Digital and Privacy Law
Hot Topics on the Horizon for 2012: Security, Promotions and Behavioral Advertising

Dominique Shelton
Partner, Los Angeles

June 6, 2012
WHY IS THIS IMPORTANT TO COMPANIES?

- 138 Do Not Track class actions have been filed in the past 18 months.
- The plaintiffs’ bar is focusing on privacy class actions.
- The FTC has increased its enforcement activity and has announced 4 enforcement actions involving tracking in the past 6 months.
- Based upon global and US trends, more focus on privacy and tracking will occur in 2012.
Online Behavioral Advertising

- Digital Advertising
- Underlying Technologies
Digital Advertising

- Global Advertising: $500 billion in 2011 - a growth rate of 4.5%
- Online Advertising: $80.2 billion - a growth rate of 17.2%
- Online Advertising now exceeds Print Advertising
- Online Advertising
  - 16.1% of global advertising in 2011
  - 22% of global advertising in 2015
  - North America: 41.7% of the worldwide total in 2011
  - Europe: Double digit growth for Olympics
  - China: 145% growth between 2011 and 2015
Digital Advertising

• Introduction

- Non-targeted Advertising
- Contextual Advertising
- Demographic Advertising
- First Party Behavioral Advertising
- Third Party Behavioral Advertising
- ISP Behavioral Advertising

- Information
  - Name
  - Profession
  - Contact Details
  - Browsing History
  - Interests
  - Location
  - Demographics
  - Health
  - Religion
  - Financial
  - IP Address
First Party Behavioral Advertising

- Website content becomes relevant to use of website
- Customers also looked at:

Online Electronics Dot Com

Website Owner
Digital Advertising

• Third Party Behavioral Advertising

• Other
  - Analytics
  - Ad Reporting
  - Ad Delivery
  - Retargeting

Prior website viewing becomes relevant to use of other websites
Behavioral Advertising on Mail Portals
Digital Advertising

- Behavioral Advertising on Social Media
  - 2007 Microsoft bought a 1.6% stake in Facebook, which valued it at $15 billion. Facebook had practically no revenue back then.
  - Facebook announced April 19, 2010 the roll out of its new “Like” function
  - Over 550 million users. And, after “Like” feature. Facebook's value shot to $50 billion in 2010.
  - Now, IPO estimated at $100 billion valuation.
Underlying Technology

• Cookies
• Flash Cookies
• HTML5 & eTags
• Unique Identifiers
• Other technologies
  – Log-in Profiling
  – GPS / Locations Based Services
• HTML5 & eTags

– HTML5
  • Local Storage
  • 5MB
  • Permanent

– eTags
  • HTTP Cache
  • HTTP Cookie Substitute
  • Undeletable
Underlying Technology

- Cookies
  - Persistent or Session
  - First Party or Third Party
  - Non-OBA uses
    - User Experience (Shopping Cart, Log In)
    - Google Analytics
• Flash Cookies

  – Flash Cookies v HTTP Cookies

  Flash Cookies Properties:
  Size: 100KB
  Expiry: Unlimited
  Location: Not browser

  HTTP Cookies Properties:
  Size: 4KB
  Expiry: Limited
  Location: Browser specific

  – Example

  Example:
  C:\Documents and Settings\rgraham\Application
  Data\Macromedia\Flash
  Player\#SharedObjects\XRSGNDYD\www.hulu.com\cram.swf

  – Flash Cookie Respawning
Underlying Technology

• Unique Identifiers

- Name
- Age
- Username
- E-mail address
- Nationality
- Mobile Number
- Facebook Account
- Twitter Account
- Online Status
- Gender
- Geo Location
- Application Use
- Application Shut Down
- Games Played
- Gaming Scores Achieved
- In-game Messages
What has prompted the interest in tracking?

- FTC Report: December 2010

Protecting Consumer Privacy in an Era of Rapid Change

A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS
What has prompted the interest in tracking?

- Do Not Track

**FTC Do Not Track Proposal:**

There should be a universal setting similar to a persistent cookie on a consumer’s browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements. To be effective, there must be an enforceable requirement that sites honor those choices.

