Why Trademark Owners Need To Be Concerned About Privacy Law

May 15, 2012

Presented by:

Michael Ridgway Jones
Associate, Advanced Media & Technology Department,
Loeb & Loeb LLP

Nerissa Coyle McGinn
Senior Counsel, Advanced Media & Technology Department,
Loeb & Loeb LLP

LOEB & LOEB LLP

PRIVACY IN THE HEADLINES

May 8, 2012 4:54 PM PRINT

Myspace settles with FTC on privacy charges

By Chenda Ngak Topics Tech Talk

Operators of Virtual Worlds Fined $3M

Websites Illegally Collected and Disclosed Children's Personal Information

By Liz Crenshaw | Friday, May 13, 2011 | Updated 5:05 PM EDT

Italian court convicts 3 Google execs in video privacy case

Updated 2/24/2010 8:45 PM | Comments 22 | Recommend 5 E-mail | Print | RSS

Senate hearing on NebuAd, privacy set for tomorrow

July 8, 2008 — 6:19am ET | By Jim O'Neill

+1 0

MediaPost: NebuAd to pay $2.4m to settle class action #privacy lawsuit over #behavioral targeting technology. bit.ly/o5BQJA

Ask questions at any time using Q and A box. Download slides using green Resources button.

DATA SECURITY IN THE HEADLINES

News

TJX data breach: At 45.6M card numbers, it's the biggest ever

It eclipses the compromise in June 2005 at CardSystems Solutions

By Jaikumar Vijayan

March 29, 2007 12:00 PM ET 2 Comments + Briefcase What's this?

Heartland Breach Cost Company $12.6 Million So Far

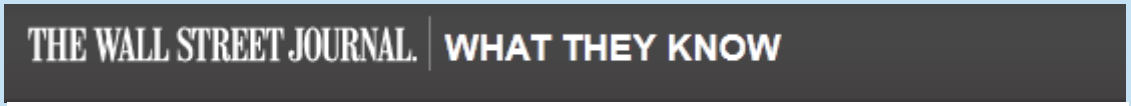
By Kim Zetter May 7, 2009 | 5:42 pm | Categories: Breaches

RockYou Settles Pending Charges for $250K Over Data Breach

By John P. Mello Jr., PCWorld Mar 27, 2012 3:30 PM

Ask questions at any time using Q and A box. Download slides using green Resources button.

MOBILE PRIVACY IN THE HEADLINES


THE WALL STREET JOURNAL. | WHAT THEY KNOW

WHAT THEY KNOW | December 17, 2010, 10:01 p.m. ET

Your Apps Are Watching You

A WSJ Investigation finds that iPhone and Android apps are breaching the privacy of smartphone users

Thursday, 15 March 2012 09:33

Follow us on Twitter and Facebook for the latest Class Action Settlement News!

Mobile App Makers Hit with Privacy Class Action Lawsuit

By Sarah Pierce

CNET › News › InSecurity Complex

Tech firms agree to privacy protections for mobile apps

In an effort led by California's attorney general, Apple, Google, Microsoft, and others have agreed to require developers to inform users about data usage policies before they download apps.

MMA Unveils Final Privacy Policy Guidelines for Mobile Apps

January 25, 2012 -- By **Michael** Like 0 Tweet 75 Share 3 Share 26

Ask questions at any time using Q and A box. Download slides using green Resources button.

