VENABLE LLP

# the download

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



ISSUE EDITORS

**Stuart P. Ingis**
singis@Venable.com
202.344.4613

**Michael A. Signorelli**
masignorelli@Venable.com
202.344.8050

ADDITIONAL CONTRIBUTORS

**Emilio W. Cividanes**
ecividanes@Venable.com
202.344.4414

**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

OCTOBER 3, 2011

## In this Issue:



## Heard on the Hill

### House Examines Impact of EU Regulations on U.S. Business

On September 15, 2011, the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade ("CMT Subcommittee") held a hearing to investigate how the complexity and compliance costs of European Union ("EU") regulations impact U.S. companies. Rep. Bono Mack (R-CA), Chairman of the CMT Subcommittee, commented that the EU Data Protection Directive ("EU Directive") has created uneven regulatory regimes and unintended consequences for commerce. Rep. Stearns (R-FL) cautioned CMT Subcommittee members against embracing an EU framework. He said the EU has stifled innovation through regulation, and that if the United States had adopted a similar approach, many of the great U.S. companies and their services valued by U.S. consumers would not exist today.

Among other witnesses, Dr. Tucker from the MIT Sloan School of Management appeared and explained that her research shows that strict regulation can damage online innovation and the advertising industry. According to Dr. Tucker, the 2002 EU e-Privacy Data Directive has limited the ability of companies to collect user data for behavioral advertising and is associated with a 65% decrease in online advertisement performance.

The CMT Subcommittee's September hearing was the second in a planned series to examine privacy issues. A third hearing focusing on children's online privacy is expected to occur in October. The first hearing, held on July 14, 2011, was a joint subcommittee hearing exploring the regulation of Internet privacy, featuring witnesses from the Federal Trade Commission, Federal Communications Commission, and the National Telecommunication and Information Administration. Rep. Bono Mack has said the hearings are intended to explore how to balance innovation and privacy.

## Senate Judiciary Committee Passes Data Security Legislation

Multiple Senate committees are considering data security and breach notification legislation, following the White House's endorsement of such legislation earlier this year. Data security measures are often discussed in the context of cybersecurity, and could be added to any cybersecurity legislation that advances in Congress.

The Senate Judiciary Committee passed three data security and breach notification bills on September 22, 2011. The bills are Chairman Leahy's (D-VT) S. 1151, Personal Data Privacy and Security Act; Sen. Feinstein's (D-CA) S. 1408, Data Breach Notification Act; and Sen. Blumenthal's (D-CT) S. 1535, Personal Data Protection and Breach Accountability Act. Chairman Leahy's and Sen. Blumenthal's bills share some similarities. Both bills give the Attorney General the primary enforcement role and impose the requirements of notice to the FBI and Secret Service for any breach involving a database of a certain size, although Sen. Blumenthal has included a private right of action and increased criminal penalties for certain online data collection practices. Unlike the other bills, Sen. Feinstein's bill is limited to data breach notification and would not impose data security requirements. The Commerce Committee is also expected to consider Sen. Pryor's (D-AR) and Sen. Rockefeller's (D-WV) S. 1207, Data Security and Breach Notification Act, after a markup was scheduled for September and postponed. Finally, the Senate Banking Committee is considering Sen. Carper's (D-DE) S. 1434, Data Security Act.

The House also saw a flurry of activity on data security on the eve of the August recess. Following a series of hearings on data security, the House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade began marking up the Secure and Fortify Electronic Data Act ("SAFE Data Act") authored by Subcommittee Chairman Bono Mack (R-CA). This bill would require entities to provide security for data containing personal information and would establish a national breach notification standard. At a July markup, the Subcommittee removed a provision that would have allowed the Federal Trade Commission to redefine the "personal information" covered by the bill and clarified that the FTC lacked authority to determine the data minimization steps that could be imposed on companies. Further work on the bill has been postponed.

The House is also considering bills by Rep. Rush (D-IL) and Rep. Stearns (R-FL) who have reintroduced their respective Data Accountability and Trust Act ("DATA") bills (H.R. 1707 and H.R. 1841), which would take different approaches to requiring entities to provide security for electronic personal information and creating a national data breach notification standard.