Privacy By Design - Started in Canada (2005)

- Concept originally advocated in Canada in 2005. Canadian Information and Privacy Commissioner Ann Cavoukian big proponent of privacy by design. 2005, the 27th International Data Protection Commissioners Conference (Montreux Switzerland).
- 2005 Global Privacy Standard:
  - Consent
  - Accountability
  - Purposes
  - Collection Limitation
  - Use, Retention, Disclosure Limitation
  - Accuracy
  - Security
  - Openness
  - Access
  - Compliance
Privacy Principles Are Changing: New

  - The FTC report argues that the FTC’s current privacy models (the so-called “notice-and-choice” and “harm-based” approaches) insufficiently address evolving privacy issues.
  - The FTC report suggests a new framework, built around three core concepts: (1) Privacy by Design; (2) Simplification of consumer choice; and (3) Greater transparency
  - The FTC sought comments until February 28, 2011. 400+ comments.


- **March 16, 2011**, Testimony of Assistant Secretary of Commerce Lawrence E. Strickland presented to the U.S. Senate Committee on Commerce, Science and Transportation (“Strickland Testimony”) p.6. Administration called for national consumer data privacy legislation and FTC to enforce.
The FTC’s Enforcement Actions in 2011

• Enforcement Actions After Do Not Track
  
  - **June 2011 - In the Matter of Chitika, Inc.:** The FTC pursued Chitika for having an “opt out” for behavioral advertising that expired after ten (10) days – alleging this was a “deceptive” practice because the opt out was not meaningful. In its March 2011 Order, the FTC imposed notice and reporting requirements that will be in force for the next 20 years.
  
  - **August 2011 - United States of America, Plaintiff v. W3 Innovations, LLC, also d/b/a Broken Thumbs Apps:** The FTC pursued its first mobile app complaint, resulting in a consent decree against a mobile advertiser that served targeted ads to children under the age of 13 in violation of the Children’s Online Privacy Protection Act.
  
  - **November 8, 2011 – In The Matter of Scanscout Inc.** The FTC entered into issued a consent order against a digital third party advertiser for its alleged use of flash cookies to target advertising.
  
Quantcast and Clearspring Flash Cookie Class Action Settlement: Defendants agreed to settle both class action lawsuits alleging they violated people’s online privacy by using Flash cookies to track their information. The $2.4 million settlement consists of payments to plaintiffs’ counsel (up to 25% of the settlement amount and no direct payment to class members). Individual class members will not receive direct compensation. Out of the $2.4 million fund, all attorneys’ fees, costs, any enhanced awards to the named Plaintiffs, settlement administration costs, and notice and administration costs will be paid as provided for under the Settlement Agreement. See, Plaintiff’s Motion for Final Approval [Dkt 53, 2:08-cv-05948, filed 4/20/11]
Tracking, Behavioral Advertising Class Actions: Summary of the Claims and Motions to Dismiss

Dominique Shelton
Edwards Wildman Palmer LLP

- Plaintiffs filed class action against ABC, MTV Networks, NBC Universal and Quantcast for use of flash cookies on plaintiffs’ websites to track consumer behavior.

COMPLAINT FOR:

1. Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

2. Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2510;

3. Violation of Video Privacy Protection Act, 18 U.S.C. § 2710;

4. Violation of California’s Computer Crime Law, Penal Code § 502;

5. Violation of California’s Invasion Of Privacy Act, California Penal Code § 630;

6. Violation of UCL, Bus & Prof Code § 17200;

7. Violation of CLRA;

8. Unjust Enrichment
IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

JEFFREY PACILLI, SAIMA MIAN,
AMANDEEP SINGH, and MARILYN
ROBLEDO, individually and on behalf
of all others similarly situated,

Plaintiffs,

v.

CARRIER IQ, INC., AT&T INC., SPRINT
NEXTEL CORPORATION, T-MOBILE
USA, INC., HTC AMERICA, INC.,
APPLE, INC., SAMSUNG
ELECTRONICS AMERICA, INC.,
SAMSUNG TELECOMMUNICATIONS
AMERICA, LLC, and MOTOROLA
MOBILITY, INC.,

Defendants.

