Privacy for the Neophyte:
Introduction to Global Privacy Issues

Session Materials

Tuesday, October 2, 2012

Orlando, Florida

Table of Contents

The presenters would like to thank Pillsbury, Winthrop, Shaw, Pittman LLP and Venable LLP for making much of this information available for this presentation.

For further information please contact

Pillsbury, Winthrop, Shaw, Pittman LLP - Catherine Meyer - catherine.meyer@pillsburylaw.com

Venable LLP – Sona Pancholy - SNPancholy@Venable.com

Online Privacy, Data Protection and Information Security Resources

Trade Organizations (requires registration and a subscription fee)

- International Association of Privacy Professionals – www.privacyassociation.org
- Corporate Executive Board - Compliance and Ethics Leadership Council - https://www.celc.executiveboard.com
- Association of Corporate Counsel

Data Transfer Frameworks

- Safe Harbor - http://export.gov/safeharbor
- Binding Corporate Rules - http://ec.europa.eu/justice/policies/privacy/binding_rules
- APEC Privacy Framework - http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

EU Data Protection Directives and Proposed Regulation

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
- Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), 2002 O.J. (L 108) 7, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0007:0007:EN:PDF
- Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), 2002 O.J. (L 108) 21, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0021:0021:EN:PDF
- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), 2002 O.J. (L 108) 33, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0033:EN:PDF
- Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), 2002 O.J. (L 108) 51, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0051:0051:EN:PDF
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002 O.J. (L 201) 37, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

- Proposed EU Data Protection Regulation - http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Technical Frameworks

- Generally Accepted Privacy Practices – AICPA and CICA Standard - http://www.cica.ca/service-and-products/privacy/gen-accepted-privacy-principles/index.aspx
- ISO 27001/27002 - Information Technology -- Security Techniques -- Information Security Management Systems - http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103
- ISO 22307 – Financial Services – Privacy Impact Assessment - http://www.iso.org/iso/catalogue_detail?csnumber=40897
- Shared Assessments – Third Party Validation Standard - http://www.sharedassessments.org
- COBIT – Framework for IT Governance and Control - http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
- Service Organization Controls (old SAS70 attestation) - http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx

Other Online Resources or Services

- Morrison Foerster – Privacy Library - http://www.mofo.com/privacylibrary/

Privacy Audit Checklist

This Privacy Audit Checklist is intended to assist privacy professionals to establish and maintain a privacy program. All privacy programs are unique and require an assessment of each organization's practices, needs and capabilities.

Establish Context for Your Assessment:

- Assess the laws and regulatory climate affecting your organization.
- Consider likelihood and consequences of negative press in the event of a breach. (i.e., type of info collected type of business, demographics of clientele, privacy practices and current media hot-button issues).
- Account for industry/trade organization affiliations: are there any self-regulatory initiatives with which your policies and practices must correspond. (i.e., Direct Marketing Association, Mobile Marketing Association or BBB).

Develop a Classification System to Classify Information into General Categories:

- Non-sensitive/Sensitive/Highly-sensitive
- Personally identifiable/non-personally identifiable
- Information subject to specific statutory/regulatory requirements
- Medical Information Financial Information
- Information collected from children under the age of 13
- Social Security Numbers

Conduct a Privacy Risk Assessment:

- It is essential to obtain the senior management buy-in, which will be critical in successful advancement of any initiative.
- Establish an internal privacy task force or working group, including members of legal, IT, government relations, marketing, communications and other stakeholders.
- Review company procedures regarding collection, maintenance, security, use, and disclosure to third parties.

As a Part of the Assessment Determine What Information is Collected and How The Information is Collected and Stored:

- Catalog the types of information collected by your organization and the purpose for its collection.
- How is the information collected?
- Where is the information being stored?
- Are there different storage strategies in place?
- How is information cross-referenced?
- How is each class of data being used?
- How long is each class of information kept?

- Is your organization in compliance with all relevant statutory/regulatory requirements for storage of specific classes of information?
- When is information belonging to each class destroyed?
- Who is responsible for its destruction and how is it destroyed?
- How is the accuracy of collected information guaranteed?
- Are there access mechanisms in place, allowing the subject to alter/update inaccurate or obsolete information?
- To whom, in what manner, and under what circumstances may information be disclosed?

Map Your Organization's Data Flows:

- What information is moving intra-departmentally or intra-personally within your organization?
- What information is moving from your organization to third parties?
- What information is your organization receiving from third parties?
- What relevant information is moving across state/national boundaries?

The answers to these questions will determine your level of privacy-related exposure, and should inform your organizational privacy strategy.

Partners and Third Parties:

- Assess your organization's relationships including business partners, third party vendors, strategic partners, etc. which might involve the transfer of personal information.
- List the names of relevant organizations, and clearly express the details of the relationships as they affect data flows.
- Do your contracts address required data security?
- Does your web site/organization share, transfer, or release any information to third parties?
- With whom, if anyone, is the information being shared, transferred, or released?
- What specific information, if any, is being shared, transferred, or released?

Review the Organization's Information Security:

- Encryption
  - Is sensitive information encrypted?

- Identification
  - Is access to data granted to third parties outside your organization? If so, what steps have been taken to limit unauthorized access?
  - Specify whether certain groups or individuals are granted general access to data within your organization.

    - Is access to personally identifiable and/or sensitive data accountable to specific individuals to maintain control over access and preserve accountability for misuse?

- Authentication
    - How do you verify the identity of the parties accessing the data?
    - Describe the password standards (steps taken to maintain password security).
    - What mechanisms are in place to ensure security/confidentiality of customer/user information during transmission over public communication lines and within your organization?

