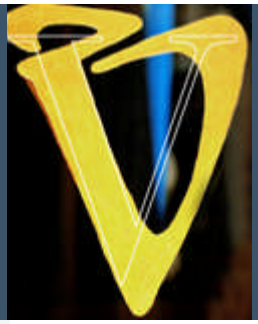
VENABLE LLP



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

MAY 2011

In this Issue:

Washington has recently ratcheted up its interest in issues of privacy, cybersecurity, and data security. In the last several weeks, new legislation has been introduced; several Congressional hearings have been held to examine privacy implications for online, offline, and mobile data; the White House has issued reports calling for cyber legislation; and federal agencies have continued their examination of industry data practices.

This issue of the Download covers these recent developments. There are articles reporting on recent legislative developments concerning privacy, data security, online intellectual property infringement, and reform of the Electronic Communications Privacy Act. This issue of the Download also includes articles that report on the examination of mobile by Congress and federal agencies, calls by the White House for cybersecurity legislation, the Obama Administration's strategy for trusted identities in cyberspace, and the Federal Trade Commission's enforcement action against an ad network. Finally, there is an article on the United Kingdom's implementation plan for the EU Privacy Directive concerning cookies.

Heard on the Hill

House and Senate Consider Privacy and Data Security

Several legislative proposals concerning privacy and data security are under consideration by Congress. Any of these bills, should one or more be passed, could have an impact on business models that rely on the seamless flow of information for use in products and services offered in the marketplace. This article identifies the key developments in the Senate and House.

Senate Developments

Following a full hearing before the Senate Committee on Commerce, Science, & Transportation ("Senate Commerce Committee") in March 2011, Sen. Kerry (D-MA) and Sen. McCain (R-AZ) introduced the "Commercial Privacy Bill of Rights Act." This bill would establish a regulatory framework governing the online and offline collection, use, and dissemination of personally identifiable information in commerce. This bill would impose new notice and choice requirements, and establish certain access, correction, and anonymization obligations for covered entities.

Building on the do-not-track ("DNT") concepts included in the Federal Trade Commission's ("FTC") 2010 Preliminary Staff Report on privacy, Sen. Rockefeller (D-WV), Chairman of the Senate Commerce Committee, introduced the "Do-Not-Track Online Act" on May 9, 2011. This bill would direct the FTC to establish standards for a DNT mechanism through which an individual could "simply and easily" indicate a preference to prevent online service providers, including those that provide mobile applications and services, from collecting an individual's "personal information." Providers of such services and applications would be prohibited from collecting personal information from an individual who expresses that preference through the DNT mechanism. The choice mechanism, however, would not apply to collection that is: (1) necessary to provide a requested service (provided the information is anonymized or deleted upon the service's provision); or (2) where the individual affirmatively consents to a "clear, conspicuous, and accurate" notice regarding the collection and use of the information.

On May 10, 2011, the new Senate Judiciary Subcommittee on Privacy, Technology and the Law held its first hearing to consider the privacy and security implications surrounding the collection, use, and sharing of information gathered from mobile devices and applications. The Senate Commerce Committee also held a hearing on May 19, 2011 to consider consumer privacy and the mobile marketplace.

House Developments

In April 2011, Rep. Stearns (R-FL) introduced the "Consumer Privacy Protection Act." This bill would require covered entities to provide consumers with brief privacy notices in certain instances, as well as to post longer privacy policy statements; give consumers the ability to opt out of having their data sold to non-affiliated entities absent contractual

protections; and oblige covered entities to have information security policies that meet certain requirements. In addition, Rep. Rush (D-IL) has reintroduced his "BEST PRACTICES Act" from last Congress. Like the legislation proposed by Rep. Stearns, Rep. Rush's bill would impose restrictions on the online and offline collection and transfer of consumer data. Under his proposed framework, entities that comply with approved self-regulatory programs would be permitted to transfer data to third parties subject to an opt out. The bill would also create accuracy, access, and dispute resolution obligations on covered entities.

Interest in children's privacy continues to be high. On May 13, 2011, Rep. Markey (D-MA) and Rep. Barton (R-TX) introduced the "Do Not Track Kids Act." This bill would amend the Children's Online Privacy Protection Act to extend, enhance, and update the provisions relating to the collection, use, and disclosure of children's personal information and would establish new protections for personal information of children and teens.