Civil Action No. _______________________

Jury Demand

CLASS COMPLAINT FOR:

1. Violation of Federal Wiretap Act,
   18 U.S.C. § 2511 AND

2. Violation of Stored Electronic Communication
   Act, 18 U.S.C. § 2701; AND

3. Violation of Federal Computer Fraud and Abuse
   Act, 18 U.S.C. § 1030
I. Harm
   A. Article III Standing
   B. Economic Loss under the ECPA.

II. Consent
   A. Privacy Policy
   B. Terms of Use
   C. Hyper Notice
This MDL is comprised of five separate class actions filed in 2010. Apple is included because the App Store approval process allegedly makes the company an "aider and abetter" to the deceptive practices of these applications.

Plaintiffs claim that “The information collected included but was not limited to: a Plaintiff’s precise home and workplace locations and current whereabouts; unique device identifier (UDID) assigned to Plaintiff’s iDevice; personal name assigned to the device (e.g., “Beth’s Phone”); Plaintiff’s gender, age, zip code, and time zone; as well as App-specific activity such as which functions Plaintiff performed on the App; search terms entered; and selections of movies, songs, restaurants or even versions of the Bible” (Dkt. 25, FAC at ¶ 2)
Class Action Claims Asserted (11/22/11)

Scott A. Kamber (pro hac vice)
skamber@kamberlaw.com
David A. Stampley (pro hac vice)
dstampley@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 202-6364
Interim Class Counsel

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE IPHONE APPLICATION LITIG.

CASE NO. 5:11-MD-02250-LHK
JURY DEMAND
FIRST AMENDED, CONSOLIDATED CLASS
ACTION COMPLAINT FOR VIOLATIONS OF:
1. STORED COMMUNICATIONS ACT,
   18 U.S.C. § 2701;
2. ELECTRONIC COMMUNICATIONS
   PRIVACY ACT, 18 U.S.C. § 2510;
3. CALIFORNIA CONSTITUTION, RIGHT TO
   PRIVACY, ART. I, SEC. 1;
4. NEGLIGENCE;
5. COMPUTER FRAUD AND ABUSE ACT,
   18 U.S.C. § 1030;
6. TRESPASS;
7. CONSUMERS LEGAL REMEDIES ACT,
   CAL. CIV. CODE § 1750;
8. UNFAIR COMPEITITION LAW, CAL. BUS. & PROF. CODE § 17200;
9. CONVERSION; and
10. COMMON counts, ASSUMPSIT, AND
    UNJUST ENRICHMENT/RESTITUTION
Harm Defense: Article III cases

- **In re iPhone/ iPad App. Consumer Privacy Litigation, 5:11-md-02250, Order Dkt. 8 (Sept. 20, 2011).**
  - Action dismissed without prejudice on September 20, 2011.
  - In so ruling, court noted that the *In re iPhone* plaintiffs did not “[I]dentify what iDevices they used,...identify which defendant (if any) accessed or tracked their personal information, d[id] not identify which apps they downloaded that access/track their personal information, and do not identify what harm (if any) resulted from the access or tracking of their personal information.
  - Amended complaint filed on November 22, 2011.
Harm Defense: Article III cases

• **In re Facebook Privacy Litigation** (N.D. Cal.)
  - Several individual class actions were consolidated into one MDL action. Plaintiffs contend that if a person knows the user ID number or "username" of an individual who is a user of Defendant's website, that person can see the user's profile and see the user's real name, gender, picture, and other information.
  - Defendants brought a motion to dismiss on the grounds that plaintiffs had failed to show injury or harm, among other things. The plaintiffs argued that the statutory violations of privacy constituted harm. On May 12, 2011, Judge Ware disagreed, dismissing the plaintiffs' ECPA claims with leave to amend.
  - Case was dismissed with prejudice on November 22, 2011.

• **In re Zynga Games Privacy Litigation**
  - Same as Facebook claims. Dismissed on 11/22/2011.
• *Genevive La Court v. Specific Media, SACV-10-1256-JW* (C.D.Cal. Apr. 28, 2011). (Successful defense example)

- Plaintiffs accused an online third-party ad network, Specific Media, of installing cookies on their computers to circumvent user privacy controls and to track Internet use without user knowledge or consent.

