VENABLE LLP

the download

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

NOVEMBER 2009

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

1.888.VENABLE
www.Venable.com

In this Issue:

Heard on the Hill

Congress Considers Removing Safeguards on Federal Trade Commission Rulemaking Authority

December is expected to bring congressional action on H.R. 3126, the Consumer Financial Protection Agency Act ("CFPA Act"). The House Financial Services Committee and the House Energy and Commerce Committee completed markup sessions for the legislation in October 2009. In the Senate, on November 10, 2009, Senate Banking, Housing, & Urban Affairs Committee Chairman Christopher Dodd (D-CT) introduced a discussion draft of the Restoring American Financial Stability Act, of which Title X of the bill constitutes the CFPA Act. These bills would reform the structure of the regulatory regime governing the consumer financial marketplace.

Unlike the House version of the CFPA Act, Chairman Dodd's bill does not include provisions, discussed below, that would broadly expand the authority of the Federal Trade Commission ("FTC"). The Senate Commerce, Science, & Transportation Committee ("Senate Commerce Committee"), which has jurisdiction over the FTC, is expected to take up these issues through separate FTC reauthorization legislation. Senator Byron Dorgan's (D-ND) FTC Reauthorization Act of 2008 may be the basis for such proposed legislation. The bill is expected to address FTC rulemaking authority, independent litigation authority, civil penalty authority, and aiding and abetting liability.

The current House version of the CFPA Act would have a significant effect on FTC rulemaking procedures. Under existing law, the FTC generally uses the rulemaking steps in the Administrative Procedure Act ("APA") when carrying out a specific congressional grant of authority, such as exists under the CAN-SPAM Act of Children's Online Privacy Protection Act. In contrast, outside of specific statutory authority, when issuing rules under its "unfair or deceptive" authority, the FTC must use enhanced procedures that provide additional public participation rights and other safeguards against agency overreaching. The CFPA Act would eliminate these safeguards.

The enhanced FTC rulemaking procedures have been in place for decades. During the 1970s, the FTC launched several controversial rulemaking efforts to declare certain businesses practices unfair or deceptive. For example, the FTC undertook a rulemaking on children's advertising that led the Washington Post's editors to brand the agency "a great national nanny."[1]

Congress, acting under Democratic leadership, enacted legislation in 1975 and 1980 to impose procedural safeguards to ensure meaningful public participation in such FTC rulemaking efforts. In its report on the 1975 legislation, the House Energy and Commerce Committee explained that "[b]ecause of the potentially pervasive and deep effect of rules defining what constitutes unfair or deceptive acts or practices and the broad standards which are set by the words 'unfair or deceptive acts or practices' … greater procedural safeguards are necessary."[2]

The CFPA Act would also expand the FTC's enforcement powers. The legislation would enable the FTC to seek civil penalties of up to $16,000 per violation for unfair or deceptive acts or practices and would provide the Commission with independent civil litigation authority.

House Energy and Commerce Committee Holds a Joint Subcommittee Hearing on Privacy

On November 19, 2009, the House Energy and Commerce Subcommittee on Communications, Technology, and the Internet, along with the Subcommittee on Commerce, Trade, and Consumer Protection, held a joint hearing on the offline and online collection and commercial use of consumer information. This hearing constituted one of several that the two Subcommittees have held throughout this year in preparation for introducing privacy legislation. While no details of such legislation were disclosed at the hearing, both Subcommittee Chairman Boucher (D-VA) and Subcommittee Chairman Rush (D-IL) expressed their intention to introduce a privacy bill soon.

Debate among the various Subcommittee Members in attendance centered on how best to protect the data of consumers without stifling commerce and negatively impacting small businesses. A number of the members focused on sensitive data and asked witnesses whether businesses may sell such information and what protections are in place to ensure that such information is not misused. Chairman Boucher focused his inquiry on exploring how best to alleviate the concerns of consumers who may resist the collection of their information. Chairman Rush stated that he would introduce legislation that would achieve a balance between consumer privacy and business interests.