Assessing Collection Practices:

When tightening or creating an organization's privacy practices, a good first step is to question the business necessity of all data being collected and to collect only that data which is of compelling business importance. In addition to the information above, the checklist below may assist in determining what data is being collected:

CONTACT INFORMATION

. . Name
. . E-mail address
. . Mailing Address
. . Phone Number
. . Facsimile Number
. . Other (Specify)_____

FINANCIAL/BILLING INFORMATION

. . Name of banking institution
. . Credit Card number
. . Salary/Income
. . Account Number
. . Routing number
. . Account balance
. . Other (Specify)_____

UNIQUE IDENTIFIERS

. . Social Security Identifier
. . Driver’s License Number
. . Proprietary global unique identifier (GUID)
. . Other (Specify)_____

DEMOGRAPHIC INFORMATION

. . Age
. . Gender
. . Ethnicity
. . Marital Status
. . Religion
. . Other (Specify)_____

MEDICAL INFORMATION

. . Medical History
. . Health Status/Present Conditions
. . Health Insurance Provider
. . Other (Specify)_____

EMPLOYMENT INFORMATION

. . Employment Status
. . Employer
. . Title
. . Business Contact info.
. . Other (Specify)_____

EDUCATION INFORMATION

. . School(s) attended
. . Degrees conferred
. . Dates of attendance
. . Transcript/Grade information
. . Other (Specify)_____

LEGAL INFORMATION

. . Criminal Record
. . Other (Specify)_____

FAMILIAL INFORMATION

. . Number of Children
. . Number of Siblings
. . Information regarding spouse/partner
. . Mother's maiden name
. . Information regarding parents
. . Years at current address
. . Other (Specify)_____

OTHER INFORMATION

. . Hobbies
. . Interests
. . Dialogue/Interaction (chat rooms, e-mail, bulletin board postings, etc.)
. . Other (Specify)_____

BY WHAT MEANS IS THIS INFORMATION BEING COLLECTED

. . Registration Forms
. . Order Forms
. . News Groups
. . Feedback Forms
. . Contact Us or Request Forms
. . Forums or Surveys
. . Electronic mail
. . Chat Rooms
. . Bulletin Boards
. . Other (Specify)_____

DOCUMENT COLLECTION PROCESS CHECKLIST *

Prepared By

Dawn L. Haghighi

*This document only provides general guidance and is not intended to be legal advice. Each investigation should be conducted based on the circumstances of that investigation.

Dhaghighi@aol.com
Dawn L. Haghighi

I. Preliminary Considerations

A. Determine the scope of the document collection.
B. Identify privacy issues.
C. Identify applicable laws that apply.
D. Identify, review and secure applicable Company Documentation Retention Policy.
E. Secure a confidential location to secure documents.
F. Assemble a Document Collection Team.
G. Conduct Document Collection Process.
H. Issue Hold Notices.

II. Privacy Issues

A. Identify any applicable privacy issues and potential privacy rights.
B. If needed, secure any consent to review documents or secure acknowledgments executed by employees regarding "No Expectation of Privacy."

III. Assemble a Document Collection Team

A. Attorney-Client Privilege: To preserve attorney-client privilege related to the Document Collection Process, the document collection should be directed by legal counsel.
    1. Document Collection notes may be discoverable and/or utilized in a court proceeding.
    2. To maintain the attorney-client privilege, the Document Collection Process summary should contain the following language: "CONFIDENTIAL: Provided to (in-house attorney or outside counsel) for the purpose of obtaining legal advice, prepared at the direction of legal counsel and in anticipation of litigation."
    3. Other possible privileges:
        a. Work Product Doctrine.
        b. Self Evaluative Privilege.
B. Outside Counsel vs. In-house Counsel: Evaluate the need to retain and use outside counsel as opposed to using in-house counsel to coordinate the Document Collection Process.
C. Transparency: Take steps to ensure the document collection team-members are independent and the collection process appears transparent.
D. Subject Matter Expertise: Identify document collection team-members with subject matter expertise.
    1. For example, determine whether an IT expert or other subject matter expert is necessary to assist with the document collection.

*This document only provides general guidance and is not intended to be legal advice. Each investigation should be conducted based on the circumstances of that investigation.

Dhaghighi@aol.com
Dawn L. Haghighi

2. Legal counsel, preferably outside counsel, should retain and direct the work of outside consultants.

IV. Document Collection Process and Preservation

A. Document Collection Process
   1. Identify and secure potential records.
      a) Paper
      b) Electronic
   2. Identify and notify the Record Custodian(s).
   3. Issue Hold Notices to all Custodians and confirm that Custodian understands that it is his/her responsibility to inform all individuals with access not to alter, edit or add to documents.
   4. Identify place to secure records during the Hold Notice Period.
   5. Prepare and create a memorandum describing the Document Collection Process.
      a) Description of record
      b) Time frame
      c) Format
   6. Prepare a written record of the document collection process.

V. Collection Process Interview

A. General Considerations
   1. Identify pertinent individuals or parties related to Document Collection Process.
      a) Employees
      b) Contractors
      c) Third Party Vendors
      d) Storage Companies
   2. Identify pertinent documents related to the individuals or parties described above.
      a) Contracts
      b) Purchase Orders
      c) Invoices
      d) Others
   3. Depending on the magnitude of the document collection process and significance of event at issue, provide the following disclosures at outset of all Document Collection Interviews.
      a) Advise employees that the Company has a responsibility to collect and preserve all documents.
      b) Advise employees that they must provide accurate and truthful information.