- The court held that plaintiffs lacked Article III standing because: (1) they had not alleged that any named plaintiff was actually harmed by defendant’s alleged conduct; and (2) they had not alleged any “particularized example” of economic injury or harm to their computers, but instead offered only abstract concepts, such as “opportunity costs,” “value-for-value exchanges,” “consumer choice” and “diminished performance.”

- Cable One, a division of the Washington Post, is an Internet Service Provider ("ISP"). On November 9, 2010, Green was deposed. He testified that he accessed his Cable One account exclusively from his home in Alabama. This admission proved fatal. Cable One's records revealed that Green's Internet subscription had been canceled one day before the NebuAd ad contract went into effect. Accordingly, Cable One filed a motion to dismiss on the ground that Green lacked Article III standing, and the Northern District of Alabama agreed. Case dismissed 2/23/2011.
Harm Defense: No Economic Loss under the CFAA

**Mortensen v. Bresnan Communications LLC LLC, 1:10-cv-00013 (D. Montana).**

- The Mortensen plaintiffs alleged that from early 2008 through June of 2008, Defendant Bresnan Communications ("Bresnan") diverted substantially all of the plaintiffs’ Internet communications to third party advertiser NebuAd. Plaintiffs also alleged that Bresnan modified its network to permit NebuAd to Install its “appliance” which gathered information to create profiles for interest based ads.

- Bresnan argued that plaintiffs’ CFAA claim could not be maintained because harm allegations were insufficiently pled for the CFAA. Court disagreed “… because defendants caused identical cookies to be placed on plaintiffs computers, unbeknownst to them.” *Id.* at 17.
Harm Defense: No Economic Loss under the CFAA

♦ **Bose v. Interclick** (Case No. 1:10-cv-09183-[ ] 8/17/2011)

♦ **Interclick** is an ad network facing a class action lawsuit over “history sniffing,” re-spawning flash cookies and hidden code to monitor online users and serve OBA.

♦ Plaintiffs also sued Advertisers (McDonalds, Microsoft, CBS, Mazda)

♦ **Claims:** CFAA, NY Deceptive Bus Practices, Trespass, Breach of Implied Contract; Tortious Interference w/ Contract
  - Contract-related claims based on website privacy policies on publisher sites where ads appeared

♦ MTD granted. CFAA dismissed b/c no quantification of $ damages and collecting consumer demographic info not $ injury (follows 4/11 Specific Media ruling). Advertising Defendants dismissed with prejudice. Case proceeds on state law grounds against Interclick.
• **Bose v. Interclick** (continued)
  - The court also stated that plaintiff Bose's “failure to meet the $5,000 threshold under the CFAA is not, as Defendants argue, necessarily fatal to Bose’s attempt to assert” federal jurisdiction under the Class Action Fairness Act. “Damages under the CFAA are narrowly defined,” the court wrote, and class members “may be entitled to damages under state law that are not cognizable under the CFAA.” Dkt., 36 at p. 17-18.
  - The court went on to deny motions to dismiss the plaintiffs’ state law claims for unfair business practices under New York Gen. Law 349 and trespass to chattel against Interclick, the advertising network, but found that the plaintiff failed to make specific allegations to sustain state law claims against the advertiser defendants (e.g., McDonalds and Mazda).
Arkansas State Computer Trespass Cases (December 30, 2010 - January 10, 2011)

- 17 consumer class actions
  - McDonalds
  - Nordstroms
  - Reebok
  - TV Guide
  - E-Trade
- Flash cookies
- State law
- Removal Barriers:
  - Under jurisdictional limits for CAFA and diversity
- Privacy Policy, TOU issues
  - Mandatory arbitration
  - Notice and consent
  - Class certification

1st MTD
- No harm
- Leave to amend

TV Guide case dismissed January 3, 2012; Pandora and Mattel (jurisdictional grounds requiring all legal actions to be brought in Los Angeles state or federal courts)
Consent as a defense

To prevail on Federal Wire Tap Act claims, the plaintiffs in the Carrier IQ cases must demonstrate that the defendants (1) intentionally (2) intercepted or endeavored to intercept (3) the contents (4) of an electronic communication (5) using a device. 18 U.S.C. § 2511(3)(a).

