



Cashing In:

Overview of Legal and Privacy Issues with Mobile Payments

James Gatto Leader of the Social Media, Entertainment & Technology Team	Deb Thoren-Peden Leader of the Privacy, Data Security & Information Use Team
Cathie Meyer Privacy, Data Security & Information Use Team	Laurie Lynch Flick Social Media, Entertainment & Technology Team

June 12, 2012

Today's Agenda

- Introduction
- Select Legal Issues with Mobile Payments
 - Intellectual Property
 - Gambling/Lotteries/Contests/Sweepstakes
 - Virtual Currency Overview
- Mobile Payments
- Privacy Overview
 - California Online Privacy Protection Act
 - FTC
 - EU
 - FCC
- Q&A

How Big is Mobile/Virtual Currency?

- **Apple Alone**

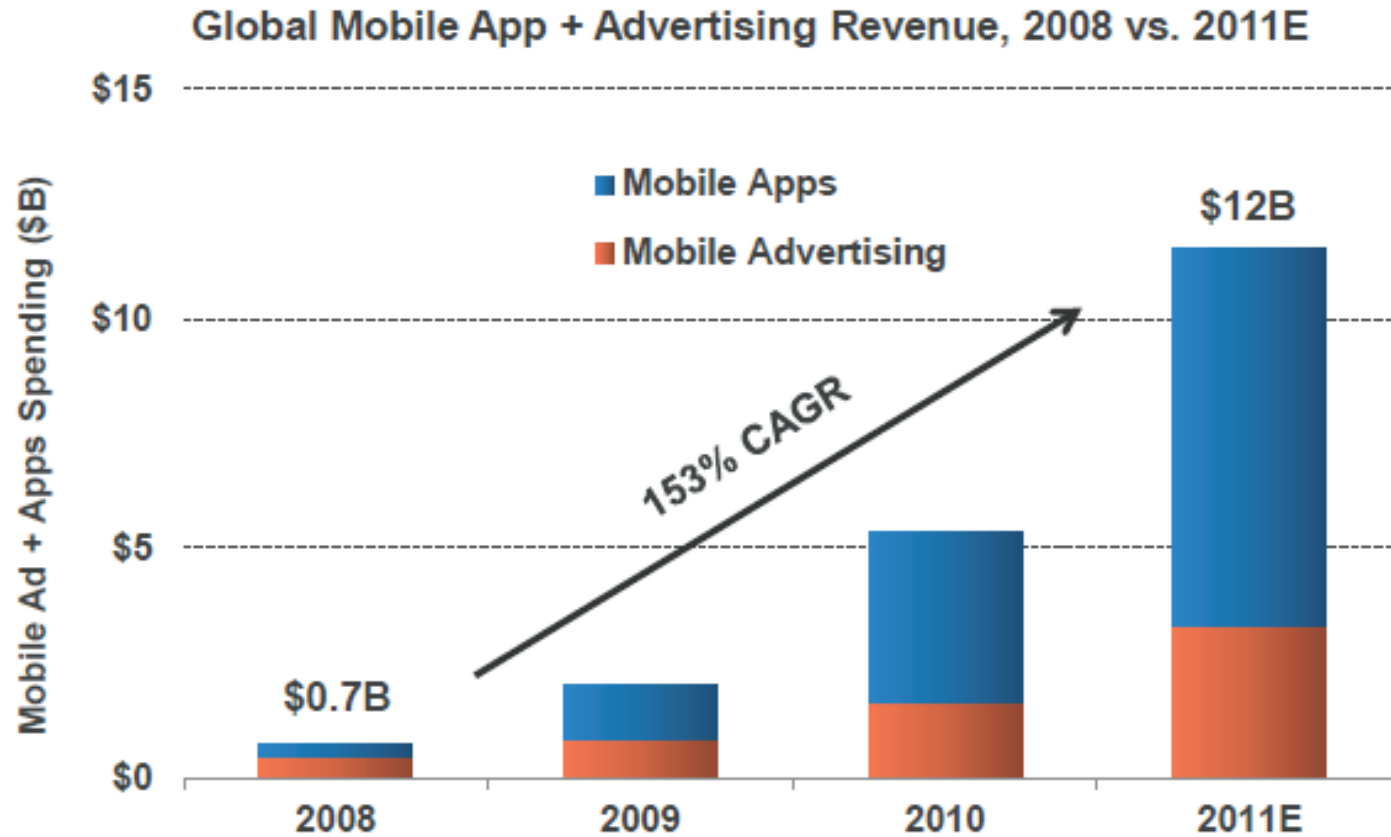
- Now more than 400 million accounts registered with its app store
- More than 30 billion apps downloaded
- Apple has written more than \$5 billion in checks to app developers

