VENABLE LLP

# the download

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

AUGUST 2010



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

### Financial Regulatory Reform Legislation Enacted

Congress enacted landmark financial regulatory reform legislation in July, but the final measure did not include provisions passed by the House that would have expanded the rulemaking and enforcement authorities of the Federal Trade Commission ("FTC").

Among other significant measures, the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act") establishes a Consumer Financial Protection Bureau ("CFPB") that will oversee consumer protection in the financial marketplace, exercising new regulatory duties as well as taking over authorities previously divided among several

agencies. The CFPB has broad jurisdiction over "consumer financial products and services" and certain activities in connection with such products and services. This jurisdiction is expected to reach many companies not traditionally considered "financial" businesses. The CFPB's powers include the authority to identify certain acts or practices as unlawfully "unfair, deceptive, or abusive." Although this mandate is similar to the FTC's unfair and deceptive acts or practices authority, the enforcement of the new "abusive" element is relatively unknown territory.

Not included in the Dodd-Frank Act are new authorities that have been sought by the FTC:

- Civil penalty authority,
- Streamlined Administrative Procedure Act rulemaking in place of Magnuson-Moss rulemaking procedures,
- Authority to pursue aiders and abettors of FTC Act violations, and
- Independent litigating authority.

While the House version of the financial reform legislation provided for such expansions of FTC authority, the Senate version did not. The Senate may consider whether to expand FTC authorities when it takes up FTC reauthorization legislation in the near future.

To read more about the CFPB, please visit http://www.venable.com/cfpb-task-force/.

## Congress Considers Consumer Privacy

With the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act on July 21, 2010, Congress has moved its attention to matters related to privacy, data security, and cybersecurity. In the weeks leading into the August recess, both the House Energy and Commerce Committee and the Senate Committee on Commerce, Trade and Transportation held hearings on privacy. A recent House hearing coincided with the introduction of new legislation. While it is not clear whether either Committee will be able to approve legislation before the end of this session, it is apparent that the stage is being set to address these issues in the 112th Congress.

**House Consideration of Privacy**

Congressional interest in issues of privacy started to rise in May 2010. On May 4, 2010, Rep. Boucher (D-VA) released a discussion draft of a privacy bill for public comment. This draft bill, which has yet to be formally introduced in Congress, would have major implications for many longstanding and important business practices. For instance, the bill would broadly restrict the collection and transfer of consumer data online as well as offline, and would establish notice and opt-out consent requirements for first party data collection and use. The bill would also effectively require opt-in consent for the transfer of personal data to third parties except in limited circumstances. Neither of these standards are the current practice in industry. In response to the release of this discussion draft, over 60 comments from various trade associations, companies, and consumer advocate groups were submitted to Rep. Boucher raising concerns with the draft legislative proposal.

On July 19, 2010, Rep. Rush (D-IL) introduced H.R. 5777, the BEST

PRACTICES Act. This bill builds on the discussion draft released by Rep. Boucher but includes several significant differences. Like Rep. Boucher's bill, H.R. 5777 would impose restrictions on the collection and transfer of consumer data online as well as offline, and establish a similar consent framework with respect to first party and third party data practices. However, Rep. Rush's bill takes a different approach in providing a safe harbor under which entities that comply with approved self-regulatory programs are not subject to certain requirements. In particular, such companies would be permitted to transfer data to third parties subject to an opt-out. Another significant aspect of this bill that is different from Rep. Boucher's draft is the inclusion of accuracy, access, and dispute resolution provisions.

The House Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection held a hearing on July 22, 2010, to consider H.R. 5777 and general consumer privacy issues. The Subcommittee, which is chaired by Rep. Rush, mainly focused on the bill's provisions that would create a safe harbor and enforcement mechanism, in particular the bill's private right of action and enforcement by the state attorneys general. Rep. Rush stated he intends to move the bill quickly to the full committee for consideration.