Under the wiretap act, a provider may divulge the contents of a communication “with the lawful consent of the originator or any addressee or intended recipient of such communication.” Id. §§ 2511(3)(b)(ii), 2702(b)(3).

Similarly, consent is a defense under the Stored Communications Act and the CFAA.
• *In re Facebook Privacy Litigation*
  
  – The court dismissed (with prejudice) claims under the Wiretap Act and the Stored Communications Act on the grounds that (a) Facebook’s privacy policy disclosed tracking; and (b) the plaintiffs addressed their communications to either Facebook to deliver to the advertisers, or directly to the advertisers. Either way, consent was present.
In a motion to dismiss, Bresnan contended that notice/consent was provided through:

- (1) Bresnan Communications Online Privacy Notice; (2) Bresnan's Online Subscriber Agreement and (3) an email notice to users that the NebuAd test was taking place which also contained instructions for users to opt-out.

- The Bresnan documents asked users to: “[A]cknowledge and agree… Bresnan... and its agents shall have the right to monitor ... postings and transmissions, including without limitation ... web space content”

- Bresnan documents notified "subscribers that Bresnan's 'equipment automatically collects information on your use of the Service including information on ... the programs and web sites you review or services you order, the time ... you ... view [them, and] other information about your 'electronic browsing"
The Bresnan privacy disclosures asked users to “acknowledge [ ] and agree[ ] Bresnan [ ] and its agents shall have the right to monitor ... postings and transmissions, including without limitation ... web space content.”

The disclosure notified “subscribers that Bresnan’s ‘equipment automatically collects information on your use of the Service including information on ... the programs and web sites you review or services you order, the time [ ]you ... view them, and..other information about your ‘electronic browsing.’” Id.

In addition, users were told that “Bresnan, its partners, affiliates and advertisers may use cookies, and/or small bits of code called ‘one pixel gifs’ or ‘clear gifs’ to make cookies more effective.”

Dismissing the ECPA claim, the district court found that, because of these disclosures, “Plaintiffs did know of the interception and through their continued use of Bresnan’s Internet Service, they gave or acquiesced their consent to such interception.” Order, Dkt. 30 at p. 12 (Dec. 13, 2010)
Consent as a defense
(not for CFAA claim)

• Bresnan’s challenges to the plaintiffs’ CFAA claims met with less success. To maintain a claim under the CFAA, 18 U.S.C. § 1030(a), plaintiffs must show that the defendant: (1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, (3) obtained or altered information, (4) from a protected computer, (5) that resulted in damage to one or more persons during any one-year period aggregating at least $5,000.

• For purposes of ruling on a Rule 12(b)(6) motion in the context of the CFAA, the court held that the disclosures were not sufficient to form consent for alteration of a consumer’s privacy settings. Order, Dkt. 30 at p. 19-20.

  – Current status: Bresnan brought a motion to compel arbitration that was denied (before ATT v. Concepcion). After rulings on motions to dismiss Bresnan brought a motion to reconsider the denial of motion to compel arbitration. On September 16, 2011 (Dkt. 48) the Court denied the motion on grounds the subscriber agreement was a contract of adhesion. Decision on appeal.
More Class Actions in 2011-2012:

♦ Enter the Class Action Bar – Privacy Litigation Targeted at Mobile.

♦ **Ringleader Digital mobile** - web advertising company sued in CDCA with a proposed class action lawsuit over its use of HTML5 to track iPhone and iPad users across a number of websites in 1st privacy tracking suit in the mobile space. 6/20/11 Confidential Settlement (not on a class basis).

♦ **Carrier IQ Litigation**. - Some **60** class actions have been filed in multiple jurisdictions (state and federal throughout the country).
  ♦ Unique because these are the first mobile tracking cases that *do not involve* serving targeted ads, but rather focus on the alleged tracking of user behavior.
  ♦ Exposure ECPA claims $10,000 per violation or $100 per day (whichever is greater for placing tracking software on 151,000,000 phone devices.)
Tracking, Behavioral Advertising: International Perspective and US Legislation

Dominique Shelton
Edwards Wildman Palmer LLP
Los Angeles
Regulatory Regime: EU

• Regulatory Compliance

- The Data Protection Directive
- The e-Privacy Directive
- Two Regimes

Fair Processing Information
Technical Storage of Information

Defining Consent
Opt-In?
Opt-Out?
The e-Privacy Directive: Technical Storage of Information

Article 5(3):

Member States shall ensure that the use of electronic communications networks to store or gain access to information, or to gain access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user to provide the service.
• Defining Consent?

