"WHAT DOES THE FUTURE LOOK LIKE FOR MARKETING IN CYBERSPACE?"

Keynote Address for the Consumer Marketing,
Advertising, Distribution and Sales Conference
Suffolk University Law School
March 23, 2012

Good morning, and thank you for having me here. I'd like to focus on how consumers' online information is used for marketing, and what the appropriate rules around use of this information should be.

A woman—we'll call her Tammy—is visiting her parents in Dorchester not too far from here. She wants to go to the new Target store to pick up a few things and uses her smartphone to get directions. She often shops at Target. Several months ago she purchased a pregnancy test at a different Target pharmacy in Framingham, where she currently lives, and she and her husband were overjoyed when it turned out positive.

While at Target in Dorchester, she gets several great deals! She buys an infant car seat, a crib and baby clothes. How could she resist? Really good coupons popped up on her smart phone as she entered the store.

Tammy expects she will be visiting the Target in Dorchester a lot. Because she is pregnant, Tammy and her husband—let's call him Jim--intend to move back to be closer to her parents. (Free babysitting, you know!) So, at a hotspot, she uses her laptop to continue searching for housing and checks to see the local pediatric practices that accept her insurance.

Tammy and Jim have told no one except their closest family about the baby and their expected move. But they have begun looking for jobs in the area. They have been researching online. Both have texted and emailed with potential employers and headhunters about jobs and to obtain more information. Unfortunately, one potential employer mentioned some party pictures from Jim's college years on a social network website, despite the fact that Jim had tried to take his page down. The pictures, which he had shared with a friend, were on the friend's website and Jim's name was "tagged" to the picture.

None of the listed actions in my story are extraordinary. A lot of Tammy and Jim's information is flowing through cyberspace. The flow of that information – who collects it, who receives it, for what purpose – raises some pretty important questions:

- Does Target know Tammy is pregnant and has it started targeting her with coupons?

- Has a data broker created a profile on Tammy that indicates she may be pregnant and wants to move?

- Can Jim get the pictures from his college years off the social networking site?

- Will Tammy and Jim receive unsolicited contacts for housing in the new area?

- And what are the appropriate practices and rules that should govern these issues?

As we contemplate "the future of marketing in cyperspace," one salient fact stands out: an enormous amount of data that was unavailable just a few years ago is now easily accessible. And the potential for aggregating and selling that data is very real. The questions I just posed are not that far-fetched. The New York Times recently had an article describing how Target uses online and offline data to predict pregnancy.[1] We know that companies are scraping and sniffing data about their employees. Just this week, there were media reports of job candidates being asked to turn over their Facebook user names and passwords during an interview.[2] Sensitive information, supposedly anonymous, has been "reidentified" by combining it with other available information. Geolocation information is being collected to offer "just in time" services such as coupons and promotions for local businesses. Pictures posted on social media sites have still been available after pages are taken down by owners.

Clearly, the proper use of data can be very beneficial to consumers. But there should be some boundaries to this ubiquitous data collection and aggregation. We at the Federal Trade Commission are working to balance the needs of a thriving internet market and appropriate levels of consumer protection. We have focused our efforts in three areas: enforcement where privacy promises are broken or practices are unfair; developing policy and best practices for industry; and proposing changes to some law and rules governing privacy.

Let's start with enforcement. We have brought law enforcement cases against companies that failed to protect the vast amount of personal information they held about consumers, including sensitive financial information. We have also brought law enforcement actions against companies that disclosed personal data that consumers expected to be private. We took action against Twitter when it made some private tweets public.[3]

And the FTC has entered into settlements with both Facebook and Google relating to their privacy practices. The FTC's complaint against Facebook alleges a number of

---

[1] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times, Feb 19, 2012, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all.

[2] *Employers Ask Job Seekers for Facebook Passwords*, Wall St. Journal, Mar. 20, 2012, *available at* http://online.wsj.com/article/AP35b6fb378cc64062a3bceb87e17e2e03.html.

