VENABLE LLP

the download

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

June 2012

Winner of *Chambers USA* "Award Excellence" for the top privacy practice in the United States

……

Winner of *Chambers USA* "Award of Excellence" for the top advertising practice in United States

……

Two of the "Top 25 Privacy Experts" by *Computerworld*

……

"Winning particular plaudits" for "sophisticated enforcement work" – *Chambers and Partners*

……

Recognized by *Chambers Global* and the *Legal 500* as a top law firm for its outstanding data protection and privacy practice

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

1.888.VENABLE
www.Venable.com

In this Issue:

……

Industry Developments

- DAA Raises Concern About Default "Do Not Track" Browser Setting

Heard on the Hill

- Congressional Committees Hold Hearings on White House and FTC Privacy Frameworks
- House Judiciary Subcommittee Holds Hearing on Geolocation Privacy

Around the Agencies

- FTC Raises Data Security and Children's Privacy Claims in RockYou Settlement
- FTC Hosts Workshop on Mobile Payments
- FTC Explores Dotcom Disclosures
- FCC Requests Comments on Privacy and Security of Information on Mobile Devices
- FCC Releases Report on Location-Based Services

In the Courts

- California Court Decision Provides Guidance to Email Marketers on Proxy Domains

International

- UK Begins Enforcing Cookie Consent Provisions

Industry Developments

DAA Raises Concern About Default "Do Not Track" Browser Setting

On May 31, 2012, the Digital Advertising Alliance ("DAA"), a coalition of the nation's leading media and marketing trade associations and companies, raised concern about Microsoft's decision to embed Do Not Track ("DNT") functionality as a default setting in version 10 of its Internet Explorer (IE) browser. The DAA made the following statement:

> Over the last three and a half years, the DAA has worked with a broad set of stakeholders with significant input from businesses, consumers, and policy makers to develop a program governing the responsible collection and use of web viewing data. The DAA has championed a balanced approach that accommodates both consumers' privacy expectations and the ability of online products and services providers to provide a sustainable business model for these services while enabling them to continue innovating with new services. Consumers enjoy the diverse range of Web sites and services they get at no charge thanks to relevant advertising. Recognizing that DAA members must also provide consumers with appropriate transparency and clear choices, it

has spearheaded the self-regulatory process, in which Microsoft has been an active participant since its inception.

The DAA's work culminated in an event in February at the White House where the Chairman of the Federal Trade Commission, the Secretary of Commerce and members of the White House publicly praised the DAA's cross-industry initiative. At that event, the DAA committed to honor browser settings that enable the use of data to continue to benefit consumers and the economy, while at the same time providing consumers with the ability to make their own choice about the collection and use of data about them. The overwhelming majority of the advertising ecosystem follows the DAA program today, and consumers have responded favorably to the increased transparency it has enabled. The Internet economy is fueling Internet growth and innovation while providing ongoing benefits to consumers.

"Advertising has always been about connecting consumers to products and services that are likely of interest to them," said DAA General Counsel Stu Ingis. "While new Web technologies deliver more relevant advertising to consumers, comprehensive industry self-regulation is also providing consumers with meaningful choices about the collection of their data. The Administration and FTC have praised these efforts. Today's technology announcement, however, threatens to undermine that balance, limiting the availability and diversity of Internet content and services for consumers."

Microsoft's technology announcement appears to include requirements that are inconsistent with the consensus achieved over the appropriate standards for collecting and using web viewing data (and which today are enforced by strong self-regulation). The DAA is very concerned that this unilateral decision by one browser maker - made without consultation within the self-regulatory process -may ultimately narrow the scope of consumer choices, undercut thriving business models, and reduce the availability and diversity of the Internet products and services that millions of American consumers currently enjoy at no charge. The resulting marketplace confusion will not benefit consumers, and will profoundly impact the broad array of advertising-supported services they currently enjoy.

Heard on the Hill

Congressional Committees Hold Hearings on White House and FTC Privacy Frameworks

Committees with jurisdiction over privacy issues in the Senate and House of Representatives have held hearings focused on the privacy frameworks released earlier this year by the White House and Federal Trade Commission ("FTC").

The first hearing to examine the frameworks was convened on March 29, 2012 in the Commerce, Manufacturing and Trade ("CMT") Subcommittee of the House Energy and Commerce Committee. The hearing was entitled "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?" Representative Mary Bono Mack (R-CA) chaired the hearing, which was attended by numerous Republican and Democratic subcommittee members.

