The Latest Legal Developments in Privacy, Data Collection and Security

June 16, 2011

Ieuan Jolly
ijolly@loeb.com | 212.407.4810

Michael Mallow
mmallow@loeb.com | 310.282.2287

Michael Thurman
mthurman@loeb.com | 310.282.2122

LOEB & LOEB LLP

Reminders

General information:

- Presentation slides, related cases and speaker biographies are available under **HANDOUTS** on the left side of your screen
- You may ask questions at any time during the program using the **CHAT** feature, also on the left side of your screen

CLE information:

You must be logged in for the entire webinar to receive credit; partial credit will NOT be granted*

- An **evaluation form** and **New York State CLE affirmation form** are available for download under **HANDOUTS** on the left side of your screen (*These documents will also be available on our website after the program and a link will be emailed to you*)
- For **New York State CLE credit**, please write down the **TWO** codes you'll see in the middle and at the end of the webinar (*We will remind you when they appear*)
- For **CLE credit in CA and IL**, please fill out the evaluation form which has a section for you to indicate in which state(s) you are seeking CLE credit

To request CLE credit, please return all forms by JULY 1 using the contact information listed on the forms

LOEB & LOEB LLP

Today's Agenda

- Update on legislative developments
- Recent litigation and enforcement actions

The Wind of Change

In the last two years, there have been important changes in the US approach to privacy:

- New state laws that are proactive and prescriptive, rather than reactive and discretionary
- More than 10 new federal privacy bills since January 2011
- FTC Privacy Report
- Commerce Department privacy “green paper”
- More enforcement actions – and more lawsuits

Selected Federal Privacy Bills Introduced Since January 2011

- Do Not Track Me Online (H.R. 654) (Speier)
- Do Not Track Online Act of 2011 (S. 913) (Rockefeller)
- Commercial Privacy Bill of Rights Act of 2011 (S. 799) (Kerry-McCain)
- Consumer Privacy Protection Act of 2011 (H.R. 1528) (Stearns-Matheson)
- BEST PRACTICES Act (H.R. 611) (Rush)
- Data Accountability and Trust Act (H.R. 1707) (Rush)
- Personal Data Privacy and Security Act of 2011 (S. 1151) (Leahy)
- Do Not Track Kids Act of 2011 (H.R. 1895) (Markey)

Kerry-McCain Bill (S. 799)

- Would require "covered entities" to
  - Provide notice of their data collection practices and to disclose the purposes for the data collection
  - Provide an opt-out mechanism for "covered information" and an opt-in mechanism for sensitive information
  - Establish procedures for safeguarding data
  - Collect only as much information as is reasonably necessary and maintain the information only as long as necessary
  - Provide consumers with access to certain information
- Would authorize the FTC to develop a safe harbor program
- Would apply to an entity:
  - That collects, uses, transfers or stores "covered information" concerning more than 5,000 individuals during any consecutive 12-month period; and
  - That is within the FTC's jurisdiction or is a common carrier under the Communications Act of 1934 or is non-profit organization
- No private right of action
- Preempts some, but not all, state privacy laws

LOEB & LOEB LLP

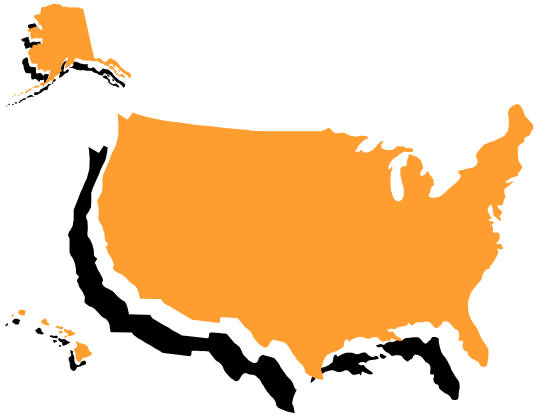
Stearns-Matheson Bill (H.R. 1528)