- **General**

- **GigaOm** - recent report found that over half of the top grossing apps in both Apple's App Store and Google's Android Market are freemium apps, and these are the apps that most frequently take advantage of virtual currency.
- Mobile analytics firm **Flurry** - more than two-thirds of mobile in-app purchases for games on iOS and Android go towards buying consumable items/virtual currencies
- **Juniper Research** - predicts that the amount of money being spent on virtual currency in mobile apps is going to more than double in the next four years, going from \$2.1bn last year to \$4.8bn by 2016.

Mobile Apps

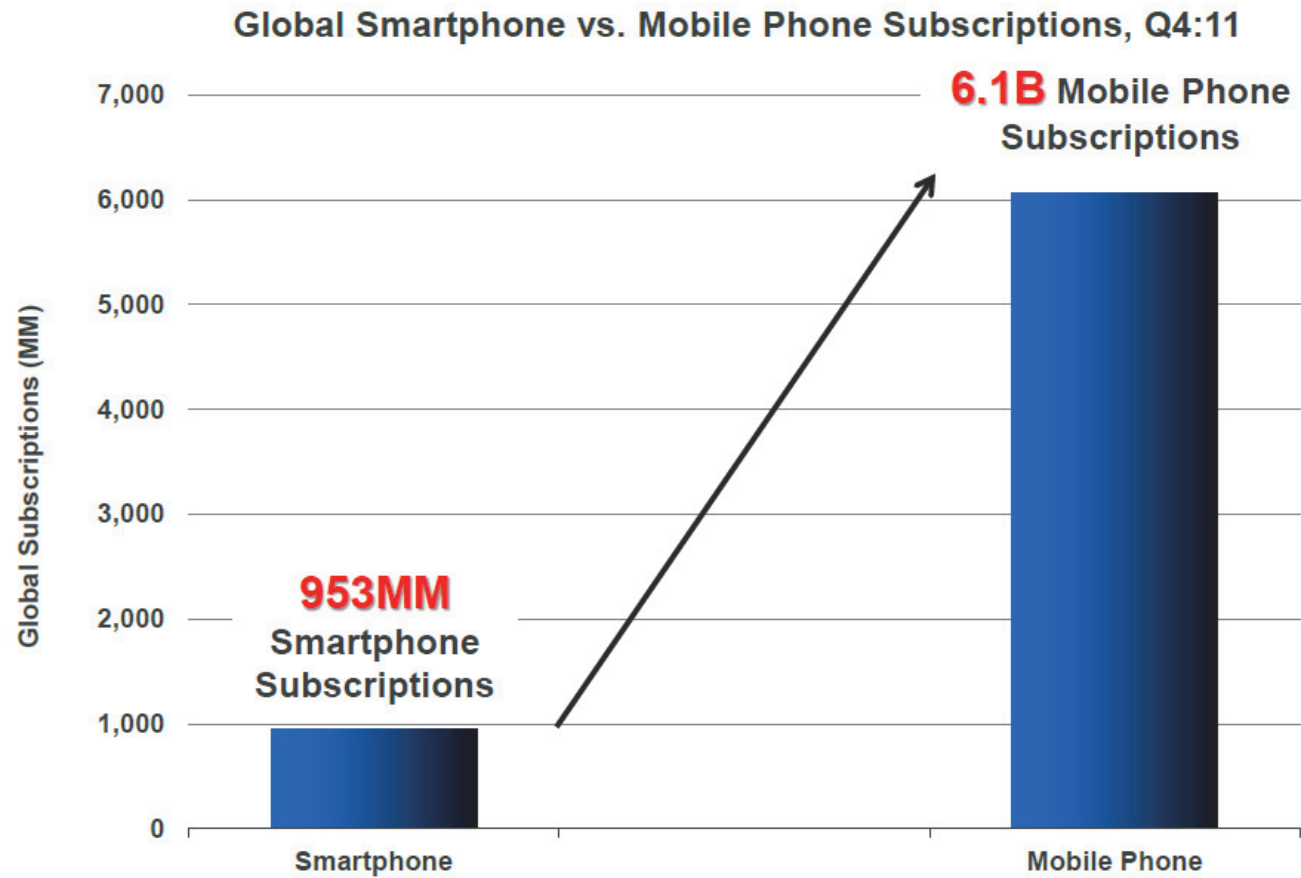
Mobile Monetization Growing Rapidly (71% Apps, 29% Ads)



