33rd Annual PMA Marketing Law Conference
Julie Brill
Commissioner, Federal Trade Commission
November 16, 2011

Good morning and thank you for that kind introduction. I have always enjoyed coming to this event – and as you regulars know, I have done so for several years, first as a state AAG, and now twice as a Commissioner of the Federal Trade Commission. I appreciate the opportunity to speak to all of you—advertisers, marketers and attorneys—who are here because you want to do the right thing.

When I spoke to you all last year, I had been at the FTC for just over seven months. At that time, the agency's big privacy rethink had not yet been released. We were still in the midst of reviewing the rule that we enforce pursuant to the Children's Online Privacy Protection Act, and our revisions to the Guides on Endorsements and Testimonials in Advertising were a little over a year old.

A lot can happen in a year. And a lot has.

Two weeks after I spoke here last year, the FTC staff's report on a new privacy framework was released. Just two months ago, we issued our proposed revisions to the COPPA rule. And over the past year, we've issued some interesting cases enforcing our Endorsements and Testimonials guide.

Privacy

Let's start with privacy. Last year, I provided you with a preview of what you might expect to see in the report. Today, I imagine many of you have taken the time to study the report in some detail.

In the report, we propose a framework to provide consumers with greater knowledge, control and choice over what happens with their information. We also believe this framework allows industry to thrive and continue to innovate.

The report outlines three critical concepts that serve as the building blocks of an improved privacy framework.[1]

First, we call for companies to build privacy and security protections into new products. Products and services shouldn't be retrofitted with privacy and security features after the fact. Privacy and security issues must be considered at the outset. This concept is often referred to as

[1] *See* A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, at 57-59 (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

"privacy by design." So, for instance, when designing new products and services, the level of security and privacy protection should be proportionate to the sensitivity of the data used. And companies should limit the amount of information collected to what is needed, and retain the data only as long as needed.

Second, we call for simpler and more streamlined choices for consumers. One way companies can streamline choices is to provide "just in time" information to consumers. Another method is to exempt "commonly accepted" practices from the first layers of these "just in time" notices. There are certain practices that are "commonly accepted"—such as sharing data with the shipping company that will deliver the product that you just ordered. If we remove the disclosures relating to these practices, consumers can pay more attention to other uses of data—ones that are unexpected.

And third, the report calls for greater transparency surrounding data—how industry collects it, uses it, and retains it. Consumers should know what kind of data companies collect, and should have access to it—in proportion to the sensitivity and intended use of the data.

This framework allows both business and consumers to continue to benefit from the information marketplace. We have received over 400 comments on the report. We are working our way through them, and continuing our conversations with industry and consumer groups, and other policy makers to develop final recommendations.

One area that has gotten significant attention is our call for Do Not Track mechanisms. I'm sure our Do Not Track recommendation has your attention as well. Do Not Track has the potential to provide consumers with information about online data collection and use practices, and to allow them to make certain choices in connection with those practices.

Industry seems to have heard – loud and clear – our call for development of Do Not Track. In the past year, we have seen considerable progress in the development of Do Not Track mechanisms. And we have seen considerable progress in industry's willingness and interest to engage with the Federal Trade Commission on these issues.

I personally have met with many individuals and organizations involved in the development of Do Not Track, both from the Digital Advertising Alliance AboutAds program, and from the browser companies. There has been meaningful and frank dialogue, and I hope that will continue.

The Commission as a whole is closely monitoring the various mechanisms and programs that are emerging. I am keeping a close eye on several issues of importance to me. Let me tell you what I see as some of the critical issues that I will be monitoring in the coming weeks and months:

First, we all need to speak the same language. DNT mechanisms enable consumers to make a choice about being "tracked." Is that word -- "tracked" -- being used consistently? I do not believe it is. Companies and consumers should have a clear and consistent understanding about what can and cannot be done with information about a consumer who has chosen not to be

"tracked." From my perspective, and from the perspective of most consumers, choices about "tracking" should include choices about collection of data about consumers, as well as choices about use of that data for serving targeted advertising.

We also need to come to an understanding about "commonly accepted practices." There are certain practices that we can probably all agree are commonly accepted. But there are other practices that are merely "common" among industry – and not commonly accepted by consumers. If the concept of exempting "commonly accepted practices" is going to have any life going forward, it must focus on those practices that are commonly accepted by consumers. For practices that are not commonly accepted by consumers, notice and meaningful choice should be provided.

Confidence in the technology supporting each Do Not Track mechanism is also critically important. If a consumer makes a choice, that choice must be honored and the technology needs to work to effectuate that choice. In this era, code is conduct. To get the conduct right, we have to get the technology right. Technological glitches – whether arising from flash cookies or supercookies, or simply from a complex consumer interface that breaks down with such regularity that consumers get frustrated – technological glitches like these need to be addressed so they won't stand in the way of putting consumer choices into effect.

The success of any particular Do Not Track program also hinges on wide adoption by industry. We need a critical mass of industry players – including advertisers and ad networks – participating and fully honoring the choices that consumers make. And a successful Do Not Track program requires a broad-based understanding by consumers. The notices and choices offered to consumers must be easy for consumers to find, and easy to use.

We have seen development of two different types of Do Not Track mechanisms: browser-based, and icon/cookie-based. The concerns I just outlined apply with equal force to both types of programs. But there is another important issue that relates to the interaction of the two kinds of programs. We need to closely examine how the two work together. We are monitoring the efforts of the W3C—a key Internet standards setting organization—to define technical standards for Do Not Track. I believe that all Do Not Track participants –the browsers, the advertisers and the ad networks – should be closely involved in development of these standards, to ensure that they work across the spectrum, for all industry players. And at some point in the very near future, I want to see the cookie based programs accepting choices made by consumers through the browser programs, and vice versa. Effective DNT programs will enable a consumer's choice about DNT to be registered and honored no matter which mechanism – a browser or an icon – the consumer uses to express her choice.

And compliance is really what it is all about—speaking as someone with 20+ years in law enforcement. Companies must honor the commitments they make to consumers about their behavioral advertising practices must be honored. Last week, the Commission announced that an ad network engaging in behavioral advertising settled FTC charges that it deceptively claimed consumers could opt out of receiving targeted ads by changing their browser settings to block

cookies.[2] But the company—ScanScout—had been using Flash cookies, which browser settings could not block. The proposed settlement