- Requires covered entities to:
  - Disclose that the personally identifiable information collected by the covered entity may be used or disclosed for purposes or transactions unrelated to that for which it was collected
  - Provide a privacy policy the first time the covered entity collects information that may be used for a purpose unrelated to a transaction
  - Provide an opt-out from the sale or disclosure for consideration of an individual's personally identifiable information
- A covered entity is "an entity (or an agent or affiliate of the entity) that collects (by any means, through any medium) sells, discloses for consideration, or uses personally identifiable information of more than 5,000 consumers during any consecutive 12-month period"
- Safe harbor for entities that participate in an approved self regulatory program
- Preempts all state laws relating to the collection and use of personal information "in commerce“
- No private right of action and no enforcement by state Attorneys General

LOEB & LOEB LLP

Different Approaches to Privacy

US Approach to Privacy



- "Balancing" privacy rights with business interests
- Notice and consent
- Self regulation
- Piece-meal, not comprehensive
- State, federal, local

EU Approach to Privacy

- Comprehensive Data Protection Directive
- Privacy is a human right
- Significant restrictions on most data collection, processing, dissemination and storage
- Consent required for most uses of personal data
- Applies to data processed inside the EU as well as throughout the world

LOEB & LOEB LLP

US Privacy Approach

- US privacy laws typically follow the “notice and consent” approach:
  - Consumers must be provided with:
    - Notice of their privacy rights; and
    - An opportunity to “opt-out” of having data collected, used or shared about them
  - Some laws require an “opt-in” – that is, affirmative consent – for the collection, use and sharing of “sensitive information,” medical information, financial information, and information collected from children
- Industry guidelines also typically follow the “notice and consent” approach

FTC Privacy Report (December 2010)

- FTC said many privacy policies are inadequate because they are difficult for consumers to understand and sometimes difficult to find
- FTC proposed a new framework:
  - Privacy by design
  - Simplified choice – easy to use; offered when consumer is making a decision about his or her data
  - Greater transparency – notice should be easy to understand; should provide consumers with access to their data (on a sliding scale)

Department of Commerce “Green Paper”

- DOC proposes a "Dynamic Privacy Framework"
- Recognition of “baseline” consumer privacy rights
- Passage of a federal security breach notification law
- Establishment of a federal Privacy Policy Office
- More self-regulatory programs for various industries
- More transparency in privacy notices
- More cooperation with other countries to harmonize international privacy standards

Privacy Policies and Disclosures

- Provide notice of how you collect, use, share, store and destroy information:
  - Make it easy to understand
  - Make it easy to find – do not bury notice in a lengthy privacy policy or terms of use (EchoMetrix settlement)
  - Appropriate size and placement for small screens
- Provide an easy to use opt-out mechanism and describe how individuals use the opt-out method
- Provide notice and an opportunity to opt-out if you change your privacy policy; a company should not apply a new privacy policy to information collected under an old privacy policy without providing notice and an opportunity to opt out
- For sensitive information (medical, financial, race, religion, sexual orientation), obtain affirmative consent before collecting, using or sharing such information
- For children, need verifiable parental consent (COPPA)

LOEB & LOEB LLP

Example of New State Law – Massachusetts 201 CMR 17.00

- Establishes requirements designed to *prevent* a security breach, not just for *responding* to a security breach
- The Massachusetts law is more similar to EU privacy laws than many other laws in the US
- It rejects the "balancing" approach – that is, balancing privacy rights with business interests – and squarely tells businesses to establish and adopt specific technical and procedural measures to protect personal information

LOEB & LOEB LLP

How Will the New Massachusetts Law Impact Businesses?

- Development of comprehensive written information security system
- Implement physical, administrative and technical controls, including the use of encryption
- Vendor management – verify that any third-party service providers that have access to personal information can protect such information

Litigation and Enforcement

The FTC and Privacy

The FTC has initiated many enforcement actions against online and offline companies for allegedly violating the FTC Act by:

- Not complying with a posted privacy policy
- Changing a privacy policy and not giving consumers notice or the opportunity to opt out of the new policy
- Failing to adequately safeguard data
- Claiming to provide adequate security for data and then failing to do so
- Failing to adequately disclose what data is collected and for what purpose
- Failing to honor op-out promises

FTC v. Playdom (COPPA)