Source: Internet Trends - D10 Conference – Mary Meeker

pillsbury

Smartphone: Still Huge Potential



Source: *Internet Trends - D10 Conference* – Mary Meeker



Real and Virtual Colliding



ZYNGA SERVE REWARDS NOW AVAILABLE IN FARMVILLE

SPEND \$25 OR MORE

- BOUQUET OF FLOWERS FOR YOUR HOUSEWARMING
- DINNER FROM THE GROCERY STORE
- YOUR LUGGAGE FEE AT THE AIRPORT
- A DOG WASH AT THE PET STORE
- TWO SUPER LOTTO TICKETS AT THE LOCAL CORNER STORE

GET FARM CASH TO BUY

- SOME LOVE PORTION
- 20 BABY BOTTLES
- A BUTTERCUP CHICKEN
- A LOBSTER
- A OURCING
- 5 TROPICAL CUPS
- AN ADVENTURE VACATION
- A SCURA GHONE
- 2 DOG TOYS
- 7 FOOD TREATS
- 3 TOY BONES
- A WATER BOWL
- PUPPY KIBBLES
- 25 SCRATCH AND WIN CARDS
- 20 BATTLE TICKETS

Farmville players earn Farm Cash with Serve® from American Express when they sign up for an account, add money, activate the prepaid card and use it for everyday purchases everywhere American Express® Cards are accepted.

serve **zynga**

American Express is teaming with Zynga on a reward program that will link offline spending on its Serve pre-paid cards to in-game rewards in Farmville - tying real-world spending to online virtual rewards.

pillsbury



INTELLECTUAL PROPERTY STRATEGY

IP Protection for Mobile Applications

- Patents have become incredibly necessary business tools
- Particularly relevant to mobile space
- Burgeoning patent market place – various factors
- Increase in number of law suits – trend will continue
- Many misconceptions about patents
- Quality Matters
- Need to focus on Offensive and Defensive Patent Strategy

Key Takeaway – critical to have a comprehensive patent strategy and work with someone who understands the space and the nuances of mobile patents

Patents For Mobile Industry

- Very misunderstood, under used for mobile applications (vs. devices)
- More valuable than most people think
- If you are doing something different than what you have seen others do and it has commercial value, consider patent protection
- Consult with a patent attorney who is knowledgeable in the field and who has handled patent applications, licensing, sales and litigation
 - Quality of patents vary widely
 - Some are worthless because of how they are handled – not because the ideas are not good or not patentable



Download: “IP Protection for Games”

www.pillsburylaw.com/socialmedia

Do it right or save your money and don't do it!

pillsbury

Some Examples



Apple was awarded a patent for a technique that sets financial transaction rules to control subsidiary financial accounts - could be used by a parent to set up a prepaid subsidiary account for a child or a by an employer setting up rules for a employee's payment account on a mobile device.

