Mobile Apps for Companies: Navigating the Legal Landmines
Mitigating Privacy and IP Liability Exposure

THURSDAY, OCTOBER 10, 2013
1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today’s faculty features:
Aaron K. Tantleff, Senior Counsel, Foley & Lardner, Chicago

The audio portion of the conference may be accessed via the telephone or by using your computer’s speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact Customer Service at 1-800-926-7926 ext. 10.
Tips for Optimal Quality

Sound Quality
If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial 1-888-601-3873 and enter your PIN when prompted. Otherwise, please send us a chat or e-mail sound@straffordpub.com immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality
To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.
Continuing Education Credits

For CLE purposes, please let us know how many people are listening at your location by completing each of the following steps:

- In the chat box, type (1) your company name and (2) the number of attendees at your location
- Click the word balloon button to send
Mobile Apps for Companies: Navigating the Legal Landmines

Mitigating Privacy and IP Liability Exposures in Development, Launch and Management of Mobile Applications

October 10, 2013
Speakers

Aaron K. Tantleff, Esq.
Senior Counsel
IP / IT & Outsourcing
Foley & Lardner LLP
Tel: 312.832.4367
atantleff@foley.com
Agenda

- The "Big" Picture
- Trends
- Preliminary Issue/Risk Assessment
- Application Store T's and C's
- Application Development
- Third Party Proprietary Software
Agenda continued

- Open Source Software
- App EULAs
- Privacy Policies
- Related Agreements
- Mobile Application Security
- Trademark/Copyright Concerns and Enforcement Strategies
The "Big" Picture

- Traditional "brick and mortar" to high tech companies
- End users can be consumers, sales personnel, workers in the field, business partners
- Brochureware to back office system access to mobile payments
The "Big" Picture continued

- Leveraging popularity of smartphones and tablets
- Over a million mobile apps. Exponential growth expected.
- Global expenditure on mobile ads (search, display and messaging) in 2011 was US$5.3 billion, according to IAB and IHS Screen Digest (June 2012)
The "Big" Picture *continued*

- Mobile APP Development versus traditional software development
- Time to market is key
- The need to differentiate the app in the marketplace
- Value proposition
The "Big" Picture continued

- Mobile banking applications used for increased convenience and fraud prevention through proactive account management
  - banking activity is account activity monitoring
  - viewing bank statements
  - fund transfers
  - online bill payments
  - locating nearby ATMs or branches

- Opportunities to market to customer
Trends

- Location Based Services
  - Main enabler to deliver services based on context
    - location, personal preference, gender, age, profession, intention, etc.
  - LBS expected to reach 1.4 billion users by 2014
    - Gartner
  - Key component is context
  - LBS marketing
    - Ability to target individual and push customized ad
Social Networking
- Continues to be fastest growing mobile app category
- Portals, way points, cloud storage
- Linked with third parties
  - Open APIs
- Infrastructure provider
- Data warehouse
Trends continued

- HTML5 & Hybrid Apps
  - Developing native apps is costly & inefficient
  - Requires dedicated engineering teams per platform, project managers, and QA testers
  - Requires app store approval process
  - Ability to create one "universal" app

- Native Apps will remain as they offer richer experiences
Trends continued

- Mobile Apps will be a marketing strategy
  - Average user downloads over 100 apps
  - Need to create engaging mobile experience

- Mobile Coupons
  - Digital coupons represent 0.5% of distribution by 10% of redemption
Trends continued

- Personal Cloud
  - Ability to sync all devices and technologies across a personal cloud
  - Hardware becomes less important; services evolve

- Task Specific Apps
  - Users turn to specific apps to accomplish tasks
Trends continued

- **Purchase ability**
  - Apps will offer greater ability to shop and pay
  - Apps will also supplement traditional POS and enhance brick & mortar shopping experiences
  - Richer shopping experiences

- **Mobile & Big Data Converge**
  - Use of Big Data to enhance apps to anticipate and deliver products, services, assistance
Contextual Search

- Combine multiple data sources to deliver better search results and allow users to take further action
- Placing orders; purchasing tickets; service requests
Changing Roles

- "Every company is a software company"
- "Rogue" or "shadow" IT
  - From sole-source provider to strategic advisor of software
- Use of Big Data to drive engagement
- Development / Update Cycle
- Testing
Preliminary Risk Assessment

- Audience for app
- Criticality to business
- Associated online services
- Types of data collected
  - Personal data
  - Geolocation
- Regulated industry
- Potential patent issues
App Security

- Mobile devices not in owner's custody all time
  - Lost / stolen
  - Untrusted party to access company data