- Playdom, operators of 20 online virtual worlds, agrees to pay $3 million to settle FTC charges they violated the Children's Online Privacy Protection Rule by illegally collecting and disclosing personal information from hundreds of thousands of children under age 13 without their parents' prior consent
- FTC stated this is the largest COPPA settlement to date
- Sites allowed users to access multi-user online games and other activities
- Sites specifically directed to children or intended for general audiences that attract a significant number of children
- Between 2006 and 2010, approximately 403,000 children registered on the defendants' general audience sites and 821,000 more users registered on the children's site

FTC v. Playdom
(continued)

- Complaint alleged sites collected children's ages and email addresses during registration and then enabled children to publicly post their full names, email addresses, instant messenger IDs, and location, among other information, on personal profile pages and in online community forums

- Site operators failed to provide proper notice or obtain parents' prior verifiable consent before collecting or disclosing children's personal information

- Operators violated the FTC Act because privacy policy misrepresented that the company would prohibit children under 13 from posting personal information online

FTC v. Ceridian (Data Security)

- FTC charged Ceridian Corporation – a provider of business payroll and HR services – with unfair and deceptive security practices
- Ceridian allegedly failed to live up to its promise to take reasonable security measures to safeguard personal info including Social Security numbers
- Ceridian claimed “Worry-Free Safety and Reliability” in accordance with ISO 27000 series standards, industry best practices and federal, state and local regulatory requirements

FTC v. Ceridian

(continued)

- Intruder breached one of Ceridian's web-based payroll processing applications in December 2009 and compromised the personal information – including Social Security numbers and direct deposit information – of approximately 28,000 employees of Ceridian's small business customers
- Company did not adequately protect its network from reasonably foreseeable attacks
- Stored personal information in clear, readable text indefinitely on its network without a business need
- Settlement order requires company to implement comprehensive information security program and obtain independent audits of the program every other year

Pineda v. Williams-Sonoma Stores

- California Supreme Court finds that that zip code information constitutes Personally Identifiable Information (PII) under California's Song-Beverly Credit Card Act of 1971 (Civil Code § 1747 et. seq.)

- Under the statute, merchants may not require consumers to provide PII as a condition to accepting a credit card as payment for the purchase of a product or service if such information is written down or otherwise recorded

- Court held that PII includes the consumer's telephone number, address, including zip code, email address, and any other information concerning the cardholder other than the information that is shown on the credit card

Pineda v. Williams-Sonoma Stores

(continued)

- Song-Beverly Credit Card Act of 1971 does not apply to transactions where the PII is not written down or otherwise recorded. Statute does not restrict merchants from requiring the production of a drivers' license, personal identification card or even PII for authentication purposes so long as the information is not recorded

- Law does not apply to:
  - Online transactions
  - Transactions involving the return of merchandise
  - Collection of PII incidental to completing the transaction, such as shipping, servicing, delivering or installing merchandise for the consumer

- Penalties:
  - Up to $250 per violation for a first-time violation
  - Up to $1,000 for subsequent violations

AT&T Mobility LLC v. Concepcion, et. al.

- US Supreme Court holds that the Federal Arbitration Act preempts California law banning class action waiver provisions in consumer arbitration agreements
- Overturned the California Supreme Court's decision in *Discover Bank v. Superior Court* holding that arbitration clause in consumer agreement containing a class action waiver was unconscionable and therefore unenforceable as a matter of law
- This ruling may limit liability to class action exposure for privacy violations

Zombie Cookies

- Federal district court in California approves settlements in two consolidated class actions over the use of “zombie cookies”
- Complaints alleged that defendants and their affiliates stored tracking data on users’ computers using the Adobe Flash Media Player rather than storing them the traditional way – in internet browser cookies – making it difficult for computer users to delete
- Plaintiffs alleged that flash cookies were re-activated even after users deleted them, and that defendants failed to provide notice of this tracking and failed to obtain consent for it
- As part of the settlement, the court issued an injunction prohibiting the use of flash cookies to re-spawn deleted cookies or to serve as an alternative to traditional cookies. It also provides for defendants to pay $2.4 million to a settlement fund

LOEB & LOEB LLP

Questions and Answers

The Latest Legal Developments in Privacy, Data Collection and Security

June 16, 2011

Ieuan Jolly
ijolly@loeb.com | 212.407.4810

Michael Mallow
mmallow@loeb.com | 310.282.2287

Michael Thurman
mthurman@loeb.com | 310.282.2122

LOEB & LOEB LLP