Dhaghighi@aol.com
Dawn L. Haghighi

c) Where appropriate, explain that actions that are viewed as compromising the collection process may result in disciplinary legal action by the Company and/or by law.
d) Where appropriate, review the Company's Anti-Retaliation Policy. In appropriate circumstances, prepare an Acknowledgment Form for all investigation participants to execute regarding review of Company policies.
e) Be prepared for responses to tough questions:
    a. May I have legal counsel present?
    b. May I take notes?
    c. May I tape record the interview?
    d. Am I obligated to answer the questions?
    e. Will I be fired?
    f. May I have a union representative present?

B. Conducting Collection Process Interviews
1. Maintain the Confidentiality of the Document Collection Process. See section III above.
2. Issues to consider for the interview
    a) In general, questions such as **who, what, why, when, where** and **how** will assist in eliciting the most valuable information. The following can be used as a reference when conducting the interview:
        a. Background information on all participants interviewed in Collection Process.
            i. Name of the person interviewed.
            ii. Dates of employment.
            iii. Identify the employee's title and name of department.
            iv. Identify the name of the employee's manager.
            v. Where appropriate, identify all positions held by the employee and department names or office location.
            vi. Obtain contact information, i.e., telephone number, email address, office telephone number
        b. Information regarding documents
            i. Do you save files to the Company's network?
            ii. Do you create backups of your electronic records or files?
                1. Floppy disks
                2. CDs/ DVDs
                3. Any other locations

*This document only provides general guidance and is not intended to be legal advice. Each investigation should be conducted based on the circumstances of that investigation.

Dhaghighi@aol.com
Dawn L. Haghighi

iii. Can you think of any other location where documents may be found in response to the Hold Notice?
iv. Do you know of anyone else who may have documents that may be in response to the Hold Notice?

c. Distinguish between first hand knowledge and speculation of facts.

3. Documenting the Document Collection Process
   a) Document the start and end time of each search.
   b) Identify where the search was conducted.
   c) Identify what was searched and found.
   d) Identify where it was found.
      a. Electronic documents.
         i. Email
         ii. Inbox
         iii. Calendar
         iv. Sent Items
         v. Personal Folders
         vi. Journal
         vii. Archive Folders
         viii. Public Folders
         ix. Blackberry
         x. Other PDAs (Palm Pilot, etc.)
         xi. MS Office
         xii. Word Files
         xiii. Excel Spreadsheets
         xiv. PowerPoint Presentations
         xv. Hard Drive
         xvi. Other Applications
      b. Paper documents.
         i. Desk File Drawers
         ii. File Cabinets
         iii. Department Files
         iv. Site Files
         v. Other Shared Files
         vi. Stored Files (e.g., LA Records)
   e) Complete Data Collection Checklist.

C. Concluding the Document Collection Process
   1. Provide contact information for person to notify if there are new records identified after the interview.

*This document only provides general guidance and is not intended to be legal advice. Each investigation should be conducted based on the circumstances of that investigation.

Dhaghighi@aol.com
Dawn L. Haghighi

2. Notify participant of the Hold Notice and provide copy to participant.
3. Where appropriate, have participant acknowledge receipt of Hold Notice.
4. Notify participant to advise of any new documents retained.
5. Where applicable, inform participant of confidential nature of the collection process.

VI. Finalizing the Collection Process

A. Hold Notice

1. Distribution of Hold Notice
    a) Issue Hold Notice.
    b) Document who received the Hold Notice.
    c) Confirm that Hold Notice recipient acknowledged receipt and has taken action.
2. Monitoring Hold Notice
    a) If appropriate, re-issue Hold Notice on a periodic basis.
    b) Obtain confirmation of acknowledgement and receipt of Hold Notice.
    c) Periodic review and communication.
3. Confirm compliance with Hold Notice.

Dhaghighi@aol.com
Dawn L. Haghighi

DATA COLLECTION CHECKLIST

Data Collection Checklist									
Paper Data	**Collection Date**	**Custodian**	**Custodian Extension**	**Custodian Email**	**Location**	**Type**	**Volume**	**Hold Notice Issued**	**Notes**
Paper Records									
General Office									
Employee Office									
File Cabinets									
File Room									
Desk Drawers									
Closets									
Company Warehouse									
Offsite Storage									
Recycle Bins									
Third Party Vendor									
Independent Contractors									
Licensors									
Other									
Electronic Records									
Machines									
POS Machines									
Fax Machines									
Copy Machines									
Voice Mail System									
Individual Employee Telephone									
Telephone Logs									
Third Party Vendors									
Vendor Computer Programs									
Videos									
Security Camera Tapes									
Security Camera Backup Tapes									
Purchasing Systems									
Oracle									
Markview									
Stockwatch									
Other									

DATA COLLECTION CHECKLIST

Paper Data	Collection Date	Custodian	Custodian Extension	Custodian Email	Location	Type	Volume	Hold Notice Issued	Notes
Shared Servers/ Network									
All network nodes									
Computers									
Desktop(s)									
Laptop(s)									
Notebook(s)									
Home Computer(s)									
Obsolete Computer Equipment									
Handheld devices and Personal Digital Assistant (PDA)									
TREO									
Blackberry									
Cellular Telephone									
Ipods									
MP3 Players									
iPhone									
Palm									
Wing Phone									
Memory Devices									
Thumb Drives									
Memory Sticks									
Flash Drives									
Digital camera Memory cards									
Phone Memory cards									
Memory cards from other devices									
Printer memory caches									
Copier/ Scanner memory caches									
External Storage Devices									
DVDs									
CDs									
Floppy drives									
Video Tapes									
Audio Tapes									
Other removable media cards									