Proposals regarding data security and breach notification are also being debated. On May 4, 2011, the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade held a hearing on data security. Subcommittee Chairman Bono Mack (R-CA) indicated that she will soon introduce a data security bill that would focus on providing consumers with timely notice of data breaches. On the same day as the hearing, Rep. Rush reintroduced his DATA Act, which was passed by the House in the 111th Congress. This bill 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. On May 12, 2011, Rep. Stearns also introduced a bill that would similarly require companies to provide reasonable security to protect computerized data containing personal information, and would establish a nationwide breach notification standard.

Congress Examines Online IP Issues

Members of Judiciary Committees in both chambers have identified combating piracy online as a priority for the 112th Congress. In the 111th Congress, the Senate Judiciary Committee considered legislation to combat illegal infringement with a particular focus on the role that registrars, registries, ad networks, Internet service providers ("ISPs"), and payment system providers could play in addressing the issue. That bill, known as the Combating Online Infringement and Counterfeits Act ("COICA"), was aimed at shutting down websites that traffic pirated goods and content.

On May 12, 2011, Sen. Leahy (D-VT), Chairman of the Senate Committee on Judiciary, introduced the "Preventing Real Online Thefts to Economic Creativity and Theft of Intellectual Property Act of 2011" or the "PROTECT IP Act." The PROTECT IP Act, which builds from COICA and incorporates some concerns expressed by stakeholders, also seeks to address rogue sites. The bill would grant the Attorney General authority to bring suits against registrants, owners, or operators of rogue sites, as well as suits against the domain names used by the rogue sites. Additionally, the Attorney General would be permitted to obtain court orders requiring ISPs and search engines to cut off access to such sites, or requiring payment processors and ad networks to cease conducting business with

the rogue sites. Rights holders would also have the option bring actions against registrants, owners, operators, and domain names of the rogue sites. To promote voluntary actions outside of court orders, the bill would protect from liability payment processors and ad networks that take actions against rogue sites. The bill would also provide a safe harbor to registries, registrars, search engines, payment processors, and ad networks that voluntarily take action against rogue sites that endanger the public health. Chairman Leahy has stated that while the bill does not provide a comprehensive solution to the rogue site issue, it nonetheless would create an environment where it would be more difficult for such sites to profit from American ingenuity.

The House also considered this matter in a two-part hearing, held on March 14, 2011 and April 6, 2011, when Judiciary Intellectual Property, Competition and the Internet Subcommittee Chairman Goodlatte (R-VA) convened a hearing to explore ways to promote investment and protect commerce online. While Chairman Goodlatte has stated that legislation is necessary to address rogue sites, he has also said that industry must be part of the solution by continuing to set forth technical solutions and business models that address the issue. Chairman Goodlatte has indicated that he intends to examine the issue from a blank slate, rather than using COICA as a starting point. A bill from the House side is expected to be introduced shortly.

Proposed Reform of the Electronic Communications Privacy Act

Senate Judiciary Chairman Patrick Leahy (D-VT) introduced legislation to update the update the Electronic Communications Privacy Act ("ECPA") on May 17, 2011. Among other amendments to ECPA, Sen. Leahy's legislation would:

- Prohibit service providers from voluntarily disclosing communications contents to law enforcement, while permitting disclosure pertinent to a cyberattack;
- Require a search warrant, issued based on probable cause, to obtain communications contents, regardless of the age of a communication;
- Require notice to an individual when communications contents are disclosed, including a copy of the search warrant, although delays are authorized under certain circumstances; and
- Establish new standards for government access to geolocation information from mobile devices and applications, including real-time and historical information.

Sen. Leahy's interest in ECPA dates to his instrumental role in enacting the statute. On April 6, 2011, he convened a hearing before the Senate Judiciary Committee entitled "The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age." The hearing involved government testimony on the subject of ECPA reform, but senators and witnesses also discussed whether ECPA reform legislation should include limits on commercial data sharing.

The hearing witnesses were Cameron Kerry, General Counsel of the Commerce Department, and James A. Baker, Associate Deputy Attorney

General in the U.S. Department of Justice. Mr. Kerry's testimony argued that Congress should seek to create a principled relationship between law enforcement access to electronic materials and access in the physical world, while also taking into account consumers' privacy expectations. Mr. Baker emphasized the importance of ensuring continued law enforcement access to electronic evidence for investigations and prosecutions, but identified eight areas of ECPA that may be ripe for reconsideration.

