a letter on May 7, 2009, CTIA-The Wireless Association ("CTIA") urged the FCC to aggressively enforce restrictions on unsolicited telemarketing calls and messages to wireless devices. CTIA specifically referred to a perceived rise in consumers receiving calls regarding auto warranties and mortgage loans.

Senator Schumer (D-NY) targeted the same calls in a May 10, 2009, letter to the FTC calling for an investigation into what he described as "intrusive and unsolicited car warranty telemarketing calls." Just days later, on May 14, 2009, the FTC announced an enforcement action against two Florida-based companies for their alleged responsibility for millions of pre-recorded calls touting extended auto service contracts. The FTC filed complaints against the companies in the Northern District of Illinois, and has obtained temporary restraining orders to stop the alleged practices while the case is pending. The FTC alleges that the companies engaged in unfair and deceptive practices; violated the Telemarketing Sales Rule by calling numbers on the Do Not Call Registry; and concealed their numbers, identities, and sales purpose in calls with consumers.

Senators Snowe (R-ME) and Nelson (D-FL) have also entered the mobile marketing debate by introducing the m-SPAM Act (S. 788), with the stated goal of limiting unsolicited text message advertisements. Both senators are high-ranking members of the Senate Commerce, Science and Transportation Committee.

On April 22, 2009, the FTC released a staff report entitled "Beyond Voice: Mapping the Mobile Marketplace," which summarized the 2008 town hall meeting of the same name. Most notably, that report announced the FTC's decision to expedite its regulatory review of the Children's Online Privacy Protection Rule ("Rule"). The review will begin in 2010, and will specifically assess whether the Rule should be modified to take account of developments in the mobile arena.

---

[1] *In the Matter of a National Broadband Plan for Our Future*, GN Docket No. 09-51, Notice of Inquiry, FCC 09-31 (April 8, 2009).
[2] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).
[3] Federal Trade Commission, *Semiannual Regulatory Agenda*, p.14, May 11, 2009.
[4] Federal Trade Commission, *Complying with the Red Flags Rule: A Do-It-Yourself Prevention Program for Businesses and Organizations at Low Risk for Identity Theft*, May 2009, *available at* http://www.ftc.gov/bcp/edu/microsites/redflagsrule/RedFlags_forLowRiskBusinesses.pdf.
[5] 74 Fed. Reg. 18688 (April 24, 2009).

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 Office Locations

BALTIMORE, MD
750 E. PRATT STREET
NINTH FLOOR
BALTIMORE, MD 21202
t 410.244.7400
f 410.244.7742

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

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

ROCKVILLE, MD
ONE CHURCH STREET
FIFTH FLOOR
ROCKVILLE, MD 20850
t 301.217.5600
f 301.217.5617

TOWSON, MD
210 ALLEGHENY AVENUE
TOWSON, MD 21204
t 410.494.6200
f 410.821.0147

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

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