ter".

gave me the choice of speaking to you today about any topic I wished. And for asons – or at least reasons that I think you will find obvious – I have chosen to speak cy in the mobile space.

sumers are increasingly turning to mobile to manage many facets of their lives – from shopping, listening to music, catching up on news, buying movie tickets, and nearby restaurant, getting driving directions, and tracking calories and exercise Vith our smartphones in hand, we can locate our children. We can play games. We banking and pay our bills. Whatever you'd like to do, there's "an app for that."

let us not forget: with our smartphones, we can even make phone calls!

ed, smartphones are not one device – they are multiple devices wrapped into one They are the Swiss Army knife of our modern age: a powerful collection of services ns in one handy package that slips right into our pocket. If it only had a corkscrew on would be perfect.

who knows, even that might come standard on the iPhone 6.

Here in the U.S., more than one-half (50.4%) of consumers now owns a smartphone,[4] and that number also is expected to grow.

Our growing dependence on mobile is even more salient in some of our communities. About 40 percent of people in households earning less than $30,000 say they go online mostly through their mobile phones, compared with just 17 percent of those earning more than $50,000. And half of African-American cellphone internet users, and 40% of Latino cellphone internet users, do most of their online browsing on their phones. And if you have teens, you know they are never without their phones. Nearly half of college students say they often check their phones before falling asleep, and over half do so before getting out of bed in the morning.[5]

Along with the explosion in popularity of our smartphones has come an explosive growth in the potential collection and use of the myriad form

So improving privacy in the mobile space will not only benefit consumers. Earning consumer trust will increasingly become a market imperative for browsers, websites, app developers, marketers, and others operating in this space, and allow this highly innovative segment of our economy to continue to thrive.

As the nation’s premier consumer protection and privacy agency, we at the FTC are committed to translating our long-standing consumer protection principles into the innovative and complex mobile space.

In the “on the go” mobile world, this translates into providing consumers with information “just in time” and through “consumer friendly” layered notices. The FTC’s call for providing better consumer choice and transparency, laid out in our big privacy report issued one year ago, applies with even greater urgency in the mobile space – where there is limited real estate, making textual disclosures harder to read, and where consumers now have limited understanding of how much of their information can be collected and used, and by whom. We are working hard to get out the message that all players in this ecosystem have a responsibility to provide more transparency and appropriate choices to consumers.

We have our work cut out for us. We have found that many players in the mobile ecosystem are still not even providing more traditional privacy policies. In 2012, the FTC released two studies that assessed the adequacy of privacy disclosures made in mobile apps directed to children.[9] We found that the majority of kids apps do not adequately give parents the information they need to determine what data is being collected from their children, how it is being shared, or who will have access to it. Probably most troubling is that many of the apps we studied shared certain information with third parties – such as device ID, geolocation, or phone number – without ever disclosing that fact to parents.

As we dive deeper into mobile issues, we have learned that understanding the technology is critical. So we have brought in top-notch computer scientists to advise the agency on evolving technology and to assist us in our enforcement and policy work. Ed Felten of Princeton served as the FTC’s first chief technology officer. After Ed returned to Princeton a few months ago, Steve Bellovin of Columbia University took over. Steve is a cybersecurity expert who, prior to becoming a professor at Columbia, had spent many e ebj8.1w [uat_-bs -.00AT&T Res002ave_-bsur we03 T

These law enforcement efforts have been bearing fruit. Of course, the tech community is well aware of our enforcement actions involving Google and Facebook's privacy practices, including the record-breaking $22.5 million civil penalty that Google paid for evading Apple's privacy protections for Safari users.[10] Industry players are also well aware that we are requiring both Google and Facebook to develop comprehensive privacy programs that an outside auditor will assess for the next 20 years.

Our enforcement activity is not limited to companies that are household names, and these less-well known cases bear similarly important lessons for the tech community. I'm not sure whether you all have noticed, but we are barely nine weeks into 2013, and we have already announced 3 mobile cases.

Our most recent case involved mobile device manufacturer HTC, in which we were concerned that HTC failed to em

This perspective of shared responsibility is also the focus of our new mobile privacy report, released last month.[17] The report makes recommendations for “best practices”, focusing on how each of the players in the mobile space – platforms, app developers, advertisers, analytic companies, and trade associations – has an important role to play in protecting consumers’ privacy. Let me highlight a few of the report’s recommendations for best practices.

Platforms and operating systems like Apple, Google, Microsoft and Research in Motion should provide “just in time” disclosures and affirmative express consent before allowing apps to access users’ sensitive content, like geolocation information, contacts, photos, and calendars. Platforms should also consider developing a consumer-facing one-stop “dashboard,” where consumers could review and manage the types of content accessed by the apps they have downloaded. And implementation of a Do Not Track mechanism by operating systems will provide consumers with an appropriate way to express their preferences about data collection