The Subcommittees heard testimony from representatives of the academic, business, and consumer communities. Witnesses generally agreed that the collection of personal information from consumers enables businesses to provide them with products and services of value (*e.g.*, free email). Witnesses explained that providing privacy protections to consumers' information makes sense for businesses because they want consumers to trust them. One business representative stated that small businesses rely on access to consumer information in order to grow. A consumer representative recommended that rules should govern consumer data collection because such information has now become a permanent record of consumers that can be used in ways that negatively impact the consumer. The academic representative focused on the lack of notice and consent required by U.S. privacy laws to sell consumer information collected offline.

Senate Commerce Committee Considers Post-Transaction Marketing Practices

On November 17, 2009, Chairman Jay Rockefeller (D-WV) convened the Senate Committee on Commerce, Science and Transportation ("Senate Commerce Committee") to hold a hearing to examine the impact that "post-transaction marketing" and related "data pass" practices have on consumers. The hearing coincided with the release of a Committee staff report, which addresses the Committee's on-going investigation into certain online sales tactics. Chairman Rockefeller suggested that the Committee consider "legislative steps" to address these practices; however, the Chairman did not offer any specific proposals. Senator Dorgan (D-ND) said he considers such practices to be a fraud and suggested that companies conducting business online that have partnered with post-transaction marketers should be held liable for enabling these marketers to engage in such practices.

The hearing focused on "post-transaction marketing," which is commonly known by industry as "pre-acquired account information" tied to free trial offers. These practices typically involve an online merchant providing a third party access to

the merchant's customer account information. Consumers provide account information (*i.e.* credit card number) when they engage in a transaction with the online merchant. Prior to "check-out," or shortly thereafter, the consumer is offered another product or service through an upsell (*i.e.* membership in a club, a rewards program, insurance, etc.) furnished by a third party. If the consumer "consents" to the terms of the offer, the third party charges the consumer's credit card account. Generally, consumers are not required to reenter their credit card numbers or provide any additional billing information. The third party obtains this information directly from the online merchant and subsequently charges the consumer's financial account monthly. The report and the hearing indicate that consumers are not aware at the time of accepting the additional offer that their credit card or financial account information is passed through to third parties to be used for subsequent billing. According to the staff report, consumers are surprised to be charged once the free trial has ended, without further communication with the seller of the second product or service.

While the investigation is still ongoing, the staff of the Senate Commerce Committee issued a report with the following findings—

- Aggressive sales tactics to sell membership clubs to consumers who do not want them is a billion-dollar business;
- Well-known websites and online retailers use aggressive sales tactics and earn millions of dollars doing so;
- The companies under investigation knowingly charged consumers for services that the consumers were unaware they had purchased;
- The customer service centers of the companies under investigation primarily handle calls from consumers who are upset, confused, and/or would like to cancel their memberships; and
- Those companies conducting business online that have partnered with the companies under investigation know that customers are harmed by such aggressive sales tactics.

The Senate Commerce Committee intends to continue its investigation into these practices and may also introduce legislation to address these activities.

Around the Agencies

Federal Trade Commission to Hold December Roundtable Discussion on Privacy

The Federal Trade Commission ("Commission") has announced that it will hold three privacy roundtable discussions to address developing challenges to consumer privacy created by new technology and business practices. The Commission has stated that the series of roundtables will explore the impact of a range of practices, including topics such as online behavioral advertising, social networking, cloud computing, and mobile marketing. The first privacy roundtable is scheduled to occur in Washington, DC on December 7, 2009 and the second roundtable will take place in Berkeley, CA on January 28, 2010. The location and date of the third roundtable have yet to be announced.

For the first privacy roundtable in December, the Commission is expected to convene panels on the following topics: (1) benefits and risks of collecting, using, and retaining consumer data; (2) consumer expectations and disclosures; (3)

online behavioral advertising; (4) information brokers; and (5) exploring existing regulatory frameworks.

Stakeholders with an interest in serving on the second roundtable panel have until December 9, 2009 to make a request to participate. Additionally, parties may submit comments to the Commission by December 21, 2009, addressing such topics as: (1) the role that privacy-enhancing technologies play in addressing Internet-related privacy concerns; and (2) challenges to consumer privacy created by innovations in the digital environment and means to address those challenges without stifling innovation.