- Data Protection Authorities
- Article 29 Working Party
- Internet Advertising Bureau Europe/European Advertising Standards Alliance
- Data Protection Legislation

No Agreed Solution
• Abroad

- EU and other country requirements are coming.
- Proposal to amend/repeal EU Data Protection Directive
- EU Draft Regulation to be published Jan. 28, 2012 (“EU Data Protection Day”),
  - Draft already disclosed
  - Needs to pass EU Parliament (perhaps 2 years); regulation would be effective immediately
  - Notification obligations included in Draft Regulation – within 24 hours.
  - Currently, notification to individuals and/or government agencies is required in some EU/EEA, but US leads the way in notice to affected individuals.
• Guidance on behavioral advertising was issued on December 6, 2011
  – OBA data will be considered personal information under PIPEDA
  – Notice and consent needed before tracking
  – Consent can be obtained through “opt-out”
  – No OBA from children.
Advertising Privacy and Data Security: Compliance
Self-regulatory Attempts: A US Example

Example: The “Power I” Icon
(Announced January 2010)

Many entertainment companies use the “Power I” icon. Many major companies running online ads will add the “Power I” icon, with small notes that say “Why did I get this ad?” When the icon is clicked, users will reach a page explaining how the advertiser used the consumer’s internet surfing history and demographic information to display an ad. The “Power I” Icon is the result of discussions between trade associations, major companies and the FTC. It is a direct response to the FTC’s calls for greater self-regulation and recent congressional interest in behavioral advertising. The purpose is (a) to notify consumers that online behavioral practices are followed on a particular web site; and (b) to provide opportunities for consumer choice.
DAA Disclosure and Opt-out

How it works:
• Privacy Policies and statements must be complete, accurate and up to date (best to reference cookies and all other tracking mechanisms)

• Privacy policy is not enough
  – Clear and conspicuous
  – Understandable
  – At point of collection
  – On ad

• Hyper notice (per IAB or FTC office actions)

• Terms of Use
  – No class relief
  – Arbitration clause
  – Concepcion v. ATT (*but see Bresnan* and California not following)

• Need an audit to confirm practices and find out what you need to disclose. Conduct audit through outside counsel to preserve work product privilege
• TCPA (47 U.S.C. Section 227 et seq.)

• CAN-SPAM (15 U.S. Sections 7701-7713)

• Overview: opt-in scheme for mobile; opt-out for e-mail

• Recent claims based on confirmatory texts from Twitter, Facebook, etc.: allege TCPA violation for text message confirming user didn’t want further text messages; Moss et al. v. Twitter et al. and Lo v. Facebook; both filed late April, Southern District of CA

• Hoang v. Reunion.com (settled): “Misleading” e-mail tool
Other Compliance Issues

• CA Shine the Light Act (CA Civil Code § 1798.83) compliance and class actions
  – Requirements
  – Conde Nast, Men’s Journal and Microsoft case
  – Statutory penalties

• CA Online Privacy Protection Act (CA Bus. & Prof. Code § 22575)

• Social media ads and rights of publicity
  – Fraley v. Facebook (N.D. CA 12/16/11)

• Third Party Platform Rules

• Advertising and related laws
  – Section 5 and state equivalents
  – Sweeps and contests
  – Endorsements and viral marketing

• UGC, CDA and DMCA
IV. SEC Data Breach and Security Risk Disclosure Guidance

What Are We Talking About?