At this hearing, David Vladeck, the Director of the Bureau of Consumer Protection at the Federal Trade Commission, offered a few suggestions for the Subcommittee to consider as part of its legislative process:

- He recommended requiring companies to provide a short disclosure at the point of collection or use.
- He further recommended simplifying consumer choice mechanisms.
- He stated that sharing of individuals' data among companies affiliated through common ownership should not necessarily be exempt from consent requirements. He explained that consumers do not understand relationships between companies based on corporate control and may not appreciate the distinction between an affiliate and a third party.

On July 28, 2010, the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security held a hearing on online privacy, social networking, and crime victimization. The Subcommittee heard testimony from federal law enforcement agencies describing the rising incidence and complexity of online crimes relating to personal information shared online, as well as law enforcement strategies to counter these criminal acts. Additionally, industry and public interest groups discussed the protection of personal information online, particularly on social networks, as well as the tools available to consumers to maintain the privacy of their data.

**Senate Commerce Holds Hearings on Consumer Online Privacy**

The Senate Committee on Commerce, Science, and Transportation held a hearing on consumer privacy on July 27, 2010. The Committee broadly explored online advertising, discussed whether consumers may be harmed by aggregating consumer data for marketing purposes, and considered the adequacy of current practices related to transparency and choice. During the hearing, Sen. Kerry (D-MA) commented that he intends to work with Sen. Pryor (D-AR) to build a record on which to develop common standards for protecting consumers online. Sen. Pryor has already chaired

two hearings on children's privacy and safety in the Subcommittee on Consumer Protection, Product Safety, and Insurance.

Chairman Leibowitz of the Federal Trade Commission ("FTC") testified at the hearing. He discussed the FTC's 2009 Staff Report on guidelines for self-regulatory principles for online behavioral advertising as well as the FTC's series of roundtable discussions on privacy. He said the FTC plans to release a report later this year making recommendations on:

- Incorporating privacy into business practices,
- Simplifying consumer choice,
- Improving transparency,
- Providing access and correction rights to data maintained by data brokers, and
- Requiring affirmative express consent for material retroactive changes to how data will be used.

Chairman Leibowitz commented that the FTC is considering various approaches to providing consumers with clear notice and choice including a mechanism for a universally recognized opt-out. Regarding transparency, Chairman Leibowitz said the FTC is considering ways to improve disclosures made through privacy policies and commented that companies could use a standardized format or terms. He also suggested that companies could provide a disclosure box, in addition to a privacy policy, in which companies could disclose material terms and provide a choice mechanism

## Around the Agencies

### Federal Trade Commission and Congress Consider Children's Online Privacy

Children's online privacy has once again risen to the top of the agenda for the Federal Trade Commission ("FTC" or "Commission") and the Senate Committee on Commerce, Science, and Transportation's Subcommittee on Consumer Protection, Product Safety, and Insurance ("Senate Commerce Subcommittee"). In March of this year, the Commission announced that it was expediting its review of the Children's Online Privacy Protection Rule ("COPPA Rule" or "Rule") in light of technological changes that have taken place since the Rule was originally promulgated a decade ago. Rather than formally proposing specific changes to the current COPPA Rule, the Commission solicited feedback from the public on virtually all aspects of the Rule to help it determine how well the regulation is positioned to address technological advancements in media, such as mobile, interactive television, interactive gaming, and other interactive media. Following a brief extension, the Commission accepted comments through July 12, 2010. As part of the Commission's review of the COPPA Rule, the FTC also convened a workshop on June 2, 2010. Both in its request for comments and at the COPPA Rule workshop, the Commission asked for feedback on whether any proposed recommendations would require changes to the Children's Online Privacy Protection Act ("COPPA").

Congress has not yet proposed modifications to COPPA. The Senate Commerce Subcommittee, however, has convened hearings on children's online privacy. Most recently, on July 15, 2010, Subcommittee Chairman Pryor (D-AR) held a hearing on protecting youth online. This hearing marked the Subcommittee's second in a series on this topic this year. Whereas April's hearing focused primarily on privacy matters, this hearing

concentrated on safety issues that may arise as children navigate the online world. The Subcommittee members espoused the many offerings that the Internet provides to children, but also cautioned that such technology can put children at risk of cyber-bullying and online harassment. At the hearing, witnesses from the Commission, industry, and advocates agreed that providing protections to youth online is a priority but did not reach consensus on the best means to implement such protections.