Federal Communications Commission Proposes Rules to Preserve an "Open Internet"

The Federal Communications Commission ("FCC" or "Commission") is seeking to codify four Internet policy principles issued four years ago through the Commission's Internet Policy Statement.[3] These principles are meant to provide guidance as to how the Commission interprets its authority under the Communications Act to enforce the federal policies of "promot[ing] the continued development of the Internet"[4] and of "encourag[ing] the development of technologies [that] maximize user control over what information is received by individuals…who use the Internet."[5] In its Notice of Proposed Rulemaking, the Commission stated that it is proposing new rules to preserve the openness of the Internet.[6]

In addition to the principles contained in its prior Internet Policy Statement, the Commission has proposed two additional principles. In total, the Commission proposes to require providers of broadband Internet access service to comply with the following six rules:

1. Subject to reasonable network management, a provider of broadband Internet access service may not prevent any of its users from sending or receiving the lawful content of the user's choice over the Internet.

2. Subject to reasonable network management, a provider of broadband Internet access service may not prevent any of its users from running the lawful applications or using the lawful services of the user's choice.

3. Subject to reasonable network management, a provider of broadband Internet access service may not prevent any of its users from connecting to and using on its network the user's choice of lawful devices that do not harm the network.

4. Subject to reasonable network management, a provider of broadband Internet access service may not deprive any of its users of the user's entitlement to competition among network providers, application providers, service providers, and content providers.

5. Subject to reasonable network management, a provider of broadband Internet access service must treat lawful content, applications, and services in a nondiscriminatory manner.

6. Subject to reasonable network management, a provider of broadband Internet access service must disclose such information concerning network management and other practices as is reasonably required for users and content, application, and service providers to enjoy the protections specified in this part.[7]

These principles would be subject to reasonable network management practices, which the Commission has proposed to include:

(1) reasonable practices employed by a provider of broadband Internet access service to:

(a) reduce or mitigate the effects of congestion on its network or to address quality-of-service concerns;

(b) address traffic that is unwanted by users or harmful;

(c) prevent the transfer of unlawful content; or

(d) prevent the unlawful transfer of content; and

(2) other reasonable network management practices.[8]

The Commission is seeking comments on these principles by January 14, 2010. Subsequently, reply comments will be due by March 5, 2010.

Food and Drug Administration Holds Hearing on Online Medical Products Advertising

On November 12-13, 2009, the U.S. Food and Drug Administration ("FDA") held a public hearing titled "Promotion of FDA-Regulated Medical Products Using the Internet and Social Media Tools." The hearing focused on the use of online communication channels to promote FDA-regulated products to consumers and to examine the practices used by industry to provide required disclosures concerning these products. The hearing was the FDA's first event to focus on this topic since 1996.

The FDA has issued guidelines for marketing in offline media, but has not yet set standards specific to online marketing. In March 2009, the FDA sent letters to several pharmaceutical companies telling them to include more risk and side effects information in the text of online advertisements. Amidst uncertainty about the FDA's expectations, many such companies have now cut back on advertising. Among other topics, hearing participants discussed how disclosures should be provided, the extent to which companies should be held responsible for consumer-created content about their products, and how companies should monitor adverse events.

Transcripts of the hearing will be available in mid-December 2009. The public comment docket for the hearing will remain open until February 28, 2010.

Federal Trade Commission COPPA Enforcement Action

Iconix Brand Group, Inc. ("Iconix") has entered into a settlement agreement with the Federal Trade Commission ("FTC" or the "Commission") over charges that the company violated the Children's Online Privacy Protection Act ("COPPA"), the Children's Online Privacy Protection Rule (the "Rule"), and the Federal Trade Commission Act. The complaint alleges that Iconix, *inter alia*, violated COPPA by failing to provide notice and obtain verifiable parental consent before collecting, using, and/or disclosing information collected from children online. As part of the settlement agreement, Iconix has agreed to pay a $250,000 civil penalty to the Commission.