[3] *In the Matter of Twitter, Inc.* FTC File No. 092-3093 (June 2010) (consent order).

deceptive and unfair practices in violation of the FTC Act.[4] These include changes made by Facebook in 2009 so that information users had designated private became public. We also called Facebook out for promises it made by did not keep: It told users it wouldn't share information with advertisers, and then it did; and the company agreed to take down photos and videos of users who had deleted their accounts, and then it did not.

The proposed FTC settlement with Facebook requires the company to obtain affirmative express consent before sharing users' information in a way that exceeds their privacy settings, and it must block access to information that users delete.

We also require Facebook to implement a comprehensive privacy program that an independent auditor will monitor for 20 years.

The FTC's settlement with Google arose from the roll out of Google's first social media product, Google Buzz.[5] We believed that Google did not give Gmail users good ways to stay out of or leave Buzz, in violation of Google's privacy policies.

We also charged that the company did not adequately disclose to users that the identity of individuals who users most frequently emailed could be made public by default. Like Facebook, Google is required to obtain consumers' express affirmative consent before sharing information in a way that is materially different from its current privacy policies and it must implement a comprehensive privacy program that will be monitored for 20 years.

At the same time that the agency's enforcement program in the data security and privacy areas have proceeded full steam ahead, we have also been reexamining the way we think about some key privacy concepts, like the role of privacy notices.

Unfortunately, most privacy notices today are so long and complicated that consumers have to go to law school to understand them—not that I have anything against going to law school! And trying to read these notices on smart phones can sometimes be virtually impossible – requiring up to 150 clicks to see the full text!

Policy: The Privacy Report.

So in December 2010, we proposed a new framework for privacy that contains several important principles to address some of these key issues.[6]

---

[4] *In the Matter of Facebook, Inc., a corporation* FTC File No. 0923184 (2011).

[5] *Google Inc., a corporation* FTC Docket No. C-4336 (Oct. 24, 2011) (Consent order). *Available at* http://www.ftc.gov/opa/2011/10/buzz.shtm.

[6] *See* A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

The first principle is Privacy by Design. This principle encourages industry to build privacy and security protections into new products and not wait until there is a privacy disaster to address problems. For example, companies should:

- Examine the information they collect about consumers and determine whether they really need to collect it; and

- Determine how long they are retaining that data and figure out whether such retention is really necessary.

The second principle of our preliminary report is simpler choice. There are a number of ways that consumer choice can be streamlined. One of the most talked about "simpler choice" recommendations that the agency is calling for is the development of Do Not Track mechanisms. These mechanisms would enable consumers to make choices about whether their online activities across various websites can be collected and used to market to them or for other purposes.

The third principle in the FTC report setting forth the preliminary framework is greater transparency. Companies should provide consumers with more information about what is being done with their personal information.

Right now, information about privacy practices is often hard to come by. The Commission's recent report on Mobile Apps for Kids concluded that mobile app stores provide parents with little or no information about the data apps collect, who has access to it or how it would be used.[7] But some progress is being made. The California Attorney General's office recently reached an agreement with six major players in the mobile apps market that requires display of privacy policies for apps prior to purchase.[8]

While seeking transparency, the Commission is well aware of the challenges posed in designing disclosures. Technology has changed greatly since our policies on Dot Com disclosures were issued twelve years ago. On May 30th the Commission will be hosting a workshop to explore the need for new guidance on disclosures for online advertisers.[9] The items to be addressed will include disclosures on the limited real estate provided on smart phones, the timing of disclosures, the layering of disclosures and the use of icons.

---

[7] *See* Mobile Apps for Kids: Current Privacy Disclosures are Dis*app*ointing (Feb. 16, 2012) *available at:* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

[8] *See Press Release,* Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications (Feb. 22, 2012) *available at* http://oag.ca.gov/news/press_release?id=2630.

[9] *See* Press Release, FTC, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012 (Feb. 29, 2012), *available at* http://www.ftc.gov/opa/2012/02/dotcom.shtm.

In issuing the 2010 report setting for the preliminary privacy framework, the FTC called on all stakeholders, including industry and the consumer advocacy community to provide the agency with input on the many issues we explored in the report. Having spent many months analyzing the input that the agency received, we will release our final report, containing the final framework, very soon.

