Keynote Address of Commissioner Ramirez
2011 Computers Freedom and Privacy Conference
Georgetown Law Center

the button – we do the rest."[4] Although photography had been around for many years, this cheaper and lighter camera enabled instant and candid photos of people in their everyday lives.[5] This technological advance coincided with the rise of a tabloid press, which now had the means to print personal and potentially embarrassing photos of anyone.[6] Warren, Brandeis, and many others were alarmed by the privacy ramifications of these developments. They cautioned that these new devices "threaten[ed] to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[7] Little did they know how such concerns would manifest themselves in the 21st century.

While the new consumer technology of the late 1800's was the Kodak snap camera, today our digital lives are being transformed by mobile technology. As of this February, nearly 70 million people in the United States own smartphones. This is a 13% increase in smartphone ownership as compared to the prior three months.[8] Today's smartphones are so powerful and sophisticated that their owners could not have imagined them just a few years ago.[9] And smartphone users can choose from hundreds of thousands of applications that offer astonishing functionality, from the mundane and frivolous, like the much-loved Arpg

I. Mobile's Defining Features Present Heightened Privacy Concerns

But what are the features of today's smartphones and tablets that make them a *new* technology with *new* privacy concerns? After all, there has been widespread access to the Internet via the desktop computer for nearly two decades. And a number of the concerns raised about mobile have been voiced about the general online environment for many years. Again, back to the Kodak snap camera: it was not the first camera sold in the United States, but it was cheaper and more widely available than prior cameras. And it was portable — mobile — in a way that earlier cameras were not. From a privacy perspective, those features made all the difference. Today's mobile devices have several defining features that also make a world of difference.

First, mobile devices are highly personal — always with you and always on. While desktop computers are often shared by multiple users, mobile phones are almost always used by only one person. And consumers take them nearly everywhere they go. Think of your own behavior. When was the last time you went out without your smartphone? For most people, that's as rare as leaving home without a wallet or purse. How often do you turn off your smartphone? For most of us, I imagine the answer is almost never, not even when we sleep. In fact, two-thirds of American adults have slept with their phone at their bedside.[10]

Then there is location. As with real estate, the three most important things about mobile are location, location, location. To an unprecedented degree, these devices collect information about consumers' precise whereabouts. When you factor in that smartphones are always with us and always on, the result can be a nearly complete record of where we spend our every moment.

---

[10] *See* Douglas McIntyre, *Do You Sleep with Your Cell Phone? Most Americans Do*, DAILY FINANCE (Sept. 3, 2010), *available at* http://www.dailyfinance.com/2010/09/03/do-you-sleep-with-your-cell-phone-most-americans-do-study-find/.

This record can reveal sensitive information such as visits to a hospital, doctor's office, church, school, or political meeting.

Third, in many cases, mobile apps can collect a wide variety of information — some of it quite revealing — about users beyond their location. The Wall Street Journal has reported that many companies access a broad range of information, including the user's contacts, phone number, gender, age, and what other apps have been installed.[11]

II. Privacy Protection Has Not Kept Pace with Advances in Mobile Technology

Industry has not yet risen to meet the unique privacy challenges presented by mobile technology. Technological innovation has far outpaced privacy protection, and, as a result, we now have a deepening "privacy deficit."[12]

Mobile data privacy has been called a "wild west,"[13] and, regrettably, the description is all too apt. Everyone understands that a navigation app or an app that provides restaurant recommendations or local coupons needs geographic information. But gaming apps and others frequently collect location data for no clear reason. This is particularly alarming when apps are directed at children.

Consumers today are given limited notice, not to mention choice, before information about their location is shared. We see some "notice and choice" today before location information is shared with apps, but what happens next? Apps are not providing effective notice and choice before passing on location data to other companies. Many consumers would also be surprised, and disturbed, to learn that apps are collecting and sharing other personal information about them, including a unique ID assigned to their phone.[14] Ad networks receiving this information from multiple apps can create detailed profiles of consumers that could be shared with a variety of online and offline companies, potentially including employers, schools, and insurance companies.

---

[12] *See, e.g.*, Matthew Ingram, *FTC: Privacy Self-Regulation Not Enough, "Do Not Track" Needed*, GIGAOM (Dec. 1, 2010) (the FTC is "thinking about the privacy deficit American consumers suffer from") (quoting FTC Chairman Jon Leibowitz), *available at* http://www.gigaom.com/2010/12/01/ftc-privacy-do-not-track/; Editorial, *There's a Privacy Deficit*, L.A. TIMES (Mar. 17, 2008), *available at* http://www.articles.latimes.com/2008/mar/17/opinion/ed-privacy17.