### Location Privacy Under Consideration

Location privacy has continued to spark debate in Congress and the agencies in recent months. Following a series of hearings on mobile data, competing bills on location privacy were introduced in June: the Geolocational Privacy and Surveillance Act introduced by Representative Chaffetz (R-UT) as H.R. 2168, and by Senator Wyden (R-OR) as S. 1212; and the Location Privacy Protection Act, S. 1223, introduced by Senators Franken (D-MN) and Blumenthal (D-CT). Both bills would generally require consent for the collection of location data and include private rights of action.

At the same time, the Federal Communications Commission ("FCC") and Federal Trade Commission ("FTC") hosted a forum to explore how consumers can remain secure while enjoying the benefits of location-based services ("LBS"). The forum examined trends in LBS, industry approaches to protecting privacy, and what parents should know about children and location data. Following the forum, the FCC accepted public comments through July 8, 2011 to help inform an expected staff-level report on how consumers may navigate LBS.

## Around the Agencies

### Federal Regulators Enforce COPPA Against Mobile App Provider

The Federal Trade Commission ("FTC"), in coordination with the Justice Department, recently announced a settlement in the first public enforcement action applying the Children's Online Privacy Protection Act ("COPPA") to mobile applications ("apps"). Regulators alleged that mobile app provider W3 Innovations, LLC d/b/a Broken Thumbs Apps ("W3 Innovations"), as well as the company's president and majority owner, violated COPPA by failing to provide adequate notice of the company's privacy practices and to obtain verifiable parental consent to the collection of children's personal information.

The targeted practices and required remedies in the W3 Innovations case are similar to those in prior COPPA enforcement actions; the novelty of the case lies in the application of these patterns to the mobile app context. The Complaint takes the position that the mobile apps offered by W3 Innovations were "online services directed to children" within the scope of COPPA because they "send and/or receive information over the Internet."[1] Specifically, the apps discussed in the Complaint contained features allowing children to e-mail the company and to post blog entries and comments to the Internet.

The FTC's Consent Decree[2] requires the defendants to:

- Delete all personal information previously collected in violation of COPPA
- Pay a civil penalty of $50,000
- Comply with COPPA within 60 days
- Submit to compliance monitoring upon FTC request
- Report on compliance to the FTC, including filing a detailed written report within 60 days
- Meet detailed record-keeping requirements
- Comply with administrative requirements such as distributing the order to relevant employees

In particular, the Consent Decree requires W3 Innovations to post a privacy notice, give direct notice to parents, and obtain verifiable parental consent for data practices in connection with covered websites and online services. The settlement does not give any explicit guidance regarding how W3 Innovations should satisfy these COPPA obligations within the limitations of the mobile environment.

## FTC Request for Comments on Proposed Rule to Amend COPPA

On September 15, 2011, The Federal Trade Commission ("FTC") released a proposed rule ("Proposed Rule") to amend its Children's Online Privacy Protection Rule ("COPPA Rule"). The COPPA Rule applies to operators of commercial web sites and online services directed to children under age 13 that collect, use, or disclose personal information from children, and operators of general audience web sites that have actual knowledge that they are collecting, using, or disclosing personal information from children under the age of 13. The COPPA Rule seeks to provide parents with tools to control how information about their children is collected online. Comments on the Proposed Rule will be accepted through November 28, 2011

In the Proposed Rule, the FTC declined to advocate for applying COPPA to teenagers aged 13 and older and retained the existing rule that COPPA applies to general audience websites only when they have actual knowledge that they are collecting personal information from children. The FTC's Proposed Rule seeks to amend five key areas:

- Definitions (including "personal information" and "collection"): The Proposed Rule would extend the current definition of "personal information" to capture certain geolocation information, visual and audio files, persistent identifiers used by first parties for purposes other than internal support, and any identifiers that link children's activities across websites. The definition of what "collection" triggers COPPA would also be expanded to include "prompting" or "encouraging" children to submit information.

- Parental Notice: The FTC proposes to require "just-in-time" notice to parents before operators may collect children's personal information, rather than relying on notice only in a privacy policy.

- Parental Consent: The FTC seeks to eliminate the "e-mail plus" means of obtaining parental consent when children's personal information is used for internal purposes only. At the same time, the Commission proposes to add more non-exclusive examples of other permissible ways to obtain consent, including electronic scans of consent forms.