DATA COLLECTION CHECKLIST

Paper Data	Collection Date	Custodian	Custodian Extension	Custodian Email	Location	Type	Volume	Hold Notice Issued	Notes
Detached/ external hard drives									
Zip drives									
Archive or Backup Media									
Backup Tapes									
File shares									
Email devices									
Hosted emails									
Archival tapes									
Attachments									
Archives									
Document Management Systems									
File net									
Jordan Lawrence									
E-Time systems									
Payroll systems									
Benefits systems									
Other systems									
Databases									
Credit card/ debit card Databases									
VOIP logs									
IM databases									
Business application databases (Quicken, Calendar, Address Book, etc.)									
Other Data Entry Systems									
Online									
Audit Logs									
Access Logs									
Web Pages									
Blogs									
Deleted/ Unused Space									
Slack Space									
Deleted/ Recovered Files									
Other									

Dawn Haghighi- dhaghighi@aol.com

CERTIFICATION

I certify that the data/statements I have supplied herein are true and complete to the best of my knowledge and belief.

_____
SIGNATURE

_____
TYPE OR PRINT NAME

_____
TITLE

_____
TELEPHONE NUMBER

_____
DATE

VENABLE® LLP

ACC Association of Corporate Counsel

Top Ten Steps to Take When the FTC Investigates Your Company's Privacy Practices

The Federal Trade Commission ("FTC") has emerged as the primary federal agency responsible for privacy and data security in the United States. When the FTC investigates a company's privacy or data security practices, the agency is acting in its law enforcement capacity. The FTC may conduct a nonpublic investigation through either informal or formal means. Informal investigations are typically conducted through "access letters," which are unenforceable requests for information that seek voluntary cooperation. Formal investigations are typically conducted through Civil Investigative Demands ("CIDs"), which are judicially enforceable demands for documents and written answers to questions. Refusal to cooperate with an informal inquiry typically results in the issuance of a CID.

There are many considerations to keep in mind when responding to an inquiry by the FTC. Assuming that your company has been served with a CID, here are our top ten suggestions for helping to bring the FTC's investigation to an early resolution based upon our collective 30 years of experience of representing companies in privacy and data security investigations:

1. UNDERSTAND.

Read the CID carefully. Jot down deadlines for production, for meeting and conferring with FTC counsel, and for filing any petitions to limit or quash the CID. Identify the "applicable time period" covered by the CID, the Commissioner who signed the CID, and the statutory authority under which the FTC is proceeding (set out in the accompanying blanket "resolution" authorizing the exercise of compulsory process). Research the FTC's authority to impose monetary penalties under the cited statutory authority. Highlight the CID's definitions. Differentiate between requests for "all" documents, on the one hand, and for documents "sufficient" to identify or describe a particular activity. Note the fact that documents submitted to the FTC are treated as confidential. And fully understand the certification that you or a business executive will be asked to execute upon completion of production.

2. PRESERVE.

As a recipient of a CID, you are now under an obligation to provide information to the FTC, and the associated duty to preserve evidence now attaches. Issue a litigation hold and instruct IT staff to suspend any scheduled systems maintenance that may affect relevant information.

3. COMMUNICATE.

Keep open communications between yourself and the FTC Staff. A simple "what is it that you are looking for" may yield insights that can help you understand their concerns, narrow the scope of the inquiry, and focus the company's response to the inquiry. Keep the Staff informed of any potential delays. Do not surprise them.

4. OFFER ALTERNATIVES.

If the CID in its current form proves to be too burdensome, develop and explore alternatives. These may include extending the deadline for completion of production, narrowing the scope of the inquiry by modifying definitions or specific interrogatories or document requests, sampling methods, and collaboration with Staff on search terms or parameters. An agreement to extend a production deadline may also include tolling the deadline for filing a petition to limit or quash the CID.

TO ENSURE YOUR COMPANY'S PRIVACY HEALTH, PLEASE CONTACT US TODAY.

EMILIO W. CIVIDANES
202.344.4414
ecividanes@Venable.com

STUART P. INGIS
202.344.4613
singis@Venable.com

5. READ.

Review the documents that you have identified as being responsive. Learn the story behind them. Review any answers to interrogatories drafted by others. Advise the general counsel or senior executives of potential legal issues arising from the documents and responses.

6. THEORIZE.

Equipped with the information that you have gleaned from the documents and draft responses, coupled with information from other sources (e.g., what the Staff has disclosed to you, the statutory authority under which the FTC is proceeding), identify potential legal theories under which the FTC could be proceeding against the company. This will help you anticipate the Staff's focus, develop a theory for the company's defense, and shape the context that should be provided for documents to be produced (see item 8).

7. CHOOSE WISELY.

Particularly when you have the flexibility to choose what information to produce (e.g., choosing documents "sufficient" to describe certain company operations), exercise your judgment. For example, in choosing documents "sufficient" to demonstrate the company's privacy training program, produce documents that answer the question that has been asked without raising new questions, which might lead to new areas of inquiry and prolong the investigation. Also, take steps to reduce the burden on the Staff. Although there are no hard-and-fast rules, the more time the Staff invests in its investigation of your company, the more likely the Staff is to want to establish a violation that justifies the time and effort it has invested.

8. CONTEXTUALIZE.

Reduce the potential for a misreading of the documents to be produced by explaining their context. What might at first blush look like a "smoking gun" to the FTC Staff may in fact be an innocuous set of communications that provides no support for any theory of liability contemplated by the Staff. If what needs explaining aren't facts but rather the application of the law to the facts, consider preparing and submitting a "White Paper" that explains the company's view of the law and the facts. Such legal briefs can help narrow the issues or theories under consideration.