[13] *See, e.g.*, Statement of Senator Blumenthal, *Hearing on Mobile Phone Privacy Protection Before the S. Subcomm. on Privacy, Technology, and the Law*, 112th Cong. (May 10, 2011), Tr. at 15.

[14] *See* Thurm & Kane, *supra* note 11.

Against this backdrop of questionable privacy practices, many consumers report serious concerns about their privacy when using a mobile phone. According to an online survey of 1,000 consumers conducted by TRUSTe and Harris Interactive earlier this year, privacy is consumers' top concern when using mobile applications.[15]

III. FTC Preliminary Staff Report: A Prescription for Better Mobile Privacy

So what can be done? Companies acknowledge that consumer privacy and trust are vitally important to the long-term growth of mobile,[16] and that more needs to be done to educate consumers about mobile privacy practices.[17] But their actions suggest they often lose sight of

fundamentally rethink a wide range of privacy issues and offer best practices for industry, as well as guidance for Congress. The first key recommendation is "privacy by design," which seeks to shift the burden of privacy protection from consumers onto companies.

Privacy by design has clear application in the mobile arena. Companies are rolling out new mobile products and services every single day. It is cheaper for industry, and better for consumers, if companies take privacy into account from the earliest stages of development. This means built-in protections on mobile devices, such as encryption and providing for a data wipe at the end of the device's life. It means embedding privacy-protective default settings. And, it means collecting only the information needed for a specific and identified business purpose.

Companies often tell the FTC that they cannot innovate unless they are broadly permitted to collect information about consumers, on the theory that they may one day identify a new use

screens to read a single privacy policy. That's not realistic. Privacy information should be presented in concise and plain English, or with universal icons or symbols, and, where possible, on a "just-in-time" basis.

For location information, there should be express, affirmative consent — opt-in consent, in other words — before the information is collected. That, of course, has clear application to the mobile arena. The Report also advocates that companies provide express affirmative consent for other sensitive data, such as medical and financial information and information about children.

As you know, the Report also recommends the establishment of a Do Not Track system for online behavioral advertising. You had what I'm sure was a lively discussion earlier today about Do Not Track, so I won't go into detail about our proposal. But I would like to point out that a majority of us on the Commission support Do Not Track, and we have made clear that it should ion ,yto phe m19Tj12.0 0 12 7240 37776 Tm00008 Tc-.0008 Tw[(f W)46(eth u)8.6(obile awebsies thea

percent of the top 340 free applications contain a link to a written privacy policy.[20] Their absence in the mobile sphere adds to the enormous uncertainty about mobile data privacy.

IV. FTC Law Enforcement in Mobile Privacy

Now, I would like to turn briefly to law enforcement in the mobile arena. In the last year, the FTC has launched a mobile forensic lab, retained distinguished technologists including Ed Felten, our first Chief Technology Officer, who you heard from earlier today, and assembled a team focused on all manner of consumer protection issues in the mobile arena. We are in the midst of an expedited review of the Child Online Privacy Protection Act ("COPPA") as applied to the mobile sphere, and you can soon expect to hear the results of that review. And FTC staff has a number of nonpublic mobile investigations in the pipeline, so you can expect to see active enforcement in the mobile arena in the coming months. But we already have significant accomplishments to report.

Most importantly, we have negotiated consent orders with two of the most significant companies in mobile today — Google and Twitter. The FTC charged that Google deceived Gmail users when it used their information to launch its social network, Google Buzz.[21] The Commission's proposed settlement contains strong injunctive relief, including limits on sharing information in certain circumstances without consumers' express affirmative consent. Google will also have to submit to independent privacy audits for the next 20 years. Significantly, the proposed *Google* order covers the full universe of Google products, including mobile.

---

[20] *See* Mark Hachman, *Most Mobile Apps Lack Privacy Policies*, PC MAG (Apr. 27, 2011), *available at* http://www.pcmag.com/article2/0,2817,2384363,00.asp; *see also* Thurm & Kane, *supra* note 11 (reporting that in a test of 101 apps, 45 failed to make written privacy policies available on a website or in the app).

[21] *See In re Google Inc.*, FTC File No. 102-3136 (Mar. 30, 2011) (proposed consent agreement), *available at* http://www.ftc.gov/opa/2011/03/google.shtm.

The *Twitter* order issued last year similarly protects Twitter's many mobile and non-mobile users. The Commission charged that serious flaws in Twitter's data security enabled hackers to access private account information and private tweets. In addition to injunctive relief, the Commission's order requires Twitter to undergo independent data security audits over the next decade.

Earlier this year, the Commission also brought its first case against text message spam.[22] And last year, the FTC brought charges against

workable, voluntary solutions to the privacy challenges presented by the remarkable mobile technology of today and tomorrow.

Thank you.