Starbucks (NSDQ: SBUX), Expedia and Capital One sued by Maxim Integrated, a California semiconductor company, over applications like "Starbucks for iPhone."





Gambling/Lotteries Contests/Sweepstakes

pillsbury

Gambling

- “Gamblification”
- Role of virtual currency
- Impact on payment processors

Gambling/Lotteries/Contests/Sweepstakes

- Most states define lotteries as having three general elements:

- 1) payment of some form of consideration;
- 2) a result determined by chance rather than skill; and
- 3) the award of a prize.

	Prize	Chance	Consideration
Lottery	X	X	X
Sweepstakes	X	X	
Contest	X		X

To avoid illegal lottery, need to carefully craft any sweepstakes, promotions or contests to not have all three of the above elements

Gambling

- Not all illegal lotteries constitute gambling
- Gambling typically requires a wager or bet - Staking or risking any thing of value on the outcome of a future contingent event over which the bettor does not have control with the understanding that he, or in some states anyone else, will receive something of value upon a specific occurrence.
- Mostly governed by state law



UIGEA

- The Wire Act
 - Recent DOJ interpretation – has paved way for states to permit online certain gambling
- UIGEA (Federal Gambling Law)
 - Primarily an Enforcement Mechanism – not substantive law
 - Focus on payment processors
 - Indictments against online poker/payment processors (some processors were duped into believing legitimate ecommerce transactions were involved)



VIRTUAL CURRENCY

What is Virtual Currency?

- **Virtual Currency**
 - “Currency”, points, vouchers and/or **other forms of stored value** used to purchase items (virtual goods, services, applications and real goods) or to access features
- Virtual Currency is an important and **often misunderstood** part of mobile payments



Select Legal Issues with Virtual Currencies

- Must Integrate Business and Legal Strategy
- Allowing users to buy, use and potentially redeem virtual currency raises a number of legal issues
- Must Strike a Balance
 - Maximize User Experience/Business Opportunities
 - Protect Assets and Users/Avoid Liability
- Leverage IP and TOS to maximize ability to go after unauthorized secondary markets.
- Regulatory Enforcements are Increasing!

More information: www.virtualworldlaw.com/virtual-currency



MOBILE PAYMENTS

Legal Landscape

- Mobile payments, virtual wallets, prepaid access, electronic payments and transfers, stored value gift cards, incentives, virtual currency
- All can be subject to federal and state laws: Bank Secrecy Act, PATRIOT Act, OFAC, CARD Act, etc.
- State laws too, including licensure (48 states)
- Applicable regardless of form, e.g., plastic, mobile wallet, digital, bar code, token, etc.
- Unclaimed property laws/limits on fees
- Privacy and many other laws too

Credit Card Accountability, Responsibility Disclosure Act of 2009 (CARD Act)

- Applies to gift cards, stored value, mall cards, open-loop prepaid, incentive, reward and promotional, most telcom, and virtual currency (limited exception).
- Imposed limits on fees, expiration dates, mandates disclosures
- Expanded consumer protections/ Regulation E

Prepaid Access Rules

- Issued by the Financial Crimes Enforcement Network (FinCEN) of the Department of the Treasury
- Part of the Bank Secrecy Act
- Makes "prepaid access" subject to BSA
- "Access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile id number or personal id number."
- Extends BSA information capture and verification and reporting and recordkeeping to "providers" and "sellers of prepaid access"; "providers must also register as an MSB with FinCEN."