The hearing's first panel was composed of two government witnesses: Jon Leibowitz, FTC Chairman, and Lawrence Strickling, Assistant Secretary for Communication and Information at the Commerce Department, who discussed the reports issued by their respective agencies. Both witnesses spoke in favor of "baseline" privacy legislation that would set national regulations applying across industries. While some members – including Subcommittee Ranking Member G.K. Butterfield (D-NC) – voiced support for such legislation, other members – including CMT Subcommittee Chairman Bono Mack and full Committee Chairman Fred Upton (R-MI) – expressed concerns that new legislation may be unnecessary and could negatively affect the Internet.

The second panel at the CMT Subcommittee hearing featured industry and nonprofit representatives, who provided a range of perspectives on the privacy frameworks. Several witnesses discussed the merits of industry self-regulation.

The Senate Commerce Committee held its own hearing on May 9, 2012, entitled "The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission." Committee Chairman Jay Rockefeller (D-WV) chaired the hearing, which was also attended by Senator Pat Toomey (R-PA) and several Democratic committee members. In his opening statement, Chairman Rockefeller stated that he does not believe industry self-regulation is sufficient to address consumers' privacy concerns. Senator John Kerry (D-MA) also delivered an opening statement, in which he suggested that his privacy legislation (co-authored with Senator John McCain (R-AZ)) could be a starting point for a "baseline" national privacy bill.

The sole panel at the Senate Commerce hearing featured FTC Chairman Jon Leibowitz; FTC Commissioner Maureen Ohlhausen; and Cameron Kerry, General Counsel of the Commerce Department. Similar to the CMT Subcommittee hearing, both Chairman Leibowitz and Mr. Kerry supported "baseline" privacy legislation. Commissioner Ohlhausen stated that she needed more time to review the proposals because she joined the FTC after the release of the framework.

House Judiciary Subcommittee Holds Hearing on Geolocation Privacy

On May 17, 2012, the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security considered the issues of geolocational privacy and surveillance at a hearing on Representative Jason Chaffetz's (R-UT) H.R. 2168, the Geolocational Privacy and Surveillance Act. A companion bill, S. 1212, has also been introduced in the Senate by Senator Ron Wyden, but the Senate has yet to hold a hearing on that bill.

H.R. 2168 would provide a framework for commercial and government entities as well as private citizens on how they may access and use geolocation information. The bill would prohibit them from collecting, using, or sharing the information except for in certain circumstances, such as when they have obtained consent. The bill, which includes a private right of action, would impose fines and imprisonment for violations.

Subcommittee Chair Jim Sensenbrenner (R-WI) chaired the hearing, which was attended by members of both sides of the aisle. Representative Chaffetz, who is a member of the Subcommittee, explained that the purpose of his bill was to establish a process for guaranteeing privacy protections and to help ensure that the government had a clear reason for obtaining geolocation information regardless of its legal authority to do so. Subcommittee Ranking Member Bobby Scott (D-VA) commended the bill as a good starting point for addressing technological advances not yet addressed by current laws.

Witnesses from the Computer & Communications Industry Association and the American Civil Liberties Union also expressed support for the bill, noting that the bill would extend Fourth Amendment protections to reflect the digital age. On the other end of the spectrum, representatives of the Federal Law Enforcement Officers Association and National District Attorneys Association voiced concern that the bill could hamper law enforcement efforts.

Around the Agencies

FTC Raises Data Security and Children's Privacy Claims in RockYou Settlement

The Federal Trade Commission ("FTC") continued its scrutiny of data security and children's privacy practices in a proposed settlement with RockYou, Inc., a social game site operator. The FTC alleged that RockYou had failed to live up to the security assurances made in its privacy policy, exposing 32 million email

addresses and passwords to hackers, and that RockYou also collected information about children without parental consent in violation of the Children's Online Privacy Protection Rule ("COPPA Rule"). To settle these charges, RockYou agreed to pay a $250,000 civil penalty and to implement a comprehensive data security program.

RockYou operates a website that allows consumers to play games and use other applications, and collects consumers' email account addresses and passwords for some of those applications. The FTC's complaint states that RockYou promised in its privacy policy that it would implement reasonable and appropriate measures to protect against unauthorized access to the personal information it obtained from consumers. The FTC argued that, despite these promises, RockYou failed to secure consumers' data. In particular, the FTC alleged that RockYou stored consumer data in plain text, failed to segment its servers, and did not protect its services from common types of hacking attacks. The complaint states that as a result of these practices, hackers obtained access to approximately 32 million RockYou accounts, including email addresses and RockYou account passwords.

The FTC also charged RockYou with failing to abide by a second part of its privacy policy—that the company would not collect information from children and, if it learned about information collected from a child, it would delete the data. RockYou allegedly requested birth years from its users and collected data from users who reported themselves to be children under 13. The FTC charged that the failures to abide by the privacy policy constituted a deceptive act under the FTC Act.