## Twitter Settles with Federal Trade Commission in Agency's First Case Against a Social Networking Service

In June, the Federal Trade Commission ("FTC") settled its first case brought against a social networking service under Section 5 of the FTC Act. In its complaint, the FTC claimed that Twitter misled users through certain statements on its website privacy policy. The FTC further alleged that Twitter failed to take reasonable steps to prevent unauthorized administrative control of its system, with the result that hackers gained administrative control of the service twice in the first half of 2009. Hackers reportedly used this control to reset passwords and send phony "tweets" from existing accounts, and may have accessed nonpublic user information. The agreement is for settlement purposes and does not constitute an admission of legal violations by Twitter.

Among other specific concerns, the FTC claimed that Twitter did not take steps to preserve the security of administrative passwords by:

- Requiring the use of hard-to-guess administrative passwords;
- Prohibiting employees from storing administrative passwords in plain text in personal email accounts;
- Suspending or disabling administrative passwords after unsuccessful login attempts;
- Providing a non-public administrative login page;
- Enforcing periodic updates of administrative passwords; and
- Restricting employee access to administrative controls.

The case places companies on notice that the FTC may expect companies to include such elements in their security practices.

Similar to prior data security cases, the consent agreement will be in effect for 20 years. Among other provisions, it requires Twitter to establish a comprehensive information security program that includes a designated accountable employee, assessment of foreseeable material risks, design and implementation of reasonable safeguards, regular testing and monitoring, reasonable steps regarding service providers, and ongoing evaluation and adjustment of the program. Twitter must also obtain biennial independent security assessments of its security program for the next 10 years.

## Office of Management and Budget Changes Guidance on Cookie Use by Government Agencies

For the past ten years, the federal government, through the Office of Management and Budget's ("OMB") June 22, 2000 Memorandum on *Privacy Policies and Data Collection on Federal Web Sites*, effectively prohibited federal government sites from using cookies to collect data from visitors.

That guidance provided that "the presumption should be that 'cookies' will not be used at Federal web sites."[1]

On June 25, 2010, the OMB retracted its prior position when it released a new *Guidance for Online Use of Web Measurement and Customization Technologies*.[2] The new guidance provides that agencies may use cookies to improve federal services online. Federal agencies may not, however, use cookies:

- to track individuals on the Internet outside the website or application from where the technology originates;
- to share data with outside agencies without a user's explicit consent;
- to cross-reference any data collected against personally identifiable information ("PII") without a user's explicit consent in order to determine individual-level online activity;
- to collect PII without a user's explicit consent; or
- for any similar usage determined by the OMB.

The OMB's guidance also imposes notice, choice, data safeguarding and privacy, data retention and access, enforcement, and verification obligations on federal agencies that use cookies. The Administration's revised policy now permits the government to offer many personalized offerings to site visitors in a manner already underway in the private sector.

## Department of Health and Human Services Issues Proposed Rules on Health Privacy

On July 8, 2010, the Department of Health and Human Services ("HHS") issued new proposals on health privacy to implement the Health Information Technology for Economic and Clinical Health ("HITECH") Act, enacted as part of federal stimulus legislation in February 2009. The proposed rules would amend the existing Privacy Rule, Security Rule, and Enforcement Rule under the Health Insurance Portability and Accountability ("HIPAA") Act.

As mandated by the HITECH Act, the proposals would require business associates of HIPAA-covered entities to comply with most requirements of the Privacy and Security Rules. Notably, HHS further proposes applying the new privacy and security requirements to subcontractors of business associates. The rules would also implement HITECH Act provisions regarding:

- New individual rights to access their protected health information and to restrict certain disclosures,
- Tighter limits on the use and disclosure of protected health information for marketing and fundraising, and
- Restrictions on the sale of protected health information without patient authorization.