Prepaid Access Rules (continued)

There are a few exceptions from being deemed a "provider" of prepaid access:

- limited types of closed loop prepaid access where no more than \$2,000 can be initially or subsequently loaded, used or withdrawn on a day, and:
 - they do not permit cash withdrawal (except as required by law),
 - may only be used for merchant goods and services at a defined merchant or location (such as a specific retailer or chain, college campus, subway system); and
 - do not permit transfer of value to 3rd parties.
- \$1,000 max value - initially or subsequently loaded used or withdrawn on any day, and:
 - international transfers of funds or value are not permitted;
 - transfers between used of prepaid value within a prepaid program are prohibited; and
 - loads of additional funds or source from a non-depository source are prohibited

Prepaid Access: “Sellers of Prepaid Access”

- Any person that receives funds or value for an initial or subsequent loading of prepaid access if that person: (1) sells prepaid access under a prepaid program that can be used before capture of extensive customer information (name, address, dob, SSN) and verification of same; or (2) sells prepaid access (including but not limited to closed loop) to funds that exceed \$10,000 to any person during any day and has not implemented policies and procedures reasonably adapted to prevent such a sale.
- A "Seller" must have a full AML program, comply with BSA filings (suspicious activity report filings, currency transaction, etc.)

New International Remittance Rules

- Effective Jan. 2013
- Apply to most any international remittance, wire or electronic payment from a consumer to an account in a foreign country.
- Small dollar transfers of \$15 or less exempt
- Imposes extensive pre-send disclosures and receipt disclosures (mobile too)
- Need to disclose all exchange rates and fees for the remittance through payout
- Consumers have the right to allege unauthorized or erroneous payment for up to 180 days
- Consumers have a right to stop the transaction for up to 30 minutes after initiated
- If you have agents, greater liability for wrongful acts of your agency

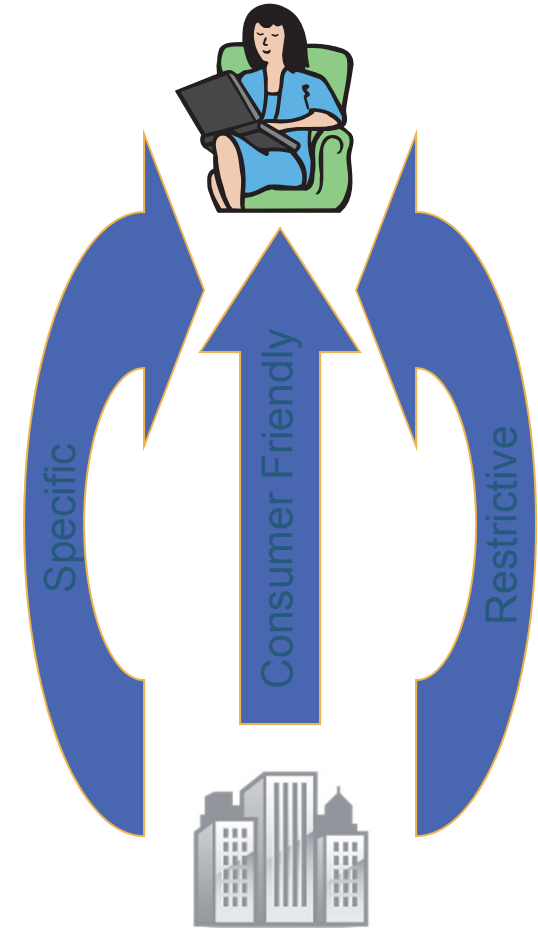


PRIVACY

pillsbury

Trends in Data Security Laws

- California started it (2003)
 - Online privacy policy
 - Duty to protect personal information
 - Notification of data security breach
 - Attorney General's settlement with Google and others over application privacy policies
- Massachusetts kicked it up a notch (2010)
 - Data Security Regulation Plan
 - Encryption of data on portable devices
 - Oversight of vendors
 - Mandatory risk assessment and training
- Europe – the “final” frontier?
 - 2012 EU Directive Revisions
 - No cookies without consent
 - Right to be forgotten
 - Geolocation, tracking and behavioral advertising



Privacy and Data Protection Triggers

- Personal information impacted
 - Name with Social Security Number, drivers license number, financial account number, medical information, passport number, date of birth, biometrics
- Collection
 - Customer information, cookies, check and credit card transactions
- Use
 - Marketing, behavioral advertising, violation of privacy policies
- Disclosure (intended or unintended)
 - Sharing, selling, unauthorized access or misuse, credit card number truncation
- Destruction or disposition
 - Records, equipment
- Imposition of state regulation on out-of-state business