Regarding the COPPA Rule, the FTC charged RockYou with violating the Rule when it obtained 179,000 children's email addresses and associated passwords, and allowed children to post information online without parental notice and consent. The FTC further alleged that RockYou failed to adequately secure children's personal information as required by the COPPA Rule.

To settle the FTC's charges, RockYou agreed to pay a $250,000 civil penalty and agreed to injunctive provisions barring deceptive claims regarding privacy and data security. Similar to other FTC cases involving data security, RockYou also agreed to implement a comprehensive data security program and submit to security audits by independent third-party auditors every other year for 20 years.

FTC Hosts Workshop on Mobile Payments

On April 26, 2012, the Federal Trade Commission ("FTC") hosted a workshop, entitled "Paper, Plastic … or Mobile? An FTC Workshop on Mobile Payments," to examine the use of mobile payments in the marketplace and how emerging technologies affect consumers. The workshop consisted of presentations and panels with representatives from business, law, finance, and consumer advocacy organizations. David Vladeck, Director of the Bureau of Consumer Protection at the FTC, delivered opening remarks stating that the purpose of the workshop was to "understand and identify [mobile payment] issues before they become widespread," and to "build best practices for adoption" by the mobile payment industry.

Mobile payment systems allow consumers to make purchases using their mobile devices, as opposed to using cash or plastic debit or credit cards. The industry is growing at a dizzying pace—mobile payments in the U.S. totaled $240 billion in 2011 and are expected to rise to $670 billion by 2015.

As was discussed at length during the workshop, mobile payment technology is in a state of innovation and flux. Companies have already brought to market systems that allow consumers to pay using their existing cards stored in a virtual "wallet" on their phone, to pay by adding the charge to their mobile carrier bill, or to pay using virtual "cash" pre-purchased from the mobile payment provider and deducted from a stored account. As the panelists and presenters pointed out, the transactional stage has its own set of technological options. Depending on the

mobile payment system chosen, consumers can pay by placing their phone next to a receptor (known as Near Field Communication, or "NFC"), by sending a text message to the merchant, or by scanning a bar code that appears on the screen of their mobile device.

On the other side of the counter, merchants are using mobile payment systems in a variety of ways. Electronic recordation of their transactions allows for easier implementation of loyalty programs, while location-based mobile services give merchants the ability to target discounts to potential customers in proximity to their store. With streamlined data collection across the transactional and social networking platforms, businesses gain access to high-level data analytics about their customers.

The workshop discussed the many benefits consumers will reap—and already are reaping—from mobile payments. Savings, in the form of synchronized discounts and loyalty programs, as well as the digitalization of receipts, are only a few that were mentioned at the workshop.

Panelists discussed the difficulties that consumers could face with mobile payment systems as FTC moderators steered the discussion to three specific areas: (1) privacy, (2) data security, (3) payment dispute resolution. Panelists, presenters, and moderators underscored the importance of developing a legal and regulatory framework that would encourage innovation in the industry while ensuring consumers remain protected in these areas.

In a separate presentation not scheduled on the official program, staff from the FTC Mobile Technology Unit revealed that they had conducted a study of 19 mobile payment providers to "observe what disclosures are made to consumers regarding these companies' dispute resolution policies." While FTC staff emphasized that the Commission was not drawing any conclusions from the study, the slides emphasized consumers' total liability for fraudulent or unauthorized purchases, as well as the sharing of consumers' personal information with third parties.

FTC Explores Dotcom Disclosures

On May 30, 2012, the Federal Trade Commission ("FTC") convened a day-long public workshop to discuss updating its "Dot Com Disclosures" guidance on presenting online advertising disclosures. The FTC is considering whether it should overhaul this guidance, which dates to 2000, to address current trends such as social media and mobile advertising. The workshop also included a panel devoted to mobile privacy disclosures. Commissioner Maureen Ohlhausen kicked off the event by explaining that the FTC does not intend to expand its Section 5 authority, but wants to shed light on how existing legal principles should apply to new technologies.

Mary Engle, the head of the FTC's Advertising Practices Division, told participants that new technology platforms should adapt to existing legal principles, not the other way around. But discussion at the workshop highlighted the challenges of reaching this goal in a way that is technically feasible and does not detract from users' experiences.

One obvious challenge is the space limitations of mobile devices and certain social media platforms, which give advertisers less room to provide disclosures. Numerous panelists opined that, despite these limitations, disclosures should still be placed near advertising claims. A few panelists suggested that ad campaigns that require extensive disclosures should not use platforms where such disclosures are not feasible.