WHY TRADEMARK OWNERS NEED TO BE CONCERNED ABOUT PRIVACY

- Privacy and data security affect virtually all companies and organizations, not just advertisers and e-tailers
- Many brands are early adopters of technology for advertising – such as mobile and social media – and these are two areas where brands need to be thinking about privacy and data security
- Privacy and data security breaches can result in brand damage
- Global brands need to understand privacy and data security laws around the world – and there are significant differences in different jurisdictions
- Costs of privacy mishaps and data security breaches can be significant

BIG BRAND INC. HYPOTHETICAL

- Big Brand.com website (and mobile-enabled website)
- Big Brand vendors/third-parties/affiliates
- Big Brand mobile applications:
  - Sponsored app
  - Product placement in an app
  - Location-based app (e.g., coupons delivered when user gets near a Big Brand store)
- Big Brand promotions directed to children
- Big Brand on social network sites
- Big Brand is successful in obtaining a new gTLD from ICANN (.bigbrand) and becomes a registry operator

OVERVIEW OF PRIVACY AND DATA SECURITY LAWS

US PRIVACY APPROACH

- US privacy laws typically follow the "notice and consent" approach:
  - Consumers must be provided with (1) notice of a company's privacy practices, and (2) 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 typically follow the "notice and consent" approach
- This means most companies have a privacy policy (even if not required by law)

THE FTC AND PRIVACY

- The FTC is the biggest US enforcer of privacy practices
- The FTC's main weapon is the FTC Act which prohibits unfair and deceptive acts or practices in commerce
- The FTC maintains that failing to comply with your privacy policy is a deceptive act or practice in violation of the FTC Act
- The FTC also enforces the Children's Online Privacy Protection Act (COPPA) and the COPPA Rule

THE FTC AND PRIVACY

- The FTC has initiated over 100 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 comply with the FTC COPPA Rule
  - Certifying compliance with the US-EU Safe Harbor Framework and failing to do so

YOUR PRIVACY POLICY

- Don't make promises in your privacy policy that you can't keep
- Make sure you understand 100% what data you, your website, your mobile apps, promotions such as sweepstakes, your vendors and affiliates are collecting, sharing, and/or disclosing
- Write a privacy policy that accurately describes your privacy practices
- Update as necessary:
  - Not just when new laws are enacted but also when you launch new promotions and/or new platforms that involve data collection
- Make sure technical mechanisms (such as opt-outs and toolbars) are working properly, as you have described them, and for as long as you say they will work

YOUR PRIVACY POLICY

In the FTC's 2012 Privacy Report, the FTC proposed a privacy framework (which should be seen as "best practices" according to the FTC):

- Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices
- There are some practices that do not require a company to provide a consumer with choice about data collection
- When a company is providing consumers with choice about data collection, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data
- Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes
- Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use

US LAWS, RULES, GUIDELINES, AND TERMS THAT MAY SHAPE WHAT YOUR PRIVACY POLICY SAYS

- State and federal laws:
  - Gramm-Leach-Bliley Act (GLB) (financial information)
  - Children's Online Privacy Protection Act (COPPA) (children)
  - Health Insurance and Portability Protection Act (HIPAA) (medical)
  - Massachusetts data security law
  - State security breach notification laws
  - California "Shine the Light" law and Online Privacy Protection Act
  - State laws limiting the disclosure of video rental and driver's license data
- Government agency rules, guidelines, white papers:
  - FTC's COPPA Rule
  - FTC's Safeguards Rule
  - Banking agency guidelines
  - White House Consumer Privacy Bill of Rights
  - FTC privacy reports
- Industry guidelines:
  - Digital Advertising Alliance guidelines for online behavioral advertising
  - Mobile Marketing Association guidelines and codes of conduct
  - Direct Marketing Association guidelines
- Third-party platform privacy policies (e.g., social media sites, mobile devices)

DATA SECURITY AND BREACH

- Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information

- Several federal bills have been introduced but none enacted:
  - For example, the Personal Data Privacy and Security Act of 2011 (S. 1151) would create a federal breach notification standard; would require companies to safeguard information; and would give individuals the ability to correct inaccurate information

- Class action litigation and government enforcement actions continue

EXAMPLE OF NEW TYPE OF DATA SECURITY 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 the 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

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

VENDORS, AFFILIATES, THIRD-PARTIES

- Review existing agreements, particularly with respect to changes in the law:
  - For example, Massachusetts' data security law may require substantive changes to agreements with vendors, affiliates and third-parties that process consumer data
- For agreements that are being negotiated, you need to know what your counter-parties are doing in terms of data collection, sharing and use

MOBILE

MOBILE INITIATIVES

- Creating a mobile app that promotes a product or a service
- Sponsoring a mobile app that appeals to a marketer's demographic
- Product placement in a mobile app
- Buying advertising that appears before a mobile app launches or after it terminates

Ask questions at any time using Q and A box. Download slides using green Resources button.