Privacy Update - States

Obligations in various states:

- Data security (11 states)
- Data destruction (25 states)
- Social Security Number protection (27 states)
- Employee record retention
- Security breach notification (46 states + DC)
- Data collection restrictions
- Data use restrictions
- Massachusetts Regulation (Vendor certification deadline March 1, 2012)

Privacy Update - States

California Attorney General acts to enforce Online Privacy Protection Act

- Act requires posting of online privacy policy on any site that collects personally indefinable information
- Applies to any online collection source: Website or Application
- February 2012: Agreement reached with Amazon, Apple, Google, Hewlett-Packard, Microsoft and Research In Motion
- These platforms have agreed to privacy principles designed to bring the industry in line with a California law requiring mobile apps that collect personal information to have a privacy policy.
 - Includes educating app developers about their privacy obligations
 - Commitment to improve compliance with privacy laws through tools to report non-compliant apps
- This agreement will allow consumers the opportunity to review an app's privacy policy before they download the app rather than after, and will offer consumers a consistent location for an app's privacy policy on the application-download screen.
- Noncompliance with their stated privacy policies can result in prosecution under California's Unfair Competition Law and/or False Advertising Law.

Privacy Update - Federal

- White House Consumer Privacy Bill of Rights – February 2012
- FTC Final Report: Protecting Consumer Privacy – March 2012
- FCC Telemarketing Rules
- FTC Mobile Applications and Children

White House Consumer Privacy Bill of Rights

February 2012 the White House released its proposed Consumer Privacy Bill of Rights

- Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- Respect for Context: Consumers have a right to expect that companies 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 is 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.

FTC Final Consumer Privacy Report

- FTC's *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FTC Report (released March 2012),
- Provides a framework for protecting online privacy and best practices for companies that collect and use consumer data.
- Applies to all commercial entities that collect or use consumer data linkable to a specific consumer, computer or device unless the entity collects only nonsensitive data from fewer than 5,000 consumers a year and does not share the data with third parties.
- The baseline principles articulated in the framework are:
 - Privacy by Design. To promote consumer privacy throughout their organizations and at every stage of the development of their products and services.
 - Choice. To provide simplified consumer choice, recognizing that certain practices do not require choice where they are consistent with the context of their interaction with consumers.
 - Transparency. To increase companies' data practice transparency through shorter, clearer privacy notices, increased access to consumer data and education of consumers.

Mobile Marketing: Get Consent

Telephone Consumer Protection Act

47 U.S.C. § 227(b)(1)(A)(iii)

“ It shall be unlawful for any person within the United States, or any person outside the United States if the recipient is within the United States—

(A) to make any call (other than a call made for emergency purposes or made with the prior express consent of the called party) using any automatic telephone dialing system or an artificial or prerecorded voice—

. . . (iii) to any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other radio common carrier service, or any service for which the called party is charged for the call”

Mobile Marketing: TCPA Then and Now

- **2003:** FCC states that the TCPA's prohibition "encompasses both voice calls and text calls to wireless numbers including, for example, short message service (SMS) calls" *In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 18 FCC Rcd. 14014, 14115 (July 3, 2003)
- **2009:** Ninth Circuit holds that text messages are "calls" under the TCPA. *Satterfield v. Simon & Shuster* (9th Cir. 2009)

FTC Telemarketing Sales Rules on Robocalls and Texts

- FTC Amended the Telemarketing Sales Rule rules restricting prerecorded calls effective September 1, 2009.
- Prohibits telemarketers from making robocalls to consumers unless those consumers have agreed in writing to receive the calls.
- Extends to text messages sent using automated dialing mechanism
- Transmitting prerecorded messages/texts to consumers without their *prior written agreement* will face penalties of up to \$16,000 per call.
- Exceptions for some prerecorded calls that deliver purely “informational” messages, and calls from politicians, banks, telephone carriers, and most charitable organizations.