9. CONTACT EXPERIENCED OUTSIDE COUNSEL.

In all candor, this one should be your first step. Experienced counsel can help the company navigate around the pitfalls inherent in an investigation. They can help preserve privilege over an internal investigation into the events that are the subject of the CID. Experienced counsel can act as a buffer with the FTC Staff, which usually views outside counsel as more independent of the client than in-house counsel. They may have interacted with the very same FTC counsel in a previous investigation, or defended another company in connection with an investigation of the same or a similar privacy practice. Experienced outside counsel are familiar with agency customs and are thereby able, for example, to reduce anxiety by explaining that the Staff's response that it "agrees to delay taking any action against your client for another 7 days" is not unduly adversarial but rather a bureaucratic means of extending deadlines without having to seek written changes to the CID, as otherwise required by the statue.

10. WAIT PATIENTLY.

FTC Staff's review of the documents and information produced by a company typically takes many months, often more than a year. After investing so much time and effort over an extended period of time to respond to the CID, it is very tempting after several months of silence to inquire regarding the status of the investigation. Resist the temptation. Time can often work to your advantage. For example, the FTC may accomplish through its settlement of another case some of the goals it had set out in connection with its investigation of your company. If you have followed steps 1-10, your patience may be rewarded with a telephone call from the Staff indicating that it has closed the investigation of your company.

VENABLE® LLP

1.888.VENABLE
www.Venable.com

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

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.

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

August 2012

In this Issue:

Heard on the Hill

Senate Commerce Ponders Self-Regulation

Under the Chairmanship of Sen. Rockefeller (D-WV), the Committee on Commerce, Science, and Transportation (the "Committee") continues to examine issues of data privacy and consumer protection. On June 28, 2012, the Committee held a hearing titled "The Need for Privacy Protections: Is Industry Self-Regulation Adequate?" This hearing followed up on the Committee's May 9th hearing to review privacy frameworks set forth by the Obama Administration and the Federal Trade Commission ("FTC").

The June hearing focused on efforts by industry to address privacy concerns via the Digital Advertising Alliance's ("DAA") self-regulatory program. The DAA is a coalition of the nation's leading media and marketing trade associations, including the Association of National Advertisers, the American Advertising Federation, the American Association of Advertising Agencies, the Direct Marketing Association, the Interactive Advertising Bureau, and the Network Advertising Initiative. The DAA administers a self-regulatory program that calls for entities engaged in collection of web viewing data to provide enhanced transparency and consumer control.

At the hearing, Chairman Rockefeller expressed his skepticism about self-regulation and pledged to continue supporting legislation and holding hearings to promote adequate consumer protection. In May 2011, he introduced S. 913, the Do-Not-Track Online Act, but the bill has not yet been formally considered in the Committee. During her opening remarks, Senator Ayotte (R-NH) cautioned against rushing toward legislation. She stated that consumers and the market, rather than Congress, are best suited to address concerns.

Mr. Bob Liodice, President and CEO, Association of National Advertisers, speaking on behalf of the DAA, reported on the evolution and progress of the DAA's Self-Regulatory Program for online data collection. He explained that the DAA Program has evolved with the FTC's encouragement, represents industry consensus on an opt-out standard, and is already being expanded to the mobile ecosystem. He emphasized the value realized for consumers through data collection and use, and explained that data collection is critical to the operation and functionality of the Internet.

Senate Examines Facial Recognition Technology

On July 18, 2012, the Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, held a hearing titled "What Facial Recognition Technology Means for Privacy and Civil Liberties" to consider the implications of facial recognition technology in law enforcement and civil applications.

Subcommittee Chairman Al Franken (D-MN) said he called the hearing to raise awareness that facial recognition technology is in widespread use today. He explained that facial recognition raises acute privacy concerns, and that he believes in the fundamental right to control biometric information because it is permanent and inalterable.

Maneesha Mithal, of the Bureau of Consumer Protection, Federal Trade Commission ("FTC"), testified to a number of examples of both beneficial and more invasive commercial uses of facial recognition technology. Ms. Mithal highlighted the FTC's December 2011 workshop on the topic, where participants discussed the increased use of facial recognition technologies due to recent developments such as better cameras and the rapid growth of online photo sharing. She recommended that companies that employ facial recognition technology should provide clear, simple, concise notice of the practice. She also revealed that the FTC plans to issue a report later this year recommending best practices for using facial recognition technologies.

Congress and the States Consider Legislation on Employer Access to Social Media Accounts

Lawmakers in the Senate and House of Representatives have introduced legislation (S. 3074, H.R. 5684) that would amend the Computer Fraud and Abuse Act to make it a federal crime, punishable

by fines, for employers to knowingly and intentionally "compel or coerce" a person to authorize access (such as by providing a password) to a computer that is not the employer's computer, for hiring, promotion or firing purposes, and thereby to obtain information from the computer. The bills would therefore leave room for employers to compel employees to grant access to computers that belong to such employers. However, the bills would also criminalize retaliation against whistleblowers and employees who refuse to provide access to computers that are not an employer's computers. The restrictions on employers would not apply in certain cases: (1) if employees are disciplined or fired for other good cause; (2) if a State wishes to waive the federal law for its own employees or for individuals who work with children; or (3) if federal agencies waive the law for classes of employees who access classified information.

