Opening Remarks for Mobile Privacy Summit
Jessica Rich, Director, Bureau of Consumer Protection
October 23, 2013
Santa Monica, California

- Good morning. This is an exciting day. I'd like to thank the Application Developers Alliance for organizing this event and for inviting me to speak to all of you. I also want to thank Attorney General Harris and her staff, who are co-hosting this event and who are providing strong leadership on privacy issues in this state and nationwide.

- It's wonderful to be here to talk about privacy. Understanding and addressing the privacy issues raised by mobile apps is critical to the FTC's mission and to this nation's consumers.

- Indeed, app developers are one of our key constituencies because you are the creative engine behind many products that consumers increasingly integrate into their daily lives.

- You're also on the front lines in the battle to capture consumers' attention and communicate effectively and accurately with them in the smallest window of time and on the smallest screen.

- The FTC has been examining the privacy implications of mobile technologies for more than a decade. We've held workshops on issues like mobile payments and mobile privacy disclosures, issued reports and surveys, and, of course, brought law enforcement actions, including hundreds of privacy-related cases.

- We've also formed a Mobile Technology Unit to ensure that we have the resources and expertise to support the agency's work on mobile issues.

- One thing we believe is that privacy is extremely important to your growing and exciting industry. As we all know, the highly personal nature of mobile devices creates a unique ability to collect and share large quantities of personal

information that can reveal, for example, where a consumer is, where she's going, who she's communicating with, what she's buying, and even what she's worried about – *all day long*.

- At the same time, consumer awareness of privacy issues has increased steadily in recent years – whether because of the debates over online tracking, the explosive growth of social networks that allow consumers to set privacy preferences, or (most recently) the revelations about Edward Snowden and the NSA.

- Just as an example – a recent survey showed that 86% of consumers reported taking steps to remove or mask their digital footprints – steps ranging from avoiding use of their names to clearing cookies, and from encrypting email to using virtual networks that mask an IP address. Such actions by consumers are bound to grow as they become more sophisticated about technology and about available privacy tools.

- So I think we can all agree that getting privacy right is important to the mobile app industry and to developing the consumer trust that's needed for your businesses to flourish. I know I'm preaching to the choir, because that's why you're all here today, which is wonderful.

- My shorthand for all of this is the simple motto – *Expect Privacy*. Consumers want privacy protections and features to be incorporated in the products and services they use. And meeting their expectations builds consumer trust. We should all *Expect Privacy*.

<u>FTC Guidance</u>

- Recognizing that privacy is important to consumers and to the mobile app industry, the FTC has developed guidance and recommendations that focus on how to implement privacy and security in the mobile space. I'll briefly touch on the key materials we've developed, but urge you to go to our website for more details. It's open for business now, and we hope it stays that way.

- Our key documents are:

    - *Marketing Your Mobile App: Get it Right from the Start*
    - Our updated *Dot.Com Disclosures* guide
    - *FTC Staff's Report on Mobile Privacy Disclosures*
    - *Mobile App Developers: Start with Security*
    - And of course, all of our materials providing guidance on how to comply with the Children's Online Privacy Protection Act (COPPA)

- A recurring theme in all of this guidance is that the same principles apply to the mobile space – and to mobile apps – as apply in other media. But these materials are tailored to a mobile audience and, in some cases, app developers in particular. So we think you'll find them helpful.

- The first one, *Marketing Your Mobile App: Get it Right from the Start*, provides an overview of the key privacy and truth-in-advertising principles that app developers should keep in mind.

- Among other things, the guide urges mobile app developers to:
    - tell the truth about what your app can do
    - build privacy considerations into your app from the start, a concept known as "privacy by design"
    - be transparent about your data practices and honor your privacy promises
    - disclose key information clearly and conspicuously
    - comply with COPPA if your app is designed for kids under 13 or you know that you're collecting personal information from such kids
    - collect sensitive information only with consent, and
    - keep user data secure.

- Second, we recently updated our *Dot.Com Disclosures* guide. This piece isn't geared specifically to privacy or mobile apps but is intended to provide guidance on how to make effective disclosures generally – disclosures that may be required by law or necessary to avoid deception.

- One of primary reasons we updated the guide was to address how to make disclosures on mobile devices and on social networks since the original version of the guide was from, if you can believe it, 2000 – well before many of today's business models had emerged.

