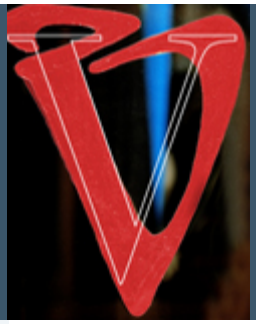
VENABLE LLP



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

Kelly A. DeMarchis
kademarchis@Venable.com
202.344.4722

Tara Sugiyama Potashnik
tspotashnik@Venable.com
202.344.4363

Julia Kernochan Tama
jktama@Venable.com
202.344.4738

Ariel S. Wolf
aswolf@Venable.com
202.344.4464

1.888.VENABLE
www.Venable.com

March 2013

In this Issue:

Heard on the Hill

Rockefeller Reintroduces Do Not Track Legislation

Chairman of the Senate Commerce Committee Jay Rockefeller (D-WV) on February 28, 2013 reintroduced his Do-Not-Track Online Act bill. He previously introduced the bill in the 112th Congress, but it gained no traction.

The Do-Not-Track Online Act would require the Federal Trade Commission ("FTC") to issue regulations regarding the collection and use of personal information concerning individuals' online activities. Specifically, the FTC would be required to establish standards for a do-not-track ("DNT") mechanism where persons could "simply and easily" indicate their preference for whether their personal information may be collected by online service providers, including those that provide mobile applications and services. Online service providers would be prohibited from such personal information collection when persons choose, through the DNT mechanism, not to have the information collected. Regardless of any preference expressed by individuals with the DNT mechanism, however, personal information would be permitted to be collected when it is: (1) necessary to provide a requested

service (provided it is anonymized or deleted upon the service's provision); or (2) where a person affirmatively consents to "clear, conspicuous, and accurate" notice of the information collection and use.

From the White House

President Signs Executive Order on Cybersecurity

President Obama used the occasion of his State of the Union Address to announce that he signed a cybersecurity executive order earlier that day, which was issued with an accompanying Presidential Policy Directive. The executive order was formally rolled out at a press event the following day, which featured speakers from multiple government agencies, including the Department of Commerce, the Department of Homeland Security, and the National Security Agency. The executive order does not preclude the introduction of cybersecurity legislation. Instead, many of the speakers at the press event discussed the executive order as a "down payment" on eventual legislation. Comprehensive cybersecurity legislation has not yet been introduced in this Congress.

The executive order directs federal agencies to develop standards designed to protect critical infrastructure. Development of these standards will largely reside with the National Institute of Standards and Technology ("NIST") within the Department of Commerce. NIST will facilitate the information gathering that underpins development of the standards by soliciting industry input through multistakeholder processes, requests for information, and workshops. The ultimate result of this process would be a "baseline framework" of standards that govern critical infrastructure. The framework is intended to be flexible and technology neutral, and will adapt over time, although a preliminary framework will be required to be published by NIST within 240 days of the date of the order. The Department of Homeland Security would have responsibility for developing a voluntary program to support industry's adoption of the framework. As part of the executive order's rollout, NIST issued its first Request for Information, seeking information on some of industry's existing cybersecurity practices.

The executive order also seeks to facilitate information sharing by requiring the timely production of unclassified reports of cyber threats, intended to be shared with industry. Classified information sharing would also be increased with the order. Additionally, the executive order speaks to privacy concerns and requires Homeland Security to produce a public report on any risks to privacy and civil liberties arising from activities in connection with the activities facilitated by the cybersecurity report. The first deadline tied to the executive order happens 120 days from the

date of the order, when the Secretary of Homeland Security, the Attorney General, and the Director of National Intelligence are required to issue instructions to ensure the timely production of the unclassified reports of cyber threats discussed above.

Around the Agencies

Federal Trade Commission Issues Recommendations for Mobile Privacy Disclosures

In February, the Federal Trade Commission ("FTC") released a staff report on "Mobile Privacy Disclosures: Building Trust through Transparency." FTC staff predict in the report that policy, enforcement, and education will all be key areas in the agency's ongoing work on mobile privacy.

In the policy arena, the new report includes recommendations aimed at platforms, app developers, third parties (including ad networks), and trade associations. These recommendations, which are independent of the NTIA's multistakeholder process, are based in part on the mobile privacy disclosures panel convened by the FTC in May 2012 as part of an event on updating the agency's "Dot Com Disclosures" advertising guidance. The FTC's report is independent of the recent recommendations issued by the California Attorney General, but FTC officials have stated that the FTC views the two sets of recommendations as consistent.

The FTC's new recommendations encourage "platforms" (providers of operating systems and corresponding app markets) to provide timely disclosures and obtain users' affirmative express consent before allowing apps to access sensitive data (such as geolocation) or other data that may be sensitive depending on context (such as address books). The report also suggests that platforms should impose privacy best practices on app developers by contract, consider additional transparency methods such as icons, and consider offering a user choice mechanism for third-party data collection across apps.