- Confidentiality and Security of Children's Personal Information: The FTC also proposes to require operators to delete children's personal information when it is no longer reasonably necessary and to ensure that service providers and third parties with whom they share children's personal information have reasonable procedures in place to protect the confidentiality, security, and integrity of such information.

- Self-Regulatory Safe Harbor Programs: The Proposed Rule would require safe harbor programs to annually audit each of their members and to report their findings and any disciplinary actions to the FTC.

At least once every ten years, the FTC conducts a review of its regulations to determine whether they should be retained or modified. Previously, the FTC conducted a voluntary review of the COPPA Rule in 2001 and a statutorily mandated review in 2005, retaining the COPPA Rule without change after the most recent review. The FTC explained that another review of the COPPA Rule is warranted at this time because a change has occurred in how people access the Internet, particularly through the use of mobile technology.

## FTC Reiterates Concern About Data Transfers In Bankruptcy

The head of the Federal Trade Commission's ("FTC") Consumer Protection Bureau, David Vladeck, recently questioned the planned sale of email addresses and other information for about 48 million consumers by Borders Group, Inc. ("Borders") as part of that entity's bankruptcy proceeding.[3] In a public letter, Mr. Vladeck noted that the data held by Borders included records of merchandise purchased (video and books) that could be perceived as personal by many customers. The bankruptcy court ultimately allowed the data sale to proceed, while imposing privacy restrictions that are less extensive than those preferred by the FTC.

According to the FTC's letter, at least some of the data offered for sale in the bankruptcy proceeding had been collected prior to 2008 under privacy policies stating that data would not be transferred without "express consent." A later privacy policy alerted customers that data could be transferred if Borders decided to sell, buy, merge, or otherwise reorganize the business, but Mr. Vladeck took the position that the statement would not cover the company's dissolution and piecemeal sale. Mr. Vladeck therefore suggested that the sale of Borders' customer data could be unfair or deceptive.

The FTC has repeatedly scrutinized planned sales of data assets following the dissolution of a business. Previously, the FTC alleged that a bankrupt online retailer, Toysmart.com, engaged in deceptive practices by offering its customer list for sale after its privacy policy stated that personal information would "never" be shared with third parties.[4] Similarly, Mr. Vladeck warned in 2010 that the transfer of subscriber data from a discontinued magazine could be deceptive or unfair in light of the magazine's previous privacy representations that data would not be shared.[5] Mr. Vladeck further stated that the receipt of such data by a third party, in knowing violation of the privacy policy, could also be unfair.[6]

In his letter regarding the Borders bankruptcy, Mr. Vladeck took the position that it would be appropriate for Borders to specify the prospective purchaser and seek its customers' express consent prior to transferring any data. However, citing the Toysmart settlement, Mr. Vladeck also noted that the concerns associated with data transfer would be diminished if: (1) the data were not sold as a standalone asset, (2) the new data owner were engaged in a business substantially similar to that of Borders, (3) the new owner agreed to abide by the terms of the Borders privacy policy and (4) the new owner agreed to obtain consumers' affirmative consent to any material changes to the policy.

Barnes & Noble arranged to purchase Borders' customer data along with other intellectual property assets through the bankruptcy proceeding, thereby satisfying the first two principles set out by Mr. Vladeck. However, the bankruptcy court declined to require customers' express consent either to the transfer or to any material differences between the two companies' privacy policies. Instead, the companies must provide notification of the planned sale to Borders customers via email, notices on the two companies' homepages, and a newspaper ad. Customers will have 15 days from the notice to opt out of having their data transferred to Barnes & Noble.

## In the Courts

### U.S. Supreme Court Strikes Down Law Restricting Data Mining for Marketing Purposes

In the final days of its last term, the U.S. Supreme Court struck down Vermont's Prescription Confidentiality Act, which restricted data mining of physician prescriber records for drug marketing purposes. Despite urging by the state of Vermont, 35 state attorneys general, the U.S. Department of Justice, privacy advocates, and others, a 6-3 majority of the Court joined in overturning the statute. Declining to apply the intermediate scrutiny test used in past commercial speech cases, the Court instead applied the heightened scrutiny test reserved for government restrictions that are based on the content of the speech or the viewpoint of the speaker.