LOCATION-BASED ADVERTISING – WHAT IS IT?

- An advertisement, coupon, promotion or message that utilizes a user's location

- Examples include:
  - Providing a coupon that can be redeemed near the user's precise location or when the user enters a store
  - Traffic updates
  - Friend finder and check-in programs
  - Games
  - Personalized weather update
  - Location of nearest ATM

Ask questions at any time using Q and A box. Download slides using green Resources button.

MOBILE PRIVACY

- Privacy issues relating to mobile devices, location-based services, and mobile apps have been in the headlines more than any other privacy issue

- One problem is that some brands may not know what data is collected by their apps or location-based promotions

MOBILE PRIVACY

- California Attorney General "Joint Statement of Principles":
  - Agreement with mobile app market companies (Apple, Google, H-P, Microsoft, Amazon, RIM)
  - Mobile app must conspicuously post privacy policy
  - Access to policy through mobile platform's store
  - Process to report non-compliance
- MMA Mobile App Privacy Guidelines

WIRELESS ASSOCIATION'S LOCATION-BASED SERVICES (LBS) GUIDELINES

- LBS providers must provide notice describing how users' location information will be used, disclosed and protected, and how users can limit the use and sharing of such information
- Must obtain express consent before using location data
- Must describe what information is shared with third parties and what types of third parties receive information
- Must describe how users may terminate the LBS

COLLECTING DATA FROM CHILDREN

COLLECTING DATA FROM CHILDREN

- The Children's Online Privacy Protection Act (COPPA) applies to commercial web sites or online services, or any portion thereof, that are targeted to children under 13 or that knowingly collect information from children under 13

- COPPA requires:
  - Posting a privacy policy
  - Providing notice to parents
  - Getting verifiable parental consent
  - Providing access to information collected
  - Establishing procedures to safeguard children's' data
  - That a website not collect more personal information than necessary

FTC PROPOSED CHANGES TO COPPA

- **Changes to Key Definitions**: The FTC proposes updating the definition of "personal information" to include geolocation information and certain types of persistent identifiers such as tracking cookies used for behavioral advertising

- **Parental Notice**: The FTC proposes new requirements about the placement and content of parental notice such as more detail about the personal information already collected from the child, the purpose of the notification, the action that the parent can take, and how the information will be used

- **Parental Consent Mechanisms**: The FTC also proposes adding new methods to obtain verifiable parental consent, including electronic scans of signed parental consent forms, video-conferencing, and use of government-issued identification checked against a database

THE FTC AND COPPA

- In the FTC's first case involving mobile apps, the FTC announced that a mobile app developer agreed to pay $50,000 to settle FTC charges that it violated COPPA and the FTC's COPPA Rule
- The mobile app developer created and marketed mobile apps that allow users to play games and share information; several of the apps were targeted to children and were listed in the "Games-Kids" section of Apple's App Store
- The FTC charged that the developer used a number of the apps to collect and disclose the personal information of tens of thousands of children under 13 without first obtaining verifiable consent from their parents; for example, the apps encouraged children to email comments and blog postings to "Emily," a character featured in the apps, including "shout-outs" to friends and requests for advice
- As a result of these submissions, the defendants collected and stored thousands of email addresses from users of the apps
- The apps also permitted children to publicly post information, including personal information, to online discussion groups
- The FTC asserted that both practices violated its COPPA Rule, which requires the operators of websites to notify parents and obtain their consent before the collection, use or disclosure of children's personal information; according to the FTC, the apps also violated the COPPA Rule by failing to post clear, understandable and complete notice of their information collection practices