To cope with space limits, some panelists endorsed the concept of standardized icons, labels, and other shorthand signals that give consumers access to disclosures. The mobile privacy disclosures panel featured several presentations by programs that are developing such offerings. Other panelists, however,

expressed concern that these signals may not be understood by consumers, or saw a need for more consumer education to promote understanding. Numerous panelists also advocated for the FTC to retain flexibility for companies and for social media users.

Another challenge identified during the workshop is the fact that digital content can easily be relocated in cyberspace, potentially losing or altering disclosures in the process. For example, the panel on social media disclosures discussed the challenge of ensuring that disclosures travel with promotional messages when blog content is repurposed or syndicated. Disclosures presented in a sidebar will be lost if the blog is viewed in an RSS feed. Translating webpages from desktop to mobile environment can also affect how consumers see disclosures.

The FTC now faces the task of distilling these and other workshop discussions, as well as comments solicited last year, into concrete guidance for the business community. Ms. Engle, the Advertising Practices chief, pledged that the FTC will seek to turn these "shades of gray" into "as many … blacks and whites as we can." To that end, the FTC will be accepting comments until July 11 and expects to issue its new guidance as early as the fall.

FCC Requests Comments on Privacy and Security of Information on Mobile Devices

On May 25, 2012, the Federal Communications Commission ("FCC") announced that it is seeking comments on the privacy and security of information stored on mobile communications devices. Comments will be due 30 days after the notice is published in the Federal Register, and reply comments are due 45 days after the notice is published.

The FCC has long focused on protecting the privacy of customer information under section 222 of the Communications Act of 1934, as amended. Five years ago, the FCC sought comments on how carriers protect customer proprietary network information ("CPNI"). In the interim, many technological advances have been made and the FCC would like to update the administrative record. Commenters are encouraged to provide feedback on how wireless providers' treatment of customer information stored on mobile devices has since evolved. Additionally, among other topics, the public is encouraged to comment on the role of privacy by design, the role of consumers in protecting their data, and wireless providers' obligations to protect customer information.

FCC Releases Report on Location-Based Services

The Wireless Telecommunications Bureau of the Federal Communications Commission ("FCC") released its anticipated report on location-based services, entitled Location-Based Services: An Overview of Opportunities and Other Considerations ("Report").[1] The Report follows the FCC's examination of location-based services ("LBS") at last year's FCC workshop on LBS and privacy issues they may raise.

The Report highlights the many ways in which innovative LBS are providing value to consumers, but also underscores the challenges of ensuring that people enjoy such services without placing their confidential information at risk. The FCC reiterates its goals with respect to privacy, including: (1) ensuring personal information is not misused; (2) requiring transparent information practices; and (3) providing consumer control and choice. The Report notes that some members of industry have stepped up to meet these goals, but industry responses vary.

The FCC provides its perspective on key privacy issues associated with LBS,

[1] Federal Communications Commission, Wireless Telecommunications Bureau, "Location-Based Services: An Overview of Opportunities and Other Considerations," (May 2012), available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0530/DOC-314283A1.pdf (hereinafter, "FCC Report").

stating that transparent notice is "one of the most important aspects" of commercial data privacy practices, and that such notice should be clear, concise, and accurate. At the same time, the FCC recognizes the challenges of providing notice with regard to LBS, due in part to small screen sizes. The FCC takes the view that companies may derive competitive benefits from offering transparency to consumers.

The FCC acknowledges the challenge of deciding whether choice should be "opt-out" or "opt-in," but identifies a "developing consensus in the LBS industry that opt-in is appropriate" for location data.[2] Another challenge is to ensure that choice does not interfere with the user experience. The FCC suggests that uniform language for privacy choices could address this challenge. Finally, the Report identifies children's use of mobile technology as a challenge for LBS providers.

The FCC states that third party access to data also creates challenges for LBS, such as the existence of many industry players in the LBS environment, including app developers who may not have experience or resources to address privacy. The FCC reports that companies are "taking steps" to ensure that associated third parties are attentive to privacy but acknowledges that companies have a limited ability to control third party practices.[3]

Finally, the FCC states that because location data is perceived as sensitive, "heightened security requirements reasonably can be expected" of LBS providers.[4]

In the Courts

California Court Decision Provides Guidance to Email Marketers on Proxy Domains

The recent California appellate decision in Balsam v. Trancos, Inc. provides a caution to email marketers who use proxy services to send commercial emails on their behalf. The defendant, Trancos, is an email marketing company who sends marketing emails on behalf of its clients. As part of this service, Trancos generates the domain name used in the "from" line of the email. For the emails in question, it generated "fanciful" names for the domains used, which were legitimately registered to Trancos through a proxy server. The physical address provided in the body of the email also belonged to Trancos.