It has long been established that truthful commercial speech is generally protected by the First Amendment. In *Sorrell v. IMS Health*, the Supreme Court found that Vermont had imposed an impermissible burden on

protected expression by selectively burdening the sale, transfer, or use of personally identifying information used for marketing communications.[7] The ruling emphasizes that a governmental desire to protect people from persuasive speech, such as effective marketing, is not a lawful basis for restricting truthful commercial speech. *Sorrell* clarifies that legislative proposals seeking to regulate commercial data practices, including marketing and advertising activities, face high constitutional hurdles.

### *Case Background*

Vermont's Prescription Confidentiality Act, passed in 2007, sought to restrict the sale, disclosure and use of records on the pharmaceutical prescribing practices of individual doctors. Pharmaceutical companies use such data, stripped of patient identifying information, to improve and target their marketing to physicians. In relevant part, Vermont's statute provided that, subject to certain exceptions including the doctor's consent, pharmacies could not sell or use prescriber data for marketing. The law also banned drug manufacturers from using such data for marketing. Vermont offered several rationales for these restrictions, including privacy justifications and a concern that effective prescription drug marketing is not in the best interests of patients or of the State, which bears the burden of increasing health care costs. Data mining companies and drug manufacturers challenged the law, which was upheld by the trial court but overturned by the Second Circuit Court of Appeals.

### *U.S. Supreme Court Decision*

*Subjecting the law to "heightened scrutiny"*

Justice Kennedy, writing for the Court, concluded that the Vermont law raised First Amendment concerns because the State sought to restrict the availability and use of prescriber data based on (1) the identity of the recipient (pharmaceutical manufacturers) and (2) the content of the recipient's speech (marketing purposes).[8] Because Vermont's restrictions disfavored certain speakers and content, the Court found that the law should be examined under a "heightened scrutiny" standard. To survive such heightened scrutiny, the government would have to show that the restriction directly advances a substantial government interest and is drawn to achieve that interest.[9] The Court ruled that Vermont's law did not satisfy this standard.

*Vermont's privacy rationales were not persuasive*

Vermont first argued that its law was needed to protect medical privacy, including physician confidentiality. The Court found that the statute was not drawn to serve these interests because it permitted widespread sharing of data with all but a "narrow class of disfavored speakers."[10] The Court noted that a more comprehensive ban on data sharing would present a different question.

The Court further found that the statute's provision allowing data sharing with the prescribing physician's consent did not save the statute, because it merely allowed a limited degree of privacy on terms favorable to certain speech preferred by the government.[11] For the same reason, the Court noted that reversing the law's default so that physicians would have to agree individually to the data restrictions also might not make the law constitutional. [12]

The Court dismissed Vermont's arguments that the law was needed to protect physicians from harassing marketing visits and because the use of prescriber data undermines the doctor-patient relationship by influencing treatment decisions. The Court stated that "the fear that speech might persuade provides no lawful basis for quieting it."[13] Similarly, the Court likewise rejected Vermont's proffered goals of improving public health and reducing healthcare costs, concluding that Vermont may not "burden the speech of others in order to tilt the public debate in a preferred direction."[14]

*Implications for privacy regulation*

In closing, the Court spoke to the ongoing public debate over privacy regulation, stating that "[t]he capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure. In considering how to protect those interests, however, the State cannot engage in content-based discrimination to advance its own side of a debate."[15]

## International

### The EU Begins to Implement Requirements for Obtaining Consent to Use Cookies

For most EU member countries, the formal implementation date for the much-publicized cookie consent provisions of the 2002 EU Directive on Privacy and Electronic Communications came and went without a change to their respective national laws. Although all 27 member countries of the EU were supposed to implement consent provisions into their national laws by May 25, 2011, only Estonia, Finland, and the UK met that deadline by implementing some form of consent into local law. France, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Malta, and Sweden subsequently followed suit (after the deadline). The remaining member countries remain further behind on the path to implementation.