BIG BRAND ON SOCIAL NETWORK SITES

THIRD-PARTY PLATFORMS

- If Big Brand Inc. creates a page, profile or channel on a third-party platform, it will need to comply with that platform's privacy policy
- If Big Brand creates an app that runs on a third-party platform, that app may need its own privacy policy
- Big Brand Inc. should understand how various features and promotions with third-party platforms work
  - Several law suits were filed when brands partnered with social networking sites and the brands didn't understand the implications of disclosures of certain information through the social network

WHAT'S ON THE HORIZON

INTERNATIONAL ISSUES

- EU proposes overhaul of EU-wide privacy law
- EU Cookie Directive

WHITE HOUSE PRIVACY REPORT

- Feb. 2012 – proposes a Consumer Privacy Bill of Rights
- Convenes stakeholders and NTIA to create a set of sector-specific voluntary codes of conduct
- Wants new federal legislation that will be enforced by FTC
- Seeks to align US privacy approach more closely with international approach

CONSUMER PRIVACY BILL OF RIGHTS

- **Individual Control**: Consumers have a right to exercise control over what personal data organizations collect from them and how they use it
- **Transparency**: Consumers have a right to easily understandable information about privacy and security practices
- **Respect for Context**: Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data
- **Security**: Consumers have a right to secure and responsible handling of personal data
- **Access and Accuracy**: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate
- **Focused Collection:** Consumers have a right to reasonable limits on the personal data that companies collect and retain
- **Accountability**: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights

DO NOT TRACK BILLS INTRODUCED IN CONGRESS

- Do Not Track Me On-Line Act (H.R. 654) (Speier) – Requires the FTC to establish standards for an online opt-out mechanism that would allow consumers to effectively and easily "prohibit the collection of any covered information," including:
  - Online activity of the individual
  - Any unique or substantially unique identifier such as IP address
  - Name, postal address or other location information, e-mail address or user name, telephone or fax number, or government issued identification numbers
  - Financial account information
- Do Not Track Online Act of 2011 (S. 913) (Rockefeller):
  - Requires the FTC to prescribe regulations regarding the collection and use of personal information obtained by tracking the online activity of an individual and for other purposes
- Do Not Track Kids Act of 2011 (H.R. 1895) (Markey and Barton):
  - Expand the scope of services covered to include mobile applications
  - Expand definition of "personal information" to include IP addresses
  - Prohibition from using, disclosing or compiling personal information from minors for targeted marketing
  - For geolocation data for children under 13, parental consent would be required; for teens, express consent would be required
  - Digital Marketing Bill of Rights for teens
  - Eraser buttons if PII of under 18 year olds publicly available

MOBILE PRIVACY BILLS INTRODUCED IN CONGRESS

- Mobile Device Privacy Act (Markey):
  - Requires disclosure of monitoring software when consumer buys a phone
  - Requires consumer consent for manufacturers to collect and transmit information
- Location Privacy Protection Act (Franken and Blumenthal):
  - Attempts to close "loopholes" in current federal law allowing device manufacturers, app developers and telephone companies offering wireless internet service to freely share their consumer location information with third parties
  - Requires express consent from consumers before both collecting geolocation data and sharing it with third parties
- Geolocation Privacy and Surveillance Act (Wyden/Chaffetz):
  - Applies to both government (including law enforcement) and non-government entities.