The government witnesses did not offer or endorse specific legislative proposals, but stated that their agencies have been working toward agreement on areas where amendments or updates to ECPA would be appropriate. Both Sen. Leahy and Sen. Grassley noted that Congress is awaiting such legislative proposals from the Administration.

The recent hearing evidenced a continuation of congressional leaders' interest in ECPA reform. During the 111th Congress, several hearings on different aspects of ECPA reform were convened by the Senate Judiciary Committee as well as by Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the House Judiciary Committee.

Mobile under the Microscope

In the wake of news reports on data collection practices associated with mobile devices, the Federal Trade Commission ("FTC") and both houses of Congress are scrutinizing privacy issues in the mobile realm.

Senate Subcommittee Hearings

Key subcommittees of two Senate committees have both taken an interest in mobile privacy issues. The Senate Judiciary Subcommittee on Privacy, Technology and the Law held a hearing on May 10, 2011, entitled "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy." The hearing was the first convened by Sen. Al Franken (D-MN) in his role as chairman of this new subcommittee. Prior to the hearing, Sen. Franken sent a letter to Apple requesting additional information about public reports that Apple's iOS 4 operating system (used in iPhones and iPads) stored location data in an unencrypted format.

The hearing focused on this incident involving Apple as well as broader privacy and security implications surrounding the collection, use, and sharing of information gathered from mobile devices and applications. In his opening statement, Sen. Franken signaled that his Subcommittee will focus on privacy issues raised by the collection of consumer data by private corporations. He expressed the belief that existing law is insufficient, and stated that the purpose of his newly formed subcommittee is to educate the public, raise awareness, and legislate if necessary.

The Subcommittee heard testimony from Jessica Rich of the Federal Trade Commission ("FTC"), Jason Weinstein of the U.S. Department of Justice, and several industry stakeholders and advocates. Ms. Rich, in her testimony, revealed that "[FTC] Staff has a number of active investigations into privacy issues associated with mobile devices, including children's privacy." At least one of these investigations is

public. In February, the FTC filed suit in federal court against individual defendant Phillip Flora, alleging that Mr. Flora transmitted millions of unsolicited commercial text messages to consumers in violation of the CAN-SPAM Act, including deceptive advertisements.

Mr. Weinstein identified two main threats tied to mobile: (1) use of mobile data to perpetrate crimes, and (2) the collection and disclosure of location and other information by the data collectors. Mr. Weinstein stated that the Justice Department will shortly unveil a package of legislative proposals that will address mobile privacy, and expressed the view that the private sector should retain data for longer periods of time in order to aid law enforcement investigations.

The Senate Commerce Subcommittee on Consumer Protection, Product Safety and Insurance also held a hearing on May 19, 2011 to consider consumer privacy and protection in the mobile marketplace. The Subcommittee considered ways consumers could be made better aware of mobile data practices and the appropriate approach to protecting consumer data, with a particular focus on use of mobile devices and applications by children and teens. There was discussion of the various privacy bills before the Senate Commerce Committee, but Subcommittee members stopped short of calling for mobile-specific legislation.

The hearing was chaired by Sen. Pryor (D-AR) and was well-attended by a bipartisan group of senators: Sen. Rockefeller (D-WV), Sen. Kerry (D-MA), Sen. Klobuchar (D-MN), Sen. McCaskill (D-MO), Sen. Udall (D-CO), Sen. Toomey (R-PA), Sen. Blunt (R-MO), Sen. Thune (R-SD), Sen. Hellar (R-NV), Sen. Boozman (R-AR), and Sen. Rubio (R-FL). The Subcommittee heard from the following witnesses: David Vladeck of the Federal Trade Commission; Bret Taylor of Facebook; Morgan Reed of the Association for Competitive Technology; Catherine Novelli of Apple; Alan Davidson of Google Inc.; and Amy Guggenheim Shenkan of Common Sense Media.

Sen. Rockefeller, whose committee has oversight jurisdiction of the FTC, commented during the hearing that the FTC has not been aggressive on privacy and specifically stated his belief that many mobile applications are violating the Children's Online Privacy Protection Act. Sen. Kerry spoke in favor of his recently-introduced privacy legislation, and commented that mobile applications often do not include privacy policies. In response to a question from Sen. Klobuchar, Mr. Vladeck noted that there would be challenges in giving consumers' uniform choice regarding data collection for mobile devices.