While the report notes that app developers should not duplicate platforms' efforts, the FTC recommends that app developers should offer a privacy policy coupled with timely disclosures and affirmative express consent if not already provided by the platform. The FTC also calls on both app developers and third parties such as ad networks to improve coordination on third-party practices. Finally, the FTC urges trade associations to engage in policy efforts such as developing uniform short form disclosures and privacy policies.

Federal Trade Commission Announces Mobile Privacy Enforcement Actions

Continuing the Federal Trade Commission's ("FTC") focus on

mobile issues, the agency recently announced two enforcement actions related to companies' mobile privacy and security practices. The companies involved have neither admitted nor denied the FTC's allegations.

First, the FTC settled a complaint involving mobile privacy against social networking application Path. The FTC claimed that Path engaged in unfair or deceptive acts or practices when it collected address book data from users without disclosing this practice in its privacy policy and regardless of whether users declined a "find friends from your contacts" option. The FTC further alleged that Path violated the Children's Online Privacy Protection Act ("COPPA") by collecting personal information from users known to be children under 13 without parental notice or consent.

In the settlement, Path agreed to implement a comprehensive privacy program and will also provide prominent notice of address book data collection and obtain affirmative express consent prior to such collection. Although this requirement is binding on Path specifically, the FTC's report on mobile privacy disclosures, released the same day as the Path settlement documents, recommends that all app developers follow similar steps for information that may be sensitive in context. Path additionally paid civil penalties of $800,000 and will delete all children's personal information to settle the COPPA allegations.

Second, the FTC settled a complaint against mobile device manufacturer HTC America ("HTC") alleging that HTC failed to provide "reasonable and appropriate" security in designing and customizing software for its devices. The FTC took the position that HTC's security practices were unfair to consumers, and also claimed that certain user manuals and interfaces were deceptive in light of these practices. Among these alleged failures, the FTC alleged that HTC did not provide security training for engineering staff, did not assess security of its devices, failed to follow well-known secure programming practices, and did not have a process for third parties to report vulnerabilities. The FTC stated that these practices created a risk of consumer harm resulting from unauthorized data access, but did not allege that such access or harm actually occurred.

HTC agreed to release software patches to address vulnerabilities, to establish a comprehensive information security program, and to undergo independent security assessments for the next 20 years. The FTC will hold a one-day mobile security forum on June 4, 2013 that will focus on threats to smartphones and other mobile devices.

In the States

State Legislatures Consider Privacy

Attention to privacy matters is increasing among state legislatures.

Several state assemblies are considering privacy bills including California, Hawaii, Maryland, and Montana.

The California State Assembly is considering legislation that would change the privacy policy requirements for operators of commercial websites or online services that collect personally identifiable information. California Assembly Bill 242 would amend the California Online Privacy Protection Act. Specifically, the bill would require an online privacy policy to:

- be no more than 100 words;
- be written in clear and concise language;
- be written at no greater than an 8th grade reading level; and
- include a statement indicating whether the personally identifiable information may be sold or shared with others, and if so, how and with whom the information may be shared.

The bill was referred to the Judiciary Committee and is working through the committee process.

In Hawaii, legislators are considering a proposal that would require operators of commercial websites or online services that collect personally identifiable information about Hawaii residents to "conspicuously post" privacy policies on their websites or through any other reasonably accessible means. The legislation would also require privacy policies to identify the categories of personally identifiable information that the operator collects through the website or online service and the categories of third parties with whom the operator shares such information. The Hawaii Senate Committee on Technology and the Arts held a hearing on this legislation on February 5, 2013, where several industry organizations expressed opposition to the language as drafted.

In Maryland, lawmakers have proposed legislation that would make violations of the federal Children's Online Privacy Protection Act ("COPPA") actionable in Maryland courts. The bill, HB-316, would prohibit a person from violating COPPA. HB-316 would also specify additional duties and requirements for Web site operators with knowledge of data collection from children located in the state, including requiring the labeling of advertisements. The bill provides for both state enforcement of violations and private rights of action. HB-316 is pending before the House Economic Matters Committee, which has already held a hearing on the bill. Consideration of this legislation and its companion bill in the Maryland Senate takes place in the context of a strong focus on privacy by Maryland Attorney General Doug Gansler, who recently established a task force on privacy and also testified at the committee's hearing on HB-316.

In Montana, legislation entitled the "Montana Personal Data Protection Act of 2013" has been introduced. The bill would require consumers to provide explicit consent prior to the collection of their personal information, and would place several other restrictions on the collection, use, and storage of personal information. HB 400 was referred to the Montana House Business and Labor Committee, where it was the subject of a hearing on February 12, 2013. A similar bill was introduced in the previous legislative session but did not pass through the committee process.

About Venable

An *American Lawyer* 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

VENABLE'S INTERSECTION

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