GENERAL PRIVACY BILLS

- Financial Information Privacy Act (H.R. 653) (Speier) – Amends Gramm-Leach-Bliley Act to require that financial institutions obtain consumers' express Opt-In consent before disclosing non-public personal information to unaffiliated third parties; opt-out for affiliated third parties
- Best Practices Act (H.R. 611) (Rush):
  - Concise Privacy Policy
  - Require opt-in to disclose information to a third party
  - Safe harbor from Opt-In if participate in opt-out program operated by self-regulatory bodies
  - Ability to correct or amend personal information
  - Reasonable security features
  - No DO NOT Track mechanism
- Commercial Privacy Bill of Right Act of 2011 (Kerry/McCain) – The bill would require covered entities to:
  - Provide notice of their data collection practices and to disclose the purpose 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
  - Implement privacy protections throughout the life cycle of a product ("privacy by design")
- Consumer Privacy Protection Act of 2011 (Stearns/Matheson) – Requires covered entities to:
  - Develop clear and conspicuous Privacy Policy
  - Provide opt-out from the sale or disclosure for consideration of PII
- Data Accountability and Trust Act (H.R. 1701) (Rush):
  - Create a Federal Breach Notification standard
  - Authorize FTC to promulgate information security and data disposal regulations

ONLINE BEHAVIORAL ADVERTISING AND SELF-REGULATION

Digital Advertising Alliance

- OBA guidelines require:
  - Notice to consumers when behavioral information is collected or used
  - Opportunity to opt out of having tailored ads delivered
- Compliance monitored by BBB and DMA; both provide consumer complaint mechanism
- BBB announced 6 compliance actions in Nov. 2011
- DAA Multi-Site Guidelines

Network Advertising Initiative

- Issues annual compliance report, but does not name companies that are non-compliant
- No mechanism for consumer complaints

Ask questions at any time using Q and A box. Download slides using green Resources button.

ONLINE BEHAVIORAL ADVERTISING

- Digital Advertising Alliance (DAA) announced web browser companies will agree to comply when consumers use existing web browser features to opt-out of behavioral advertising
- DAA Managing Director said organization is working on mobile behavioral advertising guidelines
- DAA launched first phase of consumer education campaign
- Loeb's *Who Is Watching You? Updates in Online Behavioral Advertising and Privacy* webinar and related materials provide an in-depth look at these issues
  - www.loeb.com/obaprivacytargetingwebinar

ICANN, NEW gTLDS, AND BECOMING A REGISTRY OPERATOR

BECOMING A REGISTRY OPERATOR

COVENANTS OF REGISTRY OPERATORS

2.17 Personal Data. Registry Operator shall (i) notify each ICANN-accredited registrar that is a party to the registry-registrar agreement for the TLD of the purposes for which data about any identified or identifiable natural person ("Personal Data") submitted to Registry Operator by such registrar is collected and used under this Agreement or otherwise and the intended recipients (or categories of recipients) of such Personal Data, and (ii) require such registrar to obtain the consent of each registrant in the TLD for such collection and use of Personal Data. Registry Operator shall take reasonable steps to protect Personal Data collected from such registrar from loss, misuse, unauthorized disclosure, alteration or destruction. Registry Operator shall not use or authorize the use of Personal Data in a way that is incompatible with the notice provided to registrars.

THE WHOIS DATABASE

SPECIFICATION 4 - FOR REGISTRATION DATA PUBLICATION SERVICES

1. Registration Data Directory Services.
Until ICANN requires a different protocol, Registry Operator will operate a WHOIS service available via port 43 in accordance with RFC 3912, and a web-based Directory Service at <whois.nic.TLD> providing free public query-based access to at least the following elements in the following format. ICANN reserves the right to specify alternative formats and protocols, and upon such specification, the Registry Operator will implement such alternative specification as soon as reasonably practicable.

CONSUMER OFFERINGS USING A NEW gTLD

- There are many business plans that incorporate new gTLDs, some of which may raise privacy concerns:
  - For example, a brand that obtains a new gTLD can let consumers create their own webpage under that domain. Consumers may post material to those webpages that implicate privacy, children's privacy, right of publicity, and copyright concerns.

Why Trademark Owners Need To Be Concerned About Privacy Law

May 15, 2012

Q&A

Michael Ridgway Jones
mjones@loeb.com | 212.407.4042

Nerissa Coyle McGinn
nmcginn@loeb.com | 312.464.3130

LOEB & LOEB LLP