ABA Section of Antitrust Law
Privacy and Data Security Update
for May 2011

Pamela Jones Harbour
David Kessler
Erika Brown Lee
Sue Ross
Fulbright & Jaworski L.L.P.

June 9, 2011
Agenda

- Legislative developments;
- Regulatory/enforcement developments;
- Litigation developments; and
- Other developments.
Legislative Developments
Federal Legislation

• Do not track
  – HR 1895 (Do Not Track Kids Act)
    • Would amend COPPA to include “website, online service, online application, or mobile application”
    • Prohibits collecting personal information from “minors” (13 to 17) unless implemented a “Digital Marketing Bill of Rights for Teens”
    • Prohibits collecting geolocation data from children or minors in violation of new FTC regulations
    • Includes “right to be forgotten”
Federal Legislation (cont’d)

• Do not track (cont’d)
  – S 913 (Do Not Track Online - Rockefeller bill)
    • FTC to prescribe regulations regarding standards for implementation of a mechanism where user can “simply and easily” indicate whether to have personal information collected online (including providers of mobile applications and services).
    • Exceptions: if necessary to provide a service requested by the user or the user receives “clear, conspicuous and accurate notice” and “affirmatively consents to such collection and use.”
    • Civil penalties: $16,000/day up to $15 million
Federal Legislation (cont’d)

• Security Breaches
  – HR 1707 – Data Accountability and Trust Act (Rush bill)
  – HR 1841 – Data Accountability and Trust Act (DATA) of 2011 (Stearns bill)
  – White House cyber security plan
Federal Legislation (cont’d)

- Security breach bill comparison:
  - House bills use “standard” definition of “personal information,” but White House proposal much broader
  - All contain pre-emption language
  - All contain risk of harm trigger and a presumption of no reasonable risk of harm for encrypted data
  - None contain a private right of action
  - House bills limit fines to $11,000 per day up to $5 million; White House proposal limits fines to $1,000 per day up to $1 million.
State Legislation

- California
  - SB 761 – Do Not Track
    - Would amend California’s spyware law.
    - Would require California Attorney General to adopt regulations by July 1, 2012 to require a person or entity doing business in California that collects, uses or stores online “covered information” from California consumers to provide California consumers with an opt-out method for collection, use, and storage of covered information.
    - Would, to the extent consistent with federal law, prohibit a covered entity from selling, sharing, or transferring a consumer’s covered information.
    - Would include private right of action.
State Legislation – Cont’d

• California
  – SB 242 – Social Networking Policy
    • Social networking sites prohibited from displaying user information without express user agreement written in “plain language.”
    • Did not get majority of Senate.
Enforcement / Regulatory Developments
HIPAA

• May 16 – Office of Inspector General
  – “Audit of Information Technology Security Included in Health Information Technology Standards”
• “Audit of Information Technology Security Included in Health Information Technology Standards”
  – Review of Office of the National Coordinator for Health Information Technology’s IT specifications and IT controls
  – Findings of lack of general IT security controls “raise concern about the effectiveness of IT security for HIT . . .” (at ii)
“Nationwide Rollup Review of the Centers for Medicare and Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight”

– Audit’s purpose “was to determine the sufficiency of CMS’s oversight and enforcement actions pertaining to hospitals’ implementation of the Security Rule.” (at ii.)
HIPAA (cont’d)

– “CMS’s oversight and enforcement actions were not sufficient to ensure that covered entities, such as hospitals, effectively implemented the Security Rule. . . .”

– “Specifically, our audits of 7 hospitals throughout the Nation identified 151 vulnerabilities in the systems and controls intended to protect ePHI, of which 124 were categorized as high impact. . . .” (at iii.)
HIPAA (cont’d)

• Response – March 18, 2011 letter
  – “As a general comment, we caution against drawing conclusions about the state of compliance of all covered entities based on the small sample of narrowly focused audits performed in review of CMS oversight.”
  – “OCR maintains a process to initiate compliance reviews of covered entities in the absence of a compliant . . .:
  – “In addition, OCR performs compliance reviews of covered entities when they report a breach of unsecured protected health information affecting 500 or more individuals, . . .”
HIPAA (cont’d)