- SEC CF Disclosure Guidance: Topic No. 2
  - October 13, 2011

- Division of Corporation Finance’s views regarding disclosure obligations relating to –
  - Cybersecurity risks
  - Cyber incidents

- Applies to public companies

- “Not a rule, regulation, or statement of the SEC,” but . . .
The SEC Guidance and Existing SEC Policy

- SEC regulations have long required that public companies report “material” events to their shareholders
  - Material events are developments or events which a reasonable investor would consider important to an investment decision

- The new Guidance seeks to clarify this reporting requirement with respect to cybersecurity

- Two aspects –
  - Disclosure of cybersecurity risks
  - Disclosure of specific cybersecurity incidents
“Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky”

This requires a risk assessment

- “We expect registrants to evaluate their cybersecurity risks”
• Identify all reasonably foreseeable internal and external threats
• Identify its vulnerabilities
• Assess likelihood that each threat with the ability to exploit vulnerabilities will actually do so
• Assess impact of such an event – i.e., evaluate the potential damage that will result
• Consider the adequacy of existing security measures
• Risk-based cybersecurity is also the Law
  – FTC, GLB, HIPAA, MA regs, OR statute, NJ draft regs, etc.
  – Deploying seemingly strong security isn’t enough
  – Security must respond to the risks
Nature of the Disclosure (1)

• “The cybersecurity risk disclosure --
  – “Must **adequately describe the nature of the material risks** and specify how each risk affects the registrant.”
  – Must be “**tailored to their particular circumstances.**”

• Companies –
  – “should not present risks that could apply to any issuer or any offering and
  – should **avoid generic risk factor disclosure**”
Appropriate disclosures may include:

- Discussion of **aspects of the registrant’s business** or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant **outsources** functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- **Description of known or threatened cyber incidents** experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- **Risks related to cyber incidents that may remain undetected for an extended period**; and
- **Description of relevant insurance coverage**.
Points of Note

• Disclosures are not limited to PII risks or incidents – **All corporate data is covered**

• “The federal securities laws **do not require disclosure that itself would compromise a registrant’s cybersecurity.**”
  – “Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence”

• Failure to address disclosed risks might be a violation of applicable state or federal data security law

• **Decisions not to disclose should be documented and justified** on the basis of the risk assessment
Where Disclosures May Be Required

- **Management’s Discussion and Analysis of Financial Condition and Results of Operations**
  - “if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant’s results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition”

- **Description of Business**
  - “If one or more cyber incidents materially affect a registrant’s products, services, relationships with customers or suppliers, or competitive conditions”

- **Legal Proceedings disclosure**
  - “If a material pending legal proceeding to which a registrant or any of its subsidiaries is a party involves a cyber incident”

- **Financial Statement disclosures**
  - “Cybersecurity risks and cyber incidents may have a broad impact on a registrant’s financial statements, depending on the nature and severity of the potential or actual incident”
Going Forward, Public Companies Should . . .

- Conduct regular and rigorous cybersecurity risk assessments

- Address the risks that are identified by –
  - Developing and implementing a responsive comprehensive data security program
  - Making appropriate disclosures to SEC of material risks
  - Developing an appropriate incident response plan

- Document and justify any decisions not to disclose risks where appropriate

- Work with both data security counsel and securities counsel to coordinate foregoing and make decisions regarding SEC disclosure filings
Practical Guidance

Managing Compliance

1. Audit
   - First Party
   - Third Party
   - Functionality

2. Website Terms of Use
   - Local Terms
   - Global Terms
   - Managing Consent

3. Privacy Policy
   - Fair Processing Information

4. Ad Agency Agreements
   - Risk Avoidance and Mitigation
     - Protocols
     - Policies
     - Procedures

5. ISP Agreements
   - Compliance with laws

Repeat
Insurance

• Insurance for this: Cyber/Privacy Risk
  – Companies should consider if they have coverage for
    • Consumer privacy claims/class actions
    • Governmental investigations
    • Indemnity obligations if indemnifying others for mobile or online targeted advertising campaigns
    • Penalties & fines

• Indemnity/insurance obligations from others
  – Companies should also consider obtaining indemnity from their vendors and request minimum insurance
Thank You & Questions

Dominique R. Shelton,
Partner
Edwards Wildman Palmer LLP
9665 Wilshire Blvd.,
Suite 200
Beverly Hills
CA 90212
+ 1 310 860 8705 (Direct)

dshelton@edwardswildman.com