The FTC has not been alone in re-examining the framework that shapes the approach to privacy. The U.S. Department of Commerce has been engaged in an initiative to develop a framework that would set forth company obligations and consumer rights with regard to personal information. The White House recently released a report outlining this framework and a Consumer Privacy Bill of Rights.[10] The FTC and the Department of Commerce initiative have been complementary, and the two agencies will continue to work together as we move forward to better protect consumer privacy.

And as these initiatives have proceeded here in the United States, similar examinations have been taking place in other parts of the world. Notably, in the European Union, a new regulatory framework for privacy is also being considered—and we at the FTC have been working with our European colleagues so that we can each benefit from the information gathering and policy thinking that is taking place on both sides of the Atlantic.

Do Not Track

Even though our recommendations are not yet final, industry has responded to our call for improved practices, particularly in developing Do Not Track mechanisms. Industry has begun developing both browser-based and cookie-based opt out solutions—at least with regard to behavioral advertising. Although still a work in progress, the ad industry's icon-based Do Not Track system has buy-in from companies that deliver 90% of online behavioral ads. And the industry recently announced that its members will honor tracking choices that consumers make through their browsers. Industry has also committed not to release browsing information to those who would use it for sensitive purposes--such as hiring.

Legislation and regulation.

Proposing legislation and adopting regulations are also tools that the Commission uses to advance its privacy agenda.

The Commission is undertaking early review of its COPPA rules. As I previously noted, COPPA and the Commission's rules are designed to protect children under 13 when they venture into cyberspace.[11] And while the Commission usually reviews its rules

[10] Press Release, Digital Advertising Alliance, White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumer Online Privacy (Feb. 23, 2012) *available at* http://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf.

[11] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (1998).

every ten years, we moved up the COPPA review by five years due to explosion of mobile apps and children's use of them. In 2005, Twitter was a sound, the Cloud was something in the sky, 4G was a parking spot, Applications were what you harassed your teenagers to send into college, and Skype was a typo. The Commission's proposed changes to the COPPA Rules include:

- Expanding the definition of "personal information" to include geolocation information and persistent identifiers (unless used only for internal support purposes).

- Streamlining privacy policy and "direct notice" requirements.

- Updating methods of obtaining verifiable consent from parents.

The comment period on the proposed changes has ended and staff is working through those comments. We expect a final rule to be issued in the near future.

More fundamentally, there is a need for legislation in the area of data collection, use and security. As I've noted, vast amounts of data about us can be collected, aggregated and sold. The information, both from cyberspace and traditional sources of information, can be used for making all types of decisions about us. But only portion of this activity is governed by Federal law. The Fair Credit Reporting Act governs the use of credit reports in making decisions about credit, employment, insurance and housing.[12] Unless the activity falls within FCRA, however, consumers have no right to review and assure the accuracy of the information gathered by data brokers.

The law has not kept up with the vast amounts of data that are used to make important decisions about consumers. I believe that, where information held by data brokers is used to make decisions about substantial benefits, consumers should have the right to examine the information and to correct errors contained if necessary.

But fixing FCRA or enacting another law to address this coverage gap is not enough.

I am also concerned that currently there is no federal legislation in the areas of data security and breach notification. And I agree with the White House that it is time for enactment of baseline federal privacy legislation. The President has proposed a Consumer Bill of Rights which includes many concepts from our privacy report.

Passage of such legislation would be an important step forward in protecting the rights of consumers and ensuring their trust as they conduct more and more of their lives in cyberspace.

[12] 15 U.S.C. § 1681s(a)(2)(A).

Conclusion.

Much is going on in cyberspace while "Tammy and Jim" go about their normal activities. There are many legitimate concerns they may have about what is happening with their data. The Commission's work is designed to

- Give consumers like Tammy and Jim easy ways to understand and make choices.
- Instill their confidence in the marketplace by making sure that promises made about protecting their data are kept.
- Assure that consumer protections keep up with technological developments.

A safe and fair foundation for cyber-business is in everyone's interest. I have no doubt that together we can accomplish those goals while assuring a robust future for advertising in cyberspace.