Comments may be submitted until September 13, 2010. HHS has stated that entities will have 180 days after publication of the final rule to come into compliance with the new requirements.

In conjunction with issuing the proposed rules, HHS also updated its website where notices of large data breaches are published and launched

a new webpage designed to help visitors easily access information about HHS privacy efforts.

On July 13, 2010, HHS also announced final rules that (1) define "meaningful use" of electronic health record ("EHR") technology for the purpose of receiving federal incentive payments, and (2) identify the criteria for certifying EHR technology.

### Federal Agencies Submit an Intellectual Property Enforcement Report to the President and Congress

In June 2010, several federal agencies submitted a joint report entitled, "Joint Strategic Plan on Intellectual Property Enforcement" to the President and Congress. This report was prepared by the U.S. Departments of Agriculture, Commerce, Health and Human Services, Homeland Security, Justice, and State; the Office of the U.S. Trade Representative; and the U.S. Copyright Office. These federal agencies were directed pursuant to the Prioritizing Resources and Organization for Intellectual Property Act ("PRO-IP Act") to coordinate the development of a Joint Strategic Plan to address counterfeiting and infringement. Through this report, the agencies detailed their efforts toward this goal and made recommendations for several actions for the federal government to take to enhance U.S. intellectual property rights. The recommendations include:

***Lead by example***. The federal government should not purchase or use products that infringe on intellectual property rights.

***Support transparency***. The federal government should be transparent in the development of enforcement policy, information sharing, and reporting of law enforcement activities at home and abroad.

***Improve coordination***. The federal government should coordinate law enforcement efforts at the federal, state and local level, and internationally.

***Work with trade partners***. The federal government should work with trading partners and with international organizations to improve enforcement of American intellectual property rights internationally.

***Secure supply chains***. To curtail the stream of infringing products across U.S. borders, the federal government should improve its cooperation with the private sector.

***Monitor intellectual property-related activity***. The federal government should monitor intellectual property-related activity to assess domestic and foreign laws and enforcement activities.

## International

### Article 29 Data Protection Working Party Opinion on Online Behavioral Advertising

The European Union's ("EU") Article 29 Data Protection Working Party on June 22, 2010 adopted an opinion (the "Opinion") to clarify how EU law applies to online behavioral advertising ("OBA").[3] As a result of recent

changes to EU law that were approved by the European Council at the end of 2009 and are set to be implemented by May 2011, some confusion had arisen as to whether OBA providers that use cookies were bound by the new law. The Opinion addresses the extent to which EU law applies to OBA and underscores that OBA providers who use cookies are indeed covered by the revised law. Specifically, the Opinion states that ad networks must obtain prior informed consent before placing or retrieving information from a cookie used for OBA. The Opinion notes, however, that such consent is not required to be obtained for each subsequent reading of a cookie. Such a reading of the law differs from industry's initial interpretation of the new law. Industry had advocated in favor of a view that would not require a change among OBA providers by generally taking the position that browser settings already supply the consent required by the new law. Although the Opinion rejects the notion that browsers can generally be used to obtain prior consent, by permitting ad networks to obtain the consent, the Working Party has interpreted the law in such a manner as to allow one entity to obtain the required consent for many sites.

**Background**

In October 2009, the European Council approved a directive of the European Parliament and the Council (the "Directive")[4] that amended the 2002 Directive on Privacy and Electronic Communications (the "eDirective").[5] Specifically, the Directive revised Article 5(3) of the 2002 eDirective explicitly to require that a visitor must "give [] his or her consent" after having been provided with "clear and comprehensive information" about the purpose of a cookie before the cookie may be used. The Directive stated that such consent was not required, however, for cookies "strictly necessary" for providers of services to provide those services "explicitly requested" by visitors to a site.[6] The Directive also explained that the consent required by the revised Article 5(3) "may be expressed by using the appropriate settings of a browser or other application."[7]

Following the release of the amendment to the eDirective, differing views on its meaning emerged ranging from those who interpreted the amendment in a manner that would not require a change in OBA practices to those who read the new law as requiring web publishers to obtain permission from consumers before using cookies. The Working Party's Opinion clarifies the manner in which informed consent must be obtained before using cookies for OBA as well as the scope of EU law that covers OBA.