Even with a minority of EU states complying with the amended Directive, those countries that have taken action have failed to recognize a uniform means of obtaining consent from users, leaving companies who operate multi-jurisdictional websites without a a clear standard to implement

*The UK's Approach*

In advance of the implementation deadline, the United Kingdom followed up its earlier, more general discussion of the topic with some specific guidelines for industry. This Guidance, published by the UK Information Commissioner's Office ("ICO") is called "Changes to the rules on using cookies and similar technologies for storing information," and advises industry to check what type of cookies they are using, to assess how "intrusive" their use of cookies is, and to decide what solution to obtain consumer consent will be best.[16]

The Guidance suggests several different ways for businesses to obtain consent. Consistent with the Guidance's desire for individual businesses to determine the most appropriate means of consent for their website, none of these methods is recommended above another. The Guidance cites the following possibilities:

- Popups and similar techniques: The ICO calls this an "easy option to achieve compliance" and a "useful way of informing users of the techniques you use," but acknowledges that it may spoil the experience of a consumer on a website that uses several cookies.

- Terms and conditions: Consent may be obtained via the terms of use, provided that the consumer is made aware of any changes to the terms and specifically that these changes refer to the use of cookies. Users must then opt-in to the new terms.

- Settings-led consent: Consent may be obtained when a consumer makes a choice about how they want the site to work, such as when a consumer agrees to certain settings they have chosen.

- Feature-led consent: Consent may also be obtained when a user chooses to use a particular feature of a website, such as watching a video clip.

- Functional uses: Webpages can place text, in the footer or header of a webpage, that is highlighted or permits scrolling when setting a cookie on the consumer's device.

The Guidance acknowledges that third party consent is the "most challenging area in which to achieve compliance," and that they are continuing to work with industry and other European authorities to develop solutions. At present time, the Guidance does favorably note the use of "initiatives" that "allow [] users to make informed choices about what is stored on their device," but also keeps open the possibility of supplementing this advice with further examples.

The press release accompanying the Guidance also noted a one-year grace period on enforcement of the consent provisions, to May 26, 2012.

*France's Approach*

On August 24, 2011, France also implemented new consent requirements for cookies as well as disclosure and notification rules related to data breaches.[17] The French law complies with the EU Directive by requiring companies to provide comprehensive information and obtain users' consent prior to the use of cookies. France does, however, permit this consent to be obtained from settings on the user's device. France's law follows the UK's lead by allowing browser settings to be a valid source of consent. Unlike the UK, France does not explicitly require consumers to make an affirmative choice, seemingly leaving the door open for implied consent. Noncompliance with the provision may be punishable by up to five years' imprisonment and a sizeable fine.

## About Venable

An *American Lawyer* Global 100 law firm, Venable serves corporate, institutional, governmental, nonprofit and individual clients throughout the U.S. and around the world. Headquartered in Washington, DC, with offices in California, Maryland, New York and Virginia, Venable LLP lawyers and legislative advisors serve the needs of our domestic and global clients in all areas of corporate and business law, complex litigation, intellectual property, regulatory, and government affairs.

## 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




---

[1] Complaint, *United States v. W3 Innovations et al.,* No. 03958-PSG (N.D. Cal., filed Aug. 12, 2011) at ¶ 12.
2 Consent Decree and Order for Civil Penalties, Injunction, and Other Relief, *United States v. W3 Innovations, LLC and Justin Maples*, CV11-03958 (N.D. Cal., August 12, 2011).
[3] Letter from David C. Vladeck, FTC Consumer Protection Bureau, to Consumer Privacy Ombudsman (September 14, 2011).
[4] First Amended Complaint for Permanent Injunction and Other Relief, *FTC v. Toysmart.com, LLC et al.* (D. Mass, July 21, 2000), available at http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm.
[5] Letter from David Vladeck, FTC Bureau of Consumer Protection, to Peter Larson and Martin E. Shmagin (July 1, 2010), available at http://www.ftc.gov/os/closings/100712xy.pdf.
[6] *Id.* at 3.
[7] *Sorrell v. IMS Health Inc. et al.*, 564 U.S. __ (2011).
[8] *Id.* at 8.
[9] *Id.* at 16.
[10] *Id.* at 18.
[11] *Id.* at 18
[12] *Id.* at 19.
[13] *Id.* at 20-21.
[14] *Id.* at 23.
[15] *Id.* at 24.
[16] Information Commissioner's Office, "Changes to the rules of using cookies and similar technologies for storing information," available at www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.pdf (May 9, 2011).
[17] Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques, *available at* http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024502658&fastPos=1&fastReqId=109813509&categorieLien=id&oldAction=rechTexte.