Iconix operates a number of apparel websites popular with children. The FTC complaint explains that children were permitted to register for online activities, participate in sweepstakes contests, enroll to receive electronic updates, and share personal stories online. The complaint alleges that Iconix, as the website operator, stated in its privacy policy that the company would delete any personally identifiable information obtained from children, but in practice took no steps to do so. The complaint asserts that Iconix publically posted children's images and personal information. Additionally, the complaint states that Iconix's privacy policy failed to clearly disclose the company's information collection, use, and disclosure practices with respect to children, and did not list all of the operators that collected or maintained the children's personal information. The complaint further asserts that Iconix failed to provide parents with direct notice of its children's information practices and did not take the requisite steps to obtain verifiable consent from the parents.

Pursuant to the consent order, in addition to paying the $250,000 civil penalty, Iconix has agreed to provide the requisite notice, both on its websites or other online services, and to parents before collecting, using, and/or disclosing children's personal information. The company has also agreed to obtain verifiable parental consent. For five years, Iconix will be required to include a prescribed notice of tips from the Commission on how to protect children's privacy online in three locations: (1) in the company's privacy policy online; (2) in the direct notice provided to parents; and (3) at each location on its website where personal information is collected. Iconix has further agreed to delete any children's personal information it previously collected and maintained.

This enforcement action against Iconix serves as a reminder to operators of commercial websites or online services directed to children under 13, and operators of commercial general audience websites that have actual knowledge that specific visitors are children, that they may wish to:

- Review their online privacy policies to ensure that their children's information practices are clearly disclosed;
- Conduct an internal review to ensure that statements made in their privacy policies comport with actual practices;
- Ensure parents receive the requisite notice of the companies' children's online practices; and
- Ensure that children's information is not collected, used, or disclosed without such consent.

Federal Trade Commission Delays Enforcement of Red Flags Rule

The Federal Trade Commission ("FTC" or "Commission") has delayed enforcement of its Red Flags Rule from November 1, 2009 until June 10, 2010. Since the Red Flags Rule became effective in January 2008, there has been confusion and uncertainty within industries under the FTC's jurisdiction about what businesses are covered by this rule.

The Red Flags Rule requires creditors and financial institutions to develop and implement programs designed to identify, detect, and respond to possible risks of identity theft. The FTC promulgated its rule pursuant to the Fair and Accurate Credit Transactions Act, which amended the Fair Credit Reporting Act. Financial institutions and creditors were originally given until November 1, 2008 to comply with the Rule, but the FTC has now extended the compliance deadline multiple times.

Several associations representing separate industries, including the American Bar Association ("ABA") and the American Medical Association, have taken the position that the Red Flags Rule does not cover their respective industries. The ABA filed a suit in federal court claiming the FTC exceeded its authority in applying its rules to attorneys. On October 30, 2009, the U.S. District Court for the District of Columbia ruled in favor of the ABA, granting summary judgment on the claim that the FTC's application of the Red Flags Rule to attorneys exceeds the Commission's statutory jurisdiction and authority.

Congress has taken legislative steps to address the Commission's broad application of its rules. In October 2009, Rep. John Adler (D-NJ) introduced H.R. 3763 to provide for an exclusion from the Red Flags Rule for certain businesses. The bill, passed by the House by a vote of 400-0, would exclude small businesses (with 20 or fewer employees), such as health care practices, accounting practices, and legal practices. The bill would also permit the Commission to exclude specific companies upon application provided the company knows all of its customers or clients individually; only performs services in or around the residences of its customers; or has not experienced incidents of identity theft and identity theft is rare for businesses of that type. The Senate has not yet taken action on H.R. 3763.

Federal Reserve Board Releases Proposed Gift Card Regulations

On November 16, 2009, the Federal Reserve Board ("Board") released proposed regulations to implement the gift card provisions of the Credit Card Accountability Responsibility and Disclosure Act ("Credit CARD Act" or "Act"), which became law on May 22, 2009. The proposal was published in the Federal Register on November 20, 2009, and interested parties may submit comments by December 21, 2009.[9] Based on the timeframe outlined in the Act, the rules are set to become effective on August 22, 2010.