House Commerce Committee Letters

Key members of the House of Representatives have also shown interest in mobile privacy issues. Rep. Fred Upton (R-MI), Chairman of the House Energy and Commerce Committee, along with several colleagues from his committee, sent letters on April 25, 2011, to Apple and other developers of smartphone operating systems. The letters posed numerous questions about the companies' practices related to the tracking, use, storing or sharing of location data. In addition, the congressional leaders requested the companies' opinions about whether operating system developers are or should be subject to privacy restrictions such as those in Section 222 of the Communications Act, which addresses the privacy of customer proprietary network information handled by telecommunications carriers.

Federal Communications Commission Roundtable

On June 28, 2011, the Federal Communications Commission ("FCC") will host a public education forum to consider location-based services. Topics that will be discussed include the benefits and risk associated location-based services, industry best-practices, and how consumers can safely and securely use location-based services. The FCC intends to issue a staff report on location-based services following this forum, and has invited comment on these topics. Comments are due July 8, 2011.

From the White House

White House Calls for National Strategy for Trusted Identities in Cyberspace

On April 15, 2011, the White House released a report entitled "National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy" ("NSTIC" or "Strategy"). The NSTIC strategy calls for the creation of an "Identity Ecosystem" that would permit individuals to complete different online transactions using a centralized identity authentication system, eliminating the need to create and remember different log-in credentials for different websites. As described in the Strategy, after the consumer sets up a trusted digital identity and receives a digital credential, the consumer can then use this credential to liaise with different websites that have agreed to accept it in lieu of a conventional log-in/password. The credential would provide the appropriate level of information to each website for user authentication. For example, at a "low-assurance" transaction website, such as a website where the consumer completes a small-dollar purchase, the NSTIC credential would provide only the basic authentication information necessary to complete the transaction. For a higher-assurance website, such as a website containing the consumer's medical or financial records, the NSTIC credential would provide an advanced level of "identity proofing" to the website.

The Strategy envisions that a number of different third parties could become "identity providers" responsible for establishing, maintaining, and securing digital identities associated with individual consumers. Different credential providers may potentially provide different levels of security.

The report proposes setting up an interagency office within the Department of Commerce to be known as the National Program Office ("NPO") that will be charged, consistent with statutory authorities, with achieving the goals of the Strategy. The Report sets an interim benchmark of 3-5 years for the standardization of policy and technology and the establishment of a marketplace of private-sector identity providers and relying partner websites that agree to accept trustmarked credentials.

White House Presents Cybersecurity Legislative Proposal

Cybersecurity remains a primary focus of Congress and the Obama Administration. On May 12, 2011, the Obama Administration delivered its cybersecurity legislative proposal to Congress. The proposal would make the Department of Homeland Security ("DHS") the primary arbiter and enforcer of cybersecurity policy by vesting extensive, primary authority within DHS for cybersecurity, both by giving it responsibility over the standards and oversight that will govern the "critical infrastructure" of the private sector and by making it directly responsible for government networks and systems. A new cybersecurity center would be created within DHS for this purpose. The Department of Justice would also receive new tools to fight criminal cybersecurity violations through increased criminal penalties, primarily to be implemented through revisions to the Computer Fraud and Abuse Act.

The White House proposal also calls for data breach notification legislation. The proposal borrows heavily from similar bills previously approved by the Senate Judiciary Committee, authored by Sen. Leahy (D-VT) (S. 495 in the 110th Congress, as reported) and Sen. Feinstein (D-CA) (S. 139 in the 111th Congress). In particular, the White House drew on these earlier proposals in defining the data covered by the notification requirement; establishing exemptions for financial fraud programs and national security and law enforcement purposes; and determining the content and means of notification. The proposal also introduces some new elements not previously considered, namely by: tasking the Federal Trade Commission ("FTC"), rather than the Justice Department, with enforcing the notification rules; tasking the FTC with responsibility for receiving the results of risk assessments in those instances where companies believe there is no need to notify because there is no "reasonable" risk of harm; and naming DHS as the first point of contact for law enforcement notifications.

During the last Congress, five separate cybersecurity bills were introduced, and this Congress has already seen the introduction of one bill—the "Cyber Security Public Awareness Act of 2011" (S. 813), authored by Sen. Whitehouse (D-RI). The Act's stated purpose is to raise public awareness of cyber threats by requiring stakeholders from within the government to provide reports to Congress about cyber attacks, perceived vulnerabilities, and ways to improve security. A number of new cybersecurity bills are expected in the coming months, including bills by Sen. Klobuchar (D-MN) governing cloud computing and Sen. Hatch (R-UT) on improving and strengthening the response to cybercrime.