FCC's Revised RoboCall Rules

- FCC and FTC share jurisdiction over telemarketing
 - FCC has exclusive jurisdiction over common carriers, banks, credit unions, savings and loans, insurance companies, airlines and purely intrastate telemarketing calls
 - Do Not Call Implementation Act requires agency coordination and they have signed a Memorandum of Understanding on enforcement
- FCC amended its rules in February 2012 to more closely align them with the FTC's rules
- New rules published June 11, 2012 in the Federal Register
- New rules generally become effective July 11, 2012
- Several waiver/exemption requests remain pending

FCC Report on Location Based Services

- FCC has a joint task force with FTC on LBS
- Held a Forum in June 2011 and released report on May 25, 2012
- FCC notes that:
 - LBS developed as a carrier tool and is covered by FCC's CPNI rules
 - LBS has evolved to be an important part of the business model for device manufacturers and app developers
 - Some such entities may not have staff/knowledge to address privacy issues
 - Third party collection of location data may occur without carrier's involvement
- Report recommends further consideration of:
 - Ways to encourage privacy by design
 - Examination of the rights/duties of each player with respect to data security
 - Consideration of the timing and sufficiency of notice to consumer, opt out options
 - Whether to encourage collecting less data and storing for shorter periods

FCC Inquiry Into Data Stored on Mobile Devices

- On May 25, 2012, the FCC asked for comments regarding the protection of data stored on mobile communications devices
 - Comments and Replies due 30 and 45 days from Fed Reg publication, respectively
- Under FCC rules, wireless providers must protect Consumer Proprietary Network Information (CPNI) which includes:
 - quantity, technical configuration, type, destination, location and amount of use of telecommunications services
- Inquiry arises in part from:
 - concerns regarding software embedded on devices to collect information about performance of devices and of the provider's network
 - FCC's inquiry into Location Based Services
- Impacts device manufacturers, software designers, app developers

FCC Inquiry Into Data Stored on Mobile Devices

- Questions asked include:
 - Whether carriers' current practices raise privacy concerns
 - Whether consumers have meaningful notice and choice re: service provider's privacy policies
 - Whether privacy by design should apply to software designed for mobile devices
 - What role consumers should play in protecting their stored data
 - How the carrier's obligation to "take reasonable measures to discover and protect against attempts to gain unauthorized access" to consumers' information apply to data stored on devices
 - The role of third parties in collecting, hosting, analyzing and storing the data
 - Whether these obligations change depending on the extent to which a carrier is involved in design of operating systems, installation of pre-installed software, selling of devices

Recent FTC Focus on COPPA

Mobile Apps for Kids: Current Privacy Disclosures are DisAPPointing

- All members of the kids app ecosystem – the app stores, developers, and third parties providing services within the apps – should play an active role in providing key information to parents who download apps.
- Privacy and privacy disclosures have not kept pace with explosive app development.
- FTC Recommends:
 - App developers provide easy to find, easy to understand, simple, short disclosures or icons on the mobile device.
 - Disclosure to include information an app collects, how the information will be used, and with whom the information will be
 - Disclose if the app connects with any social media, or allows targeted advertising to occur through the app.
 - Third parties that collect user information through apps also should disclose their privacy practices, whether through a link on the app promotion page, the developers' disclosures, or another easily accessible method.
 - The app stores should provide a more consistent way for developers to display information regarding their app's data collection practices and interactive features using a designated space for disclosures and standardized icons to signal features, such as a connection with social media services.
- Released February 2012
- Available at: http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf

Recent Litigation: COPPA

- NJ v. 24x7digital, LLC
- Filed by AG Chiesa and NJ Division of Consumer Affairs, June 6, 2012 - U.S. District Court, District of New Jersey
- Defendant is mobile app developer Los Angeles-based 24x7digital, LLC, who developed and operates the “TeachMe” series of apps for the iPhone, iPad and iPod Touch.
- Educational games allegedly collect personal information from children, then transmit the information to a third-party company without notifying parents or obtaining their consent in violation of Children’s Online Privacy Protection Act (COPPA).
- Suit reflects Division’s ongoing initiative against Internet privacy violations and acts of cyber-fraud.