A competing measure introduced by Representatives Engel (D-NY) and Schakowsky (D-IL) (H.R. 5050), titled the Social Networking Online Protection Act, would prohibit employers from requiring or requesting that an employee or applicant provide access to private email or social networking accounts regardless of the computer used. "Social networking websites" are defined to include any site for managing user-generated content, a definition not limited to sites with social sharing features. The legislation also protects whistleblowers and employees who refuse to provide such access. These restrictions would be enforceable by the Secretary of Labor through civil penalties and injunctive relief. The same restrictions would apply to schools and universities that receive federal funding, with respect to the accounts of students and applicants.

These federal legislative proposals echo bills introduced in over a dozen states that would similarly prevent entities from seeking access to individuals' personal online accounts. In May, Maryland became the first state to enact such legislation. Maryland's law, which will take effect on October 1, 2012, prohibits employers from requesting or requiring access to certain personal accounts of employees or applicants and from retaliating against employees or applicants who refuse to provide access. The law specifies that employees may not download certain unauthorized data to their personal accounts, and that employers are not prevented from conducting certain internal investigations. Delaware has enacted password protection legislation that applies to higher educational institutions. Other state measures remain under consideration.

Around the Agencies

FTC and Spokeo Settle Fair Credit Reporting Act Allegations

The Federal Trade Commission ("FTC") settled allegations against consumer data provider Spokeo in what the agency described as its

first case on the sale of Internet and social media data in the employment screening context.[1] The case followed several warning letters that the FTC sent earlier this year to mobile application ("app") marketers warning that their background screening apps may be subject to the Fair Credit Reporting Act ("FCRA").[2]

The federal complaint filed against Spokeo by the U.S. Justice Department, litigating on behalf of the FTC, stated that Spokeo provides "consumer reports" subject to the FCRA because the company assembled consumer information from sources including social networking sites, provided access to individually identifiable data profiles through paid subscriptions, and offered and marketed its data for use in hiring and recruiting job candidates.[3] The complaint alleges that Spokeo failed to comply with applicable requirements of the FCRA.

The FTC further alleged that Spokeo employees endorsed company products in online forums without revealing their connection to the company, thereby engaging in deceptive advertising in violation of the FTC Act. In 2009, the FTC issued an update to its guidance on endorsements in advertising, which clarified the agency's views that online commenters should disclose material connections to companies they endorse.[4]

In addition to paying $800,000 in civil penalties, Spokeo agreed in the settlement to comply with the FCRA, to rectify its advertising endorsement practices, and to comply with reporting and recordkeeping provisions similar to those of other FTC consent agreements.

FTC Requests Further Comment on Its COPPA Rule

On August 1, 2012, the Federal Trade Commission ("FTC") issued its supplemental Notice of Proposed Rulemaking ("NPRM") in connection with its Children's Online Privacy Protection Rule ("COPPA Rule") review.[5] The NPRM proposes additional modifications to the COPPA Rule's definitions of terms: "operator," "personal information," "screen name," "support for internal operations," and "website or online service directed to children." The FTC will be taking comments until September 10, 2012.

This NPRM follows and modifies the FTC's earlier proposed rule ("Proposed Rule"), issued in September 2011, to amend the FTC's

[1] FTC Press Release, "Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA" (June 12, 2012), available at http://www.ftc.gov/opa/2012/06/spokeo.shtm.

[2] FTC Press Release, "FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act" (February 7, 2012), available at http://www.ftc.gov/opa/2012/02/mobileapps.shtm.

[3] Complaint, *United States v. Spokeo*, CV-12-05001 (C.D.Cal., filed June 7, 2012).

[4] 16 C.F.R. Part 255.

[5] FTC NPM, available at http://www.ftc.gov/opa/2012/08/coppa.shtm.

current COPPA Rule. The COPPA Rule applies to operators of commercial websites and online services directed to children under age 13 that collect, use, or disclose personal information This NPRM follows and modifies the FTC's earlier proposed rule ("Proposed Rule"), issued in September 2011, to amend the FTC's current COPPA Rule. The COPPA Rule applies to operators of commercial websites and online services directed to children under age 13 that collect, use, or disclose personal information from children, and to operators of general audience websites that have actual knowledge that they are collecting, using, or disclosing personal information from children under age 13. The COPPA Rule provides parents with tools to control how personal information about their children is collected online.

When the Commission released the Proposed Rule, it explained that it was seeking to update the regulation to help ensure that it continues to protect children's privacy online as technologies evolve. In its proposal, the FTC explained that the COPPA Rule would continue to apply to children under age 13. Additionally, the Commission noted that the regulation would still only apply to general audience websites and online services when operators have actual knowledge that they are collecting personal information from children.

The Proposed Rule includes several proposed amendments to the COPPA Rule, including among others the FTC's proposals to:

- Expand the definition of "collection";
- Consider the presence of child celebrities and celebrities who appeal to children as factors when determining if a website or online service is directed to children;
- Modify required online privacy policies and direct parental notices;
- Eliminate the sliding scale approach to obtaining verifiable parental consent;
- Create a Commission approval process for identifying new means of obtaining verifiable parental consent;
- Place data security obligations on service providers;
- Implement new data retention and deletion requirements; and
- Include audit and reporting requirements for self-regulatory safe harbor programs.

The Multistakeholder Process on Mobile Transparency Begins

On July 12, 2012, the National Telecommunications and Information Administration ("NTIA") hosted its first multistakeholder process meeting to examine mobile application transparency. Earlier this year the White House released a privacy blueprint and requested that NTIA convene interested stakeholders to develop enforceable codes of conduct. In response, the NTIA hosted a meeting titled, "Providing Transparency in How Consumer Data Is Handled by Mobile Applications." The meeting kicked off NTIA's effort to develop a code

of conduct for providing transparency for mobile apps and interactive services for mobile devices. The next meetings will be held August 22nd and 29th.