- The guide contains mockups showing how to make disclosures that are short but also "clear and conspicuous" – in texts and on Twitter, for example. Yes, it can be done!

- The third piece I'll mention is a staff report we did on mobile *privacy* disclosures in particular – called *Mobile Privacy Disclosures: Building Trust Through Transparency*. This report recommends best practices to platforms, app developers, ad networks, and others for disclosing their privacy practices to users. For app developers, it digs deeper into some of the privacy recommendations we made in the *Getting it Right* piece. It recommends that you:
    - have a privacy policy that is easily accessible,
    - provide just-in-time disclosures and obtain affirmative express consent before collecting and sharing sensitive information, to the extent that platforms haven't already done that. By just-in-time disclosures, we mean disclosures right at the point of collection and/or sharing data.
    - coordinate with ad networks and other third parties collecting data through your app so you can provide privacy disclosures to consumers that accurately reflect what's happening on your app, and
    - play an active role in self-regulatory programs and other processes to address privacy so everyone gets it right.
        - For example, the ADA – our hosts here today – played a leading role in the administration's process to develop model privacy disclosures for mobile apps. This represents an important step forward and we encourage app developers to work with ADA on consumer testing of such disclosures.

- The fourth and final guidance document I'll highlight is *Mobile App Developers: Start with Security*. This piece offers tips to help developers adopt and maintain reasonable data security practices.

    - Among other things, it urges developers to use due diligence about third party code that you use to build or augment your app. After all, you can't disclose your privacy and security practices accurately if you don't fully understand how your code operates.

    - We also advise you to remain vigilant about security issues after you ship your app, and have a plan to ship security updates if needed.

    - The guide contains a host of other tips and resources. Like the other pieces, it's on our website.

- Finally, as I mentioned, we have copious materials on COPPA compliance posted on our website, and FTC staff is always available to answer questions. Call or email Peder Magee at pmagee@ftc.gov or 202-326-3538.

Enforcement

- Now a few words about enforcement: Our hope is that all app developers will follow your good example of seeking to understand and adopt best practices for privacy and security. However, when companies don't pay attention to privacy and security and run afoul of the law, we bring law enforcement actions to bring them back into line and protect consumers.

- We're brought hundreds of cases challenging privacy and security violations under the various laws we enforce. Recently, a number have addressed violations in the mobile medium, including by app developers. I'll highlight just a couple to illustrate what *not* to do.

- First is our case involving social-networking app Path. Earlier this year, we settled charges that Path deceived consumers regarding its collection of their

address book information, and collected information from kids under age 13, without notice and parental consent as required by COPPA.

- We alleged that Path's app included an "Add Friends" feature that offered users three choices: "Find friends from your contacts," "Find friends from Facebook," and "Invite friends to join Path by email or SMS." However, regardless of the option users chose, Path automatically collected information from users' mobile device address books and stored this data on Path's servers.

- We're talking about a lot of information, including name, address, phone numbers, email address, Facebook and Twitter usernames, and date of birth of each contact.

- This case illustrates the importance of building privacy into all your products, including by testing each feature to make sure it doesn't collect more information than it should.

- This case also contains a lesson about COPPA. Path was not a child-directed app. Instead, COPPA applied because Path collected date of birth from each user upon registration, and thereby had actual knowledge that about 3,000 of its users were under 13.

- In another action, we brought charges against Frostwire, a peer-to-peer file-sharing application developer. Among other things, we alleged that its mobile app's default privacy settings violated the FTC Act's prohibition on unfair practices because they caused consumers to share everything from the mobile device – including user generated content such as photos, videos, and other stored files – and were very difficult even for a sophisticated user to change.

- This case highlights, once again, the importance of building privacy into your products and services from the start. You don't want your app to compromise your users' data or to disclose it in ways that your user would not reasonably expect. And that brings me back to *Expect Privacy*. Remember that consumers who are using your app increasingly *Expect Privacy*.

Conclusion

- As I hope my remarks have illustrated, privacy is a high priority for the Commission and helping mobile apps to get privacy right – whether through education or the tough love of enforcement – is an important element of our work in this area.

- You have an exciting day ahead of you, and will be hearing from many experts in the field, including investors, platforms, advocates, regulators, and, of course, senior staff from the office of California Attorney General. We are pleased to be a part of today's event, and to continue working alongside our California colleagues.