- All apps, even in-house developed apps may result in security violations
  - Apps should have application layer security
  - Review apps for malware
  - Limit ability to download apps
  - Rushed to market / side-step process / procedure
App Security continued

- Apps Store Sensitive Data on Device
  - Sensitive data should be stored on serve-side
  - Any data / information on device should involve careful consideration

- Review Log Files
  - Rarely done, but most attacks could be prevented or stopped if regular review of log files
  - Do various data points match (login files)
App Security continued

- Data Protection
  - Regulatory compliance
  - Competitive advantage
  - Must understand how data life cycle
  - Restrictions on access, transmission & method
  - Layering of protections
    - Deep content inspection; anti-malware; firewalls; intrusion detection; intrusion prevention
App Security *continued*

- **Users**
  - Who and where?
    - Vendors, default accounts, former user accounts
  - No generic, default or shared accounts
  - Periodic review of accounts
  - Complex passwords
  - Two factor authentication (password and device)
  - Biometrics?
App Security *continued*

- **Education / Training**
  - Commit malicious acts & "harmless" acts

- **Know Your Device**
  - All devices should be registered
  - Patches
  - Risk
  - Need to be able to manage assets & patches
  - Network access control
App Security *continued*

- **Know Your OS**
  - Every OS has well documented vulnerabilities
  - Known built-in features (e.g., iOS snapshots)

- **Third Party Apps**
  - Sync information from one app through another

- **Rooted Devices**
  - Allows unfettered access to file system
  - Download untrusted applications

- **App Stores**
  - Blind trust / lack of due diligence
Issued revised booklet on supervising technology vendors
- regulators' authority to oversee third-party vendors with contractual agreements with banks

A "financial institution's board of directors and management has the ultimate responsibility for ensuring outsourced activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations"
Most circumstances, mobile apps use cloud computing (BaaS)

FFIEC Information Technology Subcommittee considers cloud computing to be outsourcing

- the FFIEC agencies "consider cloud computing to be another form of outsourcing with the same basic risk characteristics and risk management requirements as traditional forms of outsourcing."
- "may require more robust controls due to the nature of the service."
FFIEC: Outsourced Cloud Computing (*statement*)

- Due diligence
- Vendor management
- Audit
- Information Security
- Legal
- Regulatory
- Reputation
- Business Continuity
Application Stores

- Approval period can be lengthy and unpredictable
- Unique requirements for each store/OS
- Developer agreements can be convoluted, unclear, extremely one-sided, and involve multiple documents.
- In-App purchase fee-split
Application Development

- Compare with "traditional" development
- Back office integration
- Interfacing with inventory control and other systems
- Order Fulfillment integration
- App development – generally by more than one vendor. Frequently involving offshore developers.
Third Party Proprietary Software

- Identify early
- Understand license and other contractual limitations
- Data collection rights
- IP indemnity is key
- Beware embedded open source
Open Source Software

- Viral licenses
- Placing proprietary software at risk
- No warranties
- No indemnities
- No support
App EULAs

- Identify relevant app stores
- Don't rely on default EULAs for app stores
- Ensure required app store terms are included
- Strictly limit liability and disclaim warranties
- Are associated online services involved?
  - Link to online services with related terms.
- Link to privacy policy
Privacy Policy

- When is a policy needed?
- State laws requiring policies (e.g., CA).
- Reference policy in EULA
- Ensure the policy accounts for all contemplated uses of data
"Although app developers want to provide new and innovative services, the apps may have significant risks to the private life and reputation of users of smart devices if they do not comply with EU data-protection law,"

– Joint opinion of EU's 27 data protection watchdogs, statement on the Irish Data Protection Commissioner's website
EU - Data Privacy

- Users "must be in control of their own personal data"
- Developer have "a set of important responsibilities to create a safe, secure and data-protection-compliant app environment,"
  – Article 29 Data Protection Working Party
29 Working Party

- Opinion on privacy risks of mobile apps
  - App targeted to app users within the European Union
  - Provide comprehensive information before any processing takes place
  - Collect prior, free, specific and informed consent
  - Enhance security measures
  - Protect children by adopting a more restrictive approach
  - Mobile apps players be aware of their own responsibilities and cooperate with each other
February 1, 2013, the FTC issued a new report, *Mobile Privacy Disclosures: Building Trust Through Transparency*

- Recommendations for best practices for key players in the mobile "ecosystem"
  - mobile platforms, app developers, advertising networks, and other third parties such as analytics companies that collect and use data from mobile apps
- 3 key areas
  - enforcement, outreach and policy initiatives
Potential Related Agreements

- Bundling agreements with carriers and device distributors.
- Joint marketing agreements with carriers, device distributors, resellers, and app stores.
- Social Media Integration and Partnering Arrangements.
- Transaction Processing Agreements with credit card issuers.
Potential Related Agreements

- Rewards Programs
- Data Sharing Agreements (e.g., transaction data, demographics, etc.)
Use of company names, product and service names, logos, icons and copyrighted material (images, content, videos) in the names, icons, summaries and content of apps without consent.