Despite these facts, the California appellate court determined that these emails violated California's state Anti-Spam law. Similar to the federal CAN-SPAM Act, California's Anti-Spam law prohibits commercial email which "contains or is accompanied by falsified, misrepresented, or forged header information." Earlier precedent in California had held that a commercial emailer did not misrepresent its identity when it used multiple, randomly-named, but traceable domain names in order to avoid spam filters. The key difference in Trancos, in the court's reasoning, was that the proxy domain names used here were not "traceable." Any consumer who attempted a WHOIS search of the domain names in the commercial emails would not be led back to Trancos, but would instead be directed to the proxy service with whom the domain names were registered. This lack of traceability, which would potentially prevent a consumer from determining the sender's identity or whether the sender was acting in good faith, drove the court's ruling.

The court also ruled that on this issue, the federal CAN-SPAM Act does not preempt California's statute. The California statute would apply to any entity that either sends commercial emails from California or to California consumers.

---

[2] Id.
[3] FCC Report, p. 30.
[4] Id.

International

UK Begins Enforcing Cookie Consent Provisions

In 2009, the European Council approved a Directive that changed then-current law by requiring consent for the use of cookies in Europe. Specifically, the Directive included a new requirement that a visitor must "give[] his or her consent," after having been provided with "clear and comprehensive information" about the purposes of cookies, before such cookies may be used (the "cookie consent rule"). Each European member state was required to adopt a law implementing the Directive by May 25, 2011.

At present time, a number of European member states have passed laws implementing the Directive including France, Ireland, the United Kingdon ("UK"), and Spain. Many European member states, however, including Germany and Italy, have failed to enact a law. The collective effect of the mixed record on compliance across the EU is that some countries are, in theory, already enforcing the requirements while others have not taken the necessary affirmative steps to do so.

The UK

The UK became the first to announce its plans for implementing the Directive. The press release accompanying release of guidance to the business community noted a one-year grace period on enforcement of the consent provisions, which pushed the enforcement deadline to May 26, 2012.

Guidance published in the UK in December 2011 provides implementation advice to the business community. This "Guidance on the rules on use of cookies and similar technologies" (the "Guidance"), indicates that under the UK's implementing regulations, prior consent to cookies generally is required.[5] The Guidance notes that the scope of the UK regulations includes cookies as well as similar technologies, including Local Shared Objects/flash cookies, web beacons, or bugs.[6]

The UK issued additional guidance to coincide with the commencement of enforcement ("May Guidance").[7] While the May Guidance is largely consistent with previous recommendations, it now reflects that provided that "implied consent" is a "freely given, specific and informed indication of the individual's wishes," it would be sufficient to meet the terms of the law. The May Guidance encourages businesses to look at the context of the transaction with the consumer in order to determine whether implied consent would be sufficient. Important factors to consider include: (1) the nature of the intended audience of the site; (2) the way in which users expect to receive information on the site; and (3) making sure the language is appropriate for the audience. Specifically addressing web analytics, the May Guidance recognizes that "gaining explicit opt-in consent for analytics cookies is difficult and that implied consent might be the most practical and user-friendly option," but they urge sites to give more and better information about cookies and the facility for users to make choices about cookies.

Both guidance documents inform businesses that they are obligated to do three things: (1) inform web users of cookies; (2) explain what the cookies are doing; and (3) obtain users' consent to store a cookie on their device. Consent must be obtained prior to setting the cookie; for websites that set cookies as soon as a

[5] The Guidance is available from the UK's Information Commissioner's Office webpage, here: http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx.
[6] Guidance, p. 4.
[7] The May Guidance is available here: http://www.ico.gov.uk/news/blog/2012/updated-ico-advice-guidance-e-privacy-directive-eu-cookie-law.aspx.

visitor comes to a website, the website should "wherever possible" delay setting the cookie "until users have had the opportunity to understand what cookies are being used and make their choice."[8]

The Guidance also provides "practical advice," for companies seeking to start the compliance process, summarized as follows:

- "Audit" cookies currently in use—analyze which cookies are strictly necessary and clean up web pages with unnecessary cookies;
- Assess how intrusive use of cookies is—for more intrusive cookies greater "priority" must be paid to meaningful consent;
- Determine a solution for obtaining consent.[9]

The Guidance suggests that a variety of notice and consent options may be sufficient under the UK regulations.

****

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.

[8] Guidance, p. 5.
[9] Guidance, p. 12.