Lawrence Strickling, Assistant Secretary for NTIA, greeted the more than 200 people who attended the meeting in person, with another 100 or more joining online. He said that the discussion is "the first step in a journey to develop codes of conduct for transparency in mobile apps." He reiterated that NTIA will act solely as a facilitator of the process, and it will not impose rules or its judgment on the process. He said the purpose of the first meeting is not to reach any consensus, but instead to identify issues for future meetings.

In line with the Assistant Secretary's message, the NTIA conveners guided the discussion to assist the stakeholders in identifying common ground on issues. This process resulted in the stakeholders identifying over 70 substantive points for consideration. On August 1, 2012, NTIA released a list of discussion elements grouping similar substantive points identified by the group into "working lists."[6] NTIA has suggested that stakeholders consider these issues in working groups in advance of the August meetings.

In the States

State Attorneys General to Examine Privacy

In June, Maryland Attorney General Douglas Gansler was elected president of the National Association of Attorneys General ("NAAG") and announced that his year-long presidential initiative will focus on "Privacy in the Digital Age." State attorneys general not only enforce the privacy laws of their own states; they also have authority to enforce certain federal privacy restrictions.

Attorney General Gansler, now in his second term, has been active in using his post to scrutinize privacy issues and often describes state attorneys general as "the Internet police." In announcing his initiative, Attorney General Gansler pledged that NAAG will spend the next year "bringing the energy and legal weight of this organization to investigate, educate and take steps necessary to ensure that the Internet's major players protect online privacy and provide meaningful options for privacy control, while continuing to enhance our lives and our economy."[7] As a part of this initiative, NAAG will hold a conference in April 2013 focusing on privacy issues. Although the effects remain to be seen, Attorney General Gansler's initiative may lead to increased awareness, and potentially scrutiny, of Internet privacy issues among

[6] See NTIA Working Lists Document, available at http://www.ntia.doc.gov/files/ntia/publications/draftgroupings_08012012.pdf.

[7] NAAG Website, "2012-2013 Presidential Initiative: Privacy in the Digital Age," available at http://www.naag.org/privacy-in-the-digital-age.php.

state prosecutors nationwide.

In California, Attorney General Kamala Harris recently announced the creation of a new Privacy Enforcement and Protection Unit within her Justice Department.[8] This Privacy Unit will be staffed with six prosecutors dedicated full time to enforcing state and federal privacy laws. Joanne McNabb, who previously headed the California Office of Privacy Protection, will oversee the Privacy Unit's consumer education and outreach efforts. The Privacy Unit is located within California's eCrime Unit, which the Attorney General launched in 2011 to focus on cyber crimes.

****

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] California Attorney General's Office Press Release, "Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit" (July 19, 2012).

VENABLE® LLP

are you at risk?

TEN QUESTIONS YOU SHOULD ASK YOURSELF TO ENSURE YOUR CORPORATE PRIVACY HEALTH.

Q 1. DO I USE INFORMATION ABOUT CUSTOMERS FOR MARKETING OR OTHER PURPOSES NOT RELATED TO THE PARTICULAR SALE OR TRANSACTION IN WHICH I COLLECTED THE INFORMATION?

Using or disclosing information about individuals for a "secondary purpose" – a purpose not directly related to the purpose for which the information was collected – lies at the heart of existing consumer privacy laws, and those that are being debated in legislatures across the country. If you answered yes to this question, your activity may trigger the requirements of existing privacy laws.

Q 2. DO I COLLECT CONTACT INFORMATION FROM CUSTOMERS WHEN THEY USE THEIR CREDIT CARD TO PAY FOR PURCHASES?

Some states restrict the circumstances under which a seller can use a consumer's address or telephone number if the data was collected from a credit card purchase. If you answered yes to this question, your activity may trigger the requirements of existing privacy laws.

Q 3. DO I ASK VISITORS TO MY WEB SITE TO TELL ME THEIR AGE? DO I MARKET ANYTHING TO CHILDREN ONLINE?

Online activities affecting children under age 13 are regulated by federal law and standards issued by the National Advertising Council. These laws and standards apply if a Web site either "knows" (e.g., knowledge gained by asking for age), or "should have known," that it is interacting with a child. If you answered yes to either of these questions, and collect information that can be linked to a child (e.g., first and last name, email address), your activity triggers the requirements of the Children's Online Privacy Protection Act.

Q 4. DO I RETAIN CREDIT CARD INFORMATION?

Companies who retain their customers' credit card information are required by law to take certain measures to ensure the protection of that information. If you answered yes to this question, in some circumstances you may be subject to penalties running into the millions of dollars and loss of merchant accounts.

Q 5. DO I HAVE A PRIVACY POLICY ON MY WEB SITE? IF SO, AM I DOING WHAT I TELL MY CUSTOMERS I AM DOING WITH THEIR PERSONAL INFORMATION?

Most companies voluntarily post privacy policies on their Web sites to help foster trust and confidence; California law requires online merchants to post a privacy policy on their Web sites. Either way, once a company posts a privacy policy on its Web site, federal and state laws against deceptive practices require the company to fulfill the commitments in that policy. If you answered yes to this question, you are subject to the laws prohibiting deceptive practices.

TO ENSURE YOUR COMPANY'S PRIVACY HEALTH, PLEASE CONTACT US TODAY.