The Senate's focus on cybersecurity was evidenced on April 12, 2011 when the Senate Judiciary Subcommittee on Crime and Terrorism held a hearing entitled "Cyber Security: Responding to the Threat of Cyber Crime and Terrorism." The hearing covered a wide variety of topics, including the number of federal personnel dedicated to cybercrime investigation and enforcement, efforts to prevent state sponsored cyberattacks by foreign governments, and incentivizing the private sector to improve cybersecurity protection.

Around the Agencies

Chitika Settles with the Federal Trade Commission

The Federal Trade Commission ("Commission" or "FTC") on March 14, 2011, announced In the Matter of Chitika, Inc., File No. 1023087, the Commission's first online behavioral advertising ("OBA") case. On that day, the Commission stated that it had accepted, subject to final approval, a consent agreement with Chitika, which the FTC described as an ad network engaging in OBA. The consent agreement defines OBA to mean "the practice of tracking a consumer's online activities in order to deliver advertising targeted to the individual consumer's interests." In the Commission's earlier complaint, the FTC had alleged that although Chitika's privacy policy stated that it would permit consumers to opt out of having their cookies placed on their browsers for OBA purposes, from at least May 2008 through February 2010 the company's opt out was effective for only 10 days. The complaint alleged that consumers were not informed of this expiration.

The settlement will require Chitika to provide specific notice to consumers "within close proximity" to the ad and a link to an opt-out mechanism within the ad itself. The notice must clearly and prominently disclose:

- The company collects information about consumers' activities on certain websites to deliver targeted ads;
- By opting out, the company will not collect information for the purpose of delivering targeted ads;
- The current status of a consumers' choice; and
- The consumer's choice is specific to the browser, and they must implement the mechanism again if they use a different browser.

Additionally, the settlement bars Chitika from using, disclosing, or transferring any information that can be associated with a user or a user's computer or device and that was collected during the 2008-2010 time period when the opt out allegedly expired after 10 days. The settlement also requires Chitika to place a clear and prominent notice, including a hyperlink, on its homepage indicating that it collects information about consumers' activities on certain sites for OBA, as well as a notice to consumers that those who opted out prior to March 1, 2010 must renew their opt out to avoid targeted ads. When consumers choose the opt out, the settlement requires Chitika to honor that choice for at least five years.

In Europe

UK Leads the Way in Implementing EU Privacy Directive Cookie Consent Provisions

The United Kingdom (UK) became the first Member State to announce its plans for implementing amendments to the 2002 EU Directive on Privacy and Electronic Communications (the "ePrivacy Directive"), including the much-publicized cookie consent provisions. Public statements made in connection with the release of the "Implementing the revised EU Electronic Communications Framework" ("Report"), outlining the UK's "overall approach" to implementing the ePrivacy Directive, indicates it is a priority to avoid interrupting use of digital technology and the Internet.

The UK is pursuing a three-pronged approach to meeting the ePrivacy Directive. First, it will work with browser manufacturers to see if browser settings can be enhanced to meet the consent requirements set forth in the ePrivacy Directive. Next, the UK is also supporting cross-industry work on third-party cookies used for online behavioral advertising ("OBA") and supports the lead industry approach, which the Report describes as "an easily recognizable internet icon, a privacy policy notice, a single consumer control page, with a self-regulatory compliance and enforcement mechanism." (Report, para. 323.) Third, the UK will continue exploring other solutions in order to meet the demands of new technologies. The UK plans to set up a second working group to explore these alternative solutions.

The Report indicates that a "one size fits all" solution is not appropriate for the UK and that the UK will continue to explore a "more flexible and responsive UK ecology of solutions." (Report, para. 325.) During the period while alternative technical solutions are being developed, the Report notes that it does not expect enforcement actions against businesses that are working to address the use of cookies. The EU Directive has a May 25, 2011 implementation deadline across the EU, so companies should expect to see other member states making their implementation plans public soon.

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, DC and offices in California, Maryland, New York, and Virginia.

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

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

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

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

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

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

The law firm advertisers turn to for regulatory, policy and enforcement issues.

VENABLE® LLP