- HHS issued notice of proposed rulemaking in May 31 Federal Register
- “HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act”
- Significant changes to 45 CFR §164.528
- Comments due by August 1
HIPAA (cont’d)

• 528 (accounting for disclosures) changes
  – Account for 3 (not 6) years of paper and electronic PHI disclosures
  – Disclosures of information in a designated record set (not any PHI) but includes “treatment, payment and health care operations” through electronic health records, per HITECH
  – Decreases response time to 30 (not 60) days
  – Must provide individuals with the option to limit their request to a specific timeframe, type of disclosure, or recipient
  – Must provide the accounting in form/ format requested by individual if readily producible
  – Compliance date 240 days after final rule published
HIPAA (cont’d)

- New 528 would include individual’s right to “access report” indicating who had accessed electronic protected health information in a designated record set
  - Applies to access by any member of covered entity’s / business associate’s workforce (“use”) and by someone outside these organizations (“disclosure”)
  - Report would include date and time of access; identity of person accessing the information; description of information accessed (if available); and actions taken (create, modify, view, print, etc.)
  - “Material change” to privacy notice
  - 2013 compliance date for many
U.S. v. Playdom

• FTC complaint filed against Playdom (Disney subsidiary) on May 11, 2011 alleging:
  – Collection of children’s ages and email addresses in violation of COPPA
  – Deceptive act or practice violation under Section 5 of FTC Act regarding privacy policy statements which stated that they did not collect
Registration

You are under 13 years old and we cannot ask you for your email address. In order to register, you must ask your Parent or Guardian to fill out this screen. If we find out that this information is false, you may lose your Acclaim account. Parent or Legal Guardian: You can change the email settings anytime by clicking on the My Account button. After you click on the Registration button, you will receive an email to confirm your email address. You have 30 days to activate this account.

Parent/Guardian email address

- Send me emails about Acclaim's games and its partners
- I authorize you to send emails to my child.

Enter the Image Text in the space below: J N U G 1

By clicking the button below, I acknowledge that I am over 12 years old, and I have read and agreed to the Terms of Use, Privacy Policy and Rules of Conduct.

Register  Go Back
Playdom Consent Decree

• Civil penalty of $3 million – largest fine thus far for COPPA violation

• Permanent injunction against:
  – violating COPPA requirements, including failing to obtain parental consent *prior* to collecting or disclosing children’s personal information
  – Misrepresenting privacy practices

• Consumer education remedy

• Compliance monitoring & reporting (4 yrs); record keeping (7 yrs)
In the Matter of Ceridian Corp (May 3, 2011)

- “Powerpay” - web-based payroll service that collected employee personal information
- FTC alleged Section 5 unfairness and deception claims because info was:
  1. Stored indefinitely in clear readable text
  2. Vulnerable to commonly known attacks
  3. Not protected against unauthorized access
- Complaint states that hackers were able to export information of over 27,000 people
Ceridian
Proposed Consent Order

- Prohibits misrepresentations about the privacy, confidentiality, or integrity of personal information collected from/about consumers
- Requires Ceridian to establish and maintain a comprehensive information security program
- Ceridian must provide security assessments every 2 years; order in effect for 20 yrs
In the Matter of Lookout Services (May 3, 2011)

• I-9 Solution product enables employers to comply with U.S. immigration laws

• FTC charges under Section 5 include:
  1. Inadequate security for user/password credentials
  2. Failure to adequately assess and address system vulnerability to widely-known security flaws
  3. Inaccurate statements about its data security

• Allegation that employee of Lookout customer gained access to database with personal info about 37,000 consumers
Lookout Services
Proposed Consent

• Bars misrepresentations about privacy or security of personal information collected
• Requires Lookout to create and implement a comprehensive security program
• Lookout must obtain security audits every 2 years for the next 20 years.
In the Matter of Metronet Telecom (May 3, 2011)

- FCC investigation of non-compliance with the Customer Proprietary Network Information (CPNI)
- CPNI requires annual certification that includes actions taken against data brokers and summary of complaints regarding unauthorized release of CPNI.
Metronet Telecom Consent Decree