EMILIO W. CIVIDANES
202.344.4414
ecividanes@Venable.com

STUART P. INGIS
202.344.4613
singis@Venable.com

MICHAEL A. SIGNORELLI
202.344.8050
masignorelli@Venable.com

Q 6. DO I CONDUCT BUSINESS WITH COMPANIES IN THE HEALTH CARE, FINANCIAL SERVICES OR TELECOMMUNICATIONS SECTORS?

Standards mandated by federal and state privacy laws regulating companies within the health care, financial services and telecommunications sectors extend to vendors and others that provide services to these regulated entities. If you answered yes to this question, you are likely operating under contractual requirements mandated by federal privacy laws.

Q 7. DO I DO WHAT I TELL MY EMPLOYEES I WILL DO WITH THEIR PERSONAL INFORMATION? DO I TELL MY EMPLOYEES HOW I MONITOR THEM IN THE WORKPLACE?

Employers have access to sensitive information about their employees collected in the ordinary course of business, including data collected as a result of monitoring or evaluating employee performance. Employees typically have very limited privacy rights in the workplace, but their rights can expand if you make commitments to them concerning use of that information. If you answered no to either of these questions, your activity raises privacy issues and may in fact trigger the requirements of existing workplace privacy laws.

Q 8. DO I RECEIVE PERSONAL INFORMATION (ABOUT CUSTOMERS, EMPLOYEES, VENDORS, OR OTHERS) FROM EUROPE OR OTHER FOREIGN JURISDICTIONS? DO I "OFFSHORE" OR OTHERWISE TRANSFER PERSONAL INFORMATION TO FOREIGN JURISDICTIONS?

Countries in Europe, Asia and Latin America approach privacy differently (some would say more stringently) than we do in the United States. They tend to place restrictions upon the transfer to the United States of information about individuals, even if the information does not pertain to consumers or employees, and even if the parties transferring the information are corporate affiliates. Conversely, U.S. laws often mandate that companies transferring personal information to vendors or subcontractors in foreign countries must require these data recipients to comply with U.S. privacy or security standards. If you answered yes to either of these questions, your activity may be subject to foreign data protection laws or U.S. privacy laws.

Q 9. DO I HAVE AN EFFECTIVE SECURITY PROGRAM DESIGNED TO SAFEGUARD PERSONAL INFORMATION?

Without security protections for personal information, there is no privacy. As a result, federal and state laws mandate that companies develop, implement, and periodically update programs designed to protect its confidentiality. These security obligations often exceed the safeguards that you would implement to protect your proprietary interests in the data. If you answered no to this question, you could be found in violation of law, even if the persons whose information you are storing have suffered no harm.

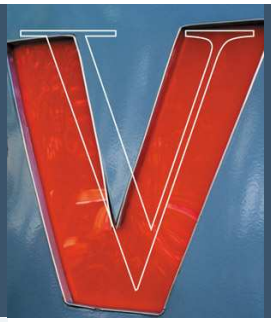
Q 10. DO I HAVE AN EFFECTIVE MITIGATION PLAN FOR PRIVACY OR SECURITY BREACHES?

Breaches of security that compromise personal information are virtually inevitable. Businesses not only must have procedures in place to prevent security breaches, but also procedures in place to respond to such breaches when they occur. More than 30 states have laws requiring notification of affected individuals when their personal information has been compromised by a security breach. If you answered no to this question, you are likely to make hasty decisions when you discover a suspected security breach, which increases the chances you will violate the security notification laws.

VENABLE® LLP

1.888.VENABLE
www.Venable.com

VENABLE® LLP



use of personal devices

VENABLE SNAPSHOT

More than 500 lawyers in seven offices

American Lawyer's AmLaw 100

129 practice groups ranked, "Best Law Firms" *U.S. News & World Report-Best Lawyers* 2011-2012

64 attorneys and 27 practice areas ranked, *Chambers USA 2012*

PRIVACY AND DATA SECURITY QUICK FACTS

More than 20 attorneys experienced in data privacy issues

Authors/editors of the forthcoming *BNA Portfolio on Privacy Law*

Exclusive sponsor of the Association of Corporate Counsel's IT, Privacy and eCommerce Committee

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

HONORS AND AWARDS

Recognized by *Chambers USA*

TOP RANKED CHAMBERS USA 2012 Venable LLP

Previous Winners of the *Chambers USA* Award for Excellence

Ranked among the nation's top firms, Technology: Data Protection & Privacy, in *Legal 500*

The LEGAL 500 UNITED STATES TOP TIER 2012

BYOD USAGE POLICY – CHECKLIST*

Preconditions for allowing employees to use a personal device for work

1. Enable security measures selected by the company.
2. Require an acknowledgement that all company policies apply. Also obtain acknowledgment that all contents of device may be subject to discovery by third parties. Explain need for "kill command" (and obtain advance consent and waiver, see items 8 & 9).
3. Amend your organization's electronic resources policy to address monitoring of personal devices.
4. Get consent to access the personal device for legitimate business purposes.
5. Prohibit use of personal accounts to conduct company business.
6. Prepare ahead of time for a potential security incident.
7. Limit the storage of sensitive information on personal devices.
8. Get consent before sending a kill command.
9. Get a release before sending a kill command.
10. Think about how your organization will retrieve business information when employment ends.

* This checklist is intended for use in conjunction with EEO and work safety policies, and after application of employee selection criteria (*e.g.*, exempt employees only) and deployment of mobile management technology.

Our combined experience—mastering the intricacies of compliance with a maze of federal laws, defending clients in regulatory actions and guiding the data and privacy aspects of corporate mergers and alliances—enables us to respond quickly when new issues arise in any client's business.

How can we help you? To find out, please contact us at 1.888.VENABLE or www.Venable.com.