- Financial institutions/banks were some of the first companies facing mobile app trademark infringement; infringing apps used bank's trademarks to allow customers that did not have their own apps to check their balances.
Trademark / Copyright

☐ Trademark
  – Use of unauthorized branding on substandard apps may lead to negative opinions and adversely affect the goodwill of the actual brand owner.

☐ Copyright
  – Decreased revenue streams (consumers may be able to download content for free).
  – Inferior copies or information may diminish and tarnish the actual brand owner's products and services.
Data Theft: an app that requests an individual's username and password and then allows the app developer to capture and store login details for future illegitimate use.

Data/Web Scraping: extracting information from the website to be used for future illegitimate use, such as developing a program that is identical to the brand owner's app.

Phishing: data theft is considered phishing when the app appears to be provided by the user's own bank, such that the user believes he/she is providing information to his/her actual bank.
Trademark Infringement

- Factors Evaluated
  - Likelihood of confusion
    - Dilution claim may be available for well known or famous marks

- Defenses
  - Fair use: app developers may be able to rely on a nominative fair use argument if they can prove that they are using marks to describe the ability of the app
  - Disclaimers: likely insufficient to remedy all likelihood of confusion issues
  - Comparative advertising
Copyright Infringement

- Can include requests for damages, profits, costs and attorney fees if developers knowingly include/use/link to unlicensed copyright materials (may also even rise to some criminal claims).
Enforcement Strategies

- Protect and enforce trademark, copyright and other rights just as you would normally (e.g., any other internet or brick/mortar context).
  - Diligent monitoring (most app marketplaces are available to be searched online)
    - Costly
    - Time consuming
    - Many elect to take action only after receiving a customer, employee or in house business inquiry/complaint
    - Consider monitoring quarterly or semi-annually (whatever periodic methodology may be practical)
    - Target specific app stores/platforms, e.g., Apple's App Store and the Android Market
    - Create internal tracking of apps, platforms and related issues
    - Engage third party service vendors (e.g., MarkMonitor and CSC)
Enforcement Strategies

- Take down notices: a notice with a take down request is sent to platform operator, which is typically followed by a (somewhat) prompt response and further followed by deactivation or a request for further information.

Bear in mind:

- The developer may continue to distribute or sell the app or other promotional goods related to the app.
- A deactivated app may still reside on a user's mobile device, such that the infringement continues to occur each time app is opened (even if it doesn’t work).
- Consumers who downloaded or paid for the app may become frustrated with brand owner because the app is now disabled.
- It is sometimes helpful to include developer's violations of platform's terms of use.
- Exercise caution as being overzealous may have negative effects.
Enforcement Strategies

- Consider contacting the developer (whose name and contact details may be available in app marketplace) prior to or concurrently with submitting a complaint through or notice letter to the platform operator.
  - Be mindful that the app developer may delay responding or may use false contact information.
- Consider including notices/statements to consumers in marketing materials to establish and publicize your actual app(s) and caution against the use of others.
- Review existing trademark registrations to consider whether scope of existing description of services covers potentially new uses.
- Consider protecting copyrightable materials/original works, e.g., photographs, writings and advertising images.
- Consider using digital tags/watermarks for any works posted online.
Enforcement Strategies

- Consider inviting developers to contribute to existing or contemplated apps (e.g., Coca-Cola recently had creators of fake Facebook pages contribute to the real one to boost its public image).

- Consider effects on public relations before taking action, depending on trademark/copyright concerns and ultimate goals, particularly any aggressive action as sending legal notices may backfire.

  Example: you may be more concerned about the app's use of a logo or icon, but not the name or content. In this scenario, it may be more efficient (and cost effective) to reach out to the developer directly to request a change, rather than to contact the platform operator, which could result in the deactivation of the app altogether and further result in a backlash from potential customers.
Selected References

- FFIEC IT Examination Handbook booklets

- FFIEC Information Technology Subcommittee – Outsourced Cloud Computing

- Press Release - Article 29 Working Party - Joint Opinion on Mobile Apps

- FTC report, Mobile Privacy Disclosures: Building Trust Through Transparency, February 1, 2013
  - http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf
Contact Info

Aaron K. Tantleff, Esq.
Senior Counsel
IT & Outsourcing
Foley & Lardner LLP
Tel: 312.832.4367
atantleff@foley.com