- Metronet required to:
  - train personnel within 30 days regarding authorized access to CPNI
  - create a disciplinary process for unauthorized access to CPNI
  - Make a voluntary contribution of $6,400 to the U.S. Treasury
DOJ on Privacy

• Deputy Assistant Attorney General for DOJ Criminal Division Jason Weinstein testified (along with FTC) before the Senate Judiciary Subcommittee on Privacy, Technology, and the Law on May 10, 2011

• DOJ focus is more on cybercrime in the mobile space – e.g., apps that install malicious code on mobile devices to steal sensitive information
Litigation Developments
NIST

• “NIST Cloud Computing Synopsis and Recommendations” (SP 800-146)
• Defines cloud computing and discusses different cloud environments
• Provides information on how organizations should consider the opportunities and risks of cloud computing, including privacy and data security issues
• Comments due by June 13
Sony Complaint - Update

- NOT cloud-related in common terms
- 40+ complaints in US alone
- Claims for breach of contract, breach of warranty of merchantability, negligent data security, etc.
- Evidence of negligence?
Computer Fraud and Abuse Act

• **United States v. Nosal**, No. 10-10038 (9th Cir. Apr. 28, 2011)
  - Criminal aspects of CFAA
  - Indictment relating to exceeding authorized access by current employees

• **Lee v. PMSI**, No. 8:10-cv-02904-SDM-TBM (M.D. Fla. May 6, 2011)
  - Civil aspects of CFAA
  - Lost productivity compensable damage?
Facebook Privacy Litigation

• In re Facebook Privacy Litigation, No. C-10-02389 (N.D. Cal. May 12, 2011)
  – Putative class action
  – Claim that Facebook’s access to personal information permitted targeted ads and Facebook provided “referrer header” information to advertiser
  – Claimed violations under ECPA, SCA, breach of contract, unjust enrichment, etc.
“Flash Cookies” Case

  - Class action against third party ad network that allegedly used “Flash cookies” (or LSOs) to circumvent users’ privacy settings
  - Claimed violations of CFAA, unjust enrichment, trespass to chattels, etc.
Other Developments:
SpiFi, WiFi, COPPA and Cookies
WiFi & Geolocation

• March 18 Capitol Hill Briefing (EPIC): "Street View, Privacy, and the Security of Wireless Networks“

• One-year anniversary after Google revealed that Street View cars intercepted consumers’ WiFi communications in more than 30 countries

• French CNIL findings – connection between competition and privacy
WiFi & Geolocation (cont’d)

• Street View cars collected personal data, including geolocation data
• FTC Bureau Director David Vladeck spoke on the proposed Google Buzz settlement, which has privacy provisions that will apply to ALL Google products
• Smartphones collecting geolocation data
• EU Approach
  – Article 29 Working Party report "Geolocation Services on Smart Mobile Devices" (Opinion 13/2011)
  – MAC addresses of WiFi routers, in combination with the location of those routers, qualify as "personal data"
  – EU limits collection and retention of such data
COPPA

- David Vladeck testimony at May 19 congressional hearing, with particular emphasis on the privacy challenges involving young people
- FTC accelerated review of COPPA rules
  - FTC believes that the COPPA and Rule are written broadly enough to apply to all forms of mobile communication
EU & Cookies

- EU privacy law on cookies went into effect on May 26
- Companies to obtain consent from Web users (i.e., opt-in) when cookies are placed on users’ computers
- Websites can continue automatically installing "cookies" that collect certain limited information
EU & Cookies (cont’d)

• UK data protection authority is giving website owners one year before enforcement

• Any business (wherever it is located) that places cookies on computers belonging to customers based in the EU would be subject to the e-Privacy Directive

• Under the new Privacy Rules, Internet and phone providers will also be required to notify Data Protection Authorities and affected consumers
Questions?

- Pamela Jones Harbour – pharbour@fulbright.com
- David Kessler – dkessler@fulbright.com
- Erika Brown Lee – ebrownlee@fulbright.com
- Sue Ross – sross@fulbright.com