Recent Litigation: COPPA

- FTC settled with W3 Innovations, LLC, (dba Broken Thumbs Apps) September 2011
- US v. W3 Innovations, LLC (USDC N.D. Cal case #CV-11-03958-PSG)
- \$50,000 fine, deletion of all children's information and consent decree including compliance reporting and certification
- Company's mobile apps allow users to play games and share information online.
- Emily's Girl World, Emily's Dress Up, Emily's Dress Up & Shop, and Emily's Runway High Fashion, were directed to children and were listed in the Games-Kids section of Apple, Inc.'s App Store.
- Violations of COPPA included collecting and maintaining children's email addresses, allowing children to publicly post information, including personal information, on message boards all without parental knowledge or consent

Privacy Update – International

- **EU publishes proposed amendment to Data Protection Directive**
 - Next steps require agreement with Council (EU Member States) and European Parliament. Timing: 1-2 years with regulations coming into force 2 years thereafter
- **Aim is to harmonize EU data protection**
 - EU based companies will be supervised by the data protection authority of their Member State
 - Multinationals supervised by Member State of their main establishment
- **Highlights:**
 - New rules apply to non-EU based companies processing personal data if they offer EU residents goods or services or monitor their behavior
 - Consent clarified: explicit, clear, affirmative action required and cannot be relied on where there is a significant imbalance in status between individual and controller (including employers)
 - Specifically includes genetic data, children (under 18, under 13), IP Addresses
 - Right to be Forgotten
 - Privacy by Design
 - Processing contracts require more detail (German model)
 - Mandatory notification of DPA of data security breach and, when serious, to individuals
 - Data Protection Officer must be appointed by enterprises with 250+ employees

Privacy Update - International

- **Specific EU International Transfer Provisions:**
 - Relaxation for transfers contracts
 - No filing or approval required for model contracts
 - Creates uniformity across EU
 - Binding Corporate Rules
 - Procedures standardized
 - Strict deadlines
- **EU Sanctions**
 - DPA will have power to ban processing and suspend data flows
 - Administrative sanctions – fines up to 2% of world-wide turnover
- **June 7, 2012:**
 - Irish MEP Sean Kelly, who is a member of the European Parliament's Industry Committee, briefs the US General Counsel of the Commerce Department, Cameron Kerry, on the issue of online privacy. Washington is “very interested.”

Privacy Update - International

- Philippines Adopts EU Style Data Privacy Act
 - June 6, 2012: The Senate ratified report on the Data Privacy Act (Senate Bill No. 2965, passed March 20, 2012)
 - Act mandates protection and preservation of the integrity, security and confidentiality of personal data collected by public and private entities.
 - Act is based heavily on the EU Directive 95/46/EC and is at par with the Asia Pacific Economic Cooperation (APEC) Information Privacy Framework standards, Angara said.
 - A National Privacy Commission will be established under the Data Privacy Act to implement and enforce the regulations of the bill.



pillsbury

Contact Information and Additional Resources

<p>James Gatto Leader of the Social Media, Entertainment & Technology Team Tel: 703.770.7754 Email: james.gatto@pillsburylaw.com</p>	<p>Deb Thoren-Peden Leader of the Privacy, Data Security & Information Use Team Tel: 213.488.7320 Email: deborah.thorenpeden@pillsburylaw.com</p>
<p>Cathie Meyer Privacy, Data Security & Information Use Team Tel: 213.488.7362 Email: catherine.meyer@pillsburylaw.com</p>	<p>Laurie Lynch Flick Social Media, Entertainment & Technology Team Tel: 202.663.8166 Email: lauren.lynch.flick@pillsburylaw.com</p>

Check out our website and blogs:

www.pillsburylaw.com

www.virtualworldlaw.com

www.commlawcenter.com

The Pillsbury logo, consisting of the word "pillsbury" in a lowercase, sans-serif font. The letters are a dark red color. The 'i' in "pillsbury" has a distinctive dot.