**Article 29 Working Group Opinion**

Below is a brief overview of highlights from the Opinion for entities engaging in OBA in the EU:

***Scope.*** The Opinion covers OBA that occurs "across several websites" that use tracking cookies and similar devices. First-party online behavioral advertisements thus fall outside the scope of the Opinion.

***Technical Specifications for OBA.*** Rather than prescribing a technical means for complying with the framework, the Opinion invites industry to dialogue with the Article 29 Working Party on this matter.

***Application of Two Directives.*** The Opinion explains that two EU directives apply to OBA, namely the eDirective and the Directive 95/46/EC (commonly referred to as the Data Protection Directive).

***Responsibilities of Different Players.*** The Opinion outlines different obligations for the various players involved in OBA: network providers, publishers, and advertisers.

**Network Providers.** The Opinion states that Article 5(3) of the Directive obligates ad providers to obtain informed consent before placing cookies and/or retrieving information from cookies. Additionally, ad network providers have obligations under Directive 95/46/EC when the OBA involves the processing of personal data.

**Publishers.** The Opinion notes that publishers have some obligations under Directive 95/46/EC as data controllers. The Opinion advises publishers to establish service agreements with ad networks to establish roles for each party.

**Advertisers.** The Opinion states that although advertisers may act as independent data controllers, the role of advertisers falls outside the scope of the Opinion.

***Obligation Under the Amended eDirective: To Obtain Prior Informed Consent.*** The Opinion reiterates that the revised Article 5(3) of the eDirective underscores the need to obtain users' informed prior consent.

**Informed Prior Consent.** The Opinion states that ad networks must obtain consent *before* placing a cookie and/or retrieving information from a user's terminal equipment, and notes that to qualify as "informed" consent, the ad network must provide information on the sending and purposes of the cookie prior to placing the cookie.

**Revocability of Consent.** Such consent must be revocable.

**Consent via Browser Settings.** The Opinion notes that few browsers contain settings that can deliver valid prior consent.

**Consent and Opt-Out Options.** The Opinion states that opt-out mechanisms can rarely (*e.g.*, when a user is aware of OBA and knows that he can opt out but chooses not to) deliver a user's consent, and are not a mechanism that can be used to obtain the average user's informed consent.

**Prior Opt-In Consent.** The Opinion advises ad network providers to create opt-in mechanisms that require an affirmative action that indicates a user's willingness to receive cookies and the subsequent monitoring of their surfing behavior for OBA purposes. The Opinion states that a visitor's single acceptance to receive a cookie may also constitute acceptance for later readings of the cookie, and thus constitute consent to monitor Internet browsing. This clarification makes clear that the new law does *not* require an ad network provider to obtain consent for *each* reading of a cookie.

**Provision of Information in the OBA Context.** The Opinion underscores the importance of being transparent about OBA practices so that users will be informed and in a position to exercise choice.

[1] OMB Memorandum M-00-13, *Privacy Policies and Data Collection on Federal Web Sites* (June 22, 2000), *available at* http://www.whitehouse.gov/omb/memoranda_m00-13/.
[2] OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies* (June 25, 2010), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-22.pdf.
[3] Article 29 Data Protection Working Party Opinion 2/2010 on Online Behavioural Advertising, 00909/10, June 22, 2010, WP 171 (*hereinafter* Opinion), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp171_en.pdf.
[4] Directive of the European Parliament and of the Council amending Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, Oct. 22, 2009, PE CONS 3674/09 (*hereinafter* Directive), *available at* http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf.
[5] Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, July 12, 2002, Art. 5(3) (*hereinafter* eDirective), *available at* http://www.aedh.eu/plugins/fckeditor/userfiles/file/Protection%20des%20donn%C3%A9es%20personnelles/Directive_EC_2002-58-_-_eng_.pdf.
[6] Directive p. 76.
[7] Directive p. 34, ¶ 66.