The proposed rule would apply to gift certificates, store gift cards, and general-use prepaid cards (collectively "cards"). Such cards by definition would exclude those that are: "(1) useable solely for telephone services; (2) reloadable and not marketed or labeled as a gift card or gift certificate; (3) a loyalty, award, or promotional gift card; (4) not marketed to the general public; (5) issued in paper form only; or (6) redeemable solely for admission to events or venues at a particular location or group of affiliated locations, or to obtain goods or services, in conjunction with admission to such events or venues, at the event or venue or at specific locations affiliated with and in geographic proximity to the event or venue."[10]

The Board's proposal would amend Regulation E, which implements the Electronic Fund Transfer Act, by restricting dormancy, inactivity, and service fees on gift certificates, store gift cards, and general-use prepaid cards. Specifically, the proposed rule would prohibit such fees unless: (1) there has been no activity on the card for at least a year; (2) only one such fee is imposed during the month; and (3) disclosures of the fees are clear and conspicuous on the card or such disclosures are provided before a purchaser buys the card.

The Board has also proposed prohibiting the sale of gift cards that may expire the funds on the card less than five years after the date of issuance or the date of when funds were last loaded. Notice of such expiration would be required to be clearly and conspicuously disclosed on the card and before a purchaser buys the card. Additionally, the proposed rule would require a disclosure informing purchasers whether there is a difference between the expiration date of the card and the expiration date of the underlying funds.

International

European Union Adopts New Measure on Use of Cookies and Data Breach Notice

On October 26, 2009, the European Council approved a Directive amending its 2002 Directive on Privacy and Electronic Communications concerning the processing of personal data and the protection of privacy in the electronic communications sector ("the "e-Privacy Directive"). The new Directive will enter into force a day after its publication in the Official Journal of the European Union. Member States will have 18 months thereafter to pass laws implementing the amended Directive. The amendment's effect is summarized below.

On its face, the amended e-Privacy Directive will require "data controllers" to provide clear and comprehensive information about a cookie's purpose and to obtain "consent" before using the cookie. This provision has created considerable concern and confusion. "Consent" need not be obtained if the cookie is used for the sole purpose of transmitting a communication, or is strictly necessary to provide a service explicitly requested by the user. The Preamble to the original e-Privacy Directive, which was not amended, stated that consent is "freely given specific and informed indication of the user's wishes" such as checking an online box.[11]

The new Directive also includes the European Union's first data breach notice requirement, which will apply narrowly to telecommunications companies and Internet service providers that operate on public networks, but not other data controllers. Notification to national authorities must be delivered "without undue delay," as well as notification to individuals if an adverse effect on the individual's data or privacy is likely. However, there is an exception to the notification requirement if the provider has implemented technical protections to make the data unintelligible.

Federal Trade Commission Settles Charges Based on Allegedly False Claims of U.S./EU Safe Harbor Compliance

The Federal Trade Commission ("FTC") announced in October that it proposed to settle complaints against six U.S. companies for unfair or deceptive acts or practices related to privacy policy statements. These coordinated cases serve as a reminder to ensure that privacy policies accurately reflect company practices, including compliance program participation and status.

The FTC alleged that the six companies had falsely claimed that they complied with the Safe Harbor framework for data transfers from the European Union. The Safe Harbor framework requires companies to self-certify their compliance with certain standards, and to inform the Commerce Department if a representation of compliance is no longer valid. The FTC alleged that the six companies' privacy policies continued to state that the companies were in compliance with the Safe Harbor framework during time periods when their compliance status was not current because they had not submitted self-certification statements to the Commerce Department.

Under the proposed settlement agreements, the companies would be prohibited from misrepresenting the extent of their participation in any privacy, security, or other compliance programs sponsored by the government or a third party. The companies would also be required to keep for five years all documents related to

compliance with the order, including all advertisements, promotional materials, and other statements, along with supporting materials, as well as any documents that call the companies' compliance into question. The administrative orders would remain in place for 20 years.

2009 U.S./EU Safe Harbor Conference

From November 16-18, 2009, the U.S. Department of Commerce hosted a conference in Washington, DC in cooperation with the European Commission Article 29 Working Party on Data Protection to address cross border data flows, protection, and privacy. This tradition of working together on data protection issues originates from the bilateral commitment made in 2000 by the United States and the European Union on the transfer of personal data between the two parties. At that time, the European Commission determined that personal data could be transmitted from the European Union to U.S. organizations only if those entities self-certified to compliance with the Safe Harbor.

The conference marked the second annual meeting between the two parties designed to advance cooperation across the Atlantic on data protection issues. The conference began with a keynote address by David Vlaceck, Director of the FTC's Bureau of Consumer Protection, who stated that notice and choice may no longer serve as an adequate means of obtaining consent. Deputy Secretary of Commerce Dennis Hightower noted that self-regulation, sector-specific laws, and the Safe Harbor Program provide sufficient protections for consumer personal data. Representing the European perspective, the Vice-Chair of the Article 29 Working Party on Data Protection, Jacob Kohnstamm, called for an international data protection framework.

Panels over the course of the conference covered a range of topics, including: (1) how to successfully navigate the U.S./E.U. Safe Harbor; (2) an overview of the European Union framework; (3) accountability, privacy, and data transfers; (4) information security and privacy; (5) behavioral advertising; (6) global data protection issues arising during pandemics; (7) social networks; (8) electronic discovery in civil litigation and cross-border data flows; and (9) the U.S.-Swiss Safe Harbor.

About Privacy, Advertising and Marketing, and Data Protection Practice

Venable's Advertising, Marketing and Data Protection lawyers, pioneers in the emerging area of information law and policy, provide an integrated approach to legal and business solutions in areas such as electronic commerce, Internet advertising and marketing, financial services, homeland security and government surveillance, telemarketing, and medical privacy. Our attorneys are well-versed on the evolving U.S., Canadian, European, and Asian regulations and policies governing our clients' businesses. In addition, they are involved in developing and drafting the major statutes and regulations in the field. Our clients hail from a variety of industries and are supported by Venable's nationally renowned practices in Legislative and Government Affairs, Advertising, IP, Financial Services, and Communications. Venable was recognized in the 2008 United States edition of Legal 500 and won the 2009 Chambers USA Award for Excellence for its outstanding data protection and privacy practice.

Venable's Privacy & Data Security Practice Wins 2009 Chambers USA Award for Excellence

On June 11, 2009, Venable's Privacy and Data Security Practice won the 2009 Chambers USA Award for Excellence for making the largest impact in the practice of privacy law over the previous year. Chambers selected Venable as the recipient of this award from more than 20 leading privacy and data security practices. Chambers is renowned globally for its annual rankings of leading lawyers and practice groups, and is among the most-used legal guides by in-house counsel.

Venable Serves as Counsel to Cross-Industry Effort to Develop Self-Regulatory Principles for Online Behavioral Advertising

Venable attorneys facilitated a major collaborative effort among leading advertising and marketing trade associations representing the entire marketing media ecosystem to develop self-regulatory principles for online behavioral advertising. These principles were designed to enhance consumers' trust and confidence in how online information is gathered and used to deliver interest based advertising.

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

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

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
NINTH FLOOR
BALTIMORE, MD 21202
t 410.244.7400
f 410.244.7742

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

---

[1] *The FTC as National Nanny*, Washington Post, March 1, 1978, at A22.
[2] H.R. Rep. No. 93-1107 (1974), *reprinted in* 1974 U.S.C.C.A.N. 7702, 7727.
[3] FCC Policy Statement, 20 FCC Rcd 14986 (2005).
[4] 47 U.S.C. §230(b)(1).
[5] 47 U.S.C. §230(b)(3).
[6] In the Matter of Preserving the Open Internet Broadband Industry Practices, GN Docket No. 09-191, FCC 09-93 (October 22, 2009).
[7] *Id.*
[8] *Id.*
[9] Board of Governors of the Federal Reserve System, Electronic Fund Transfers; Proposed Rule, 74 Fed. Reg. 60,986, 60,986 (Nov. 20, 2009).
[10] 74 Fed. Reg. at 61,006.
[11] European Parliament, "Directive 2002/58/EC on Privacy and Electronic Communications" at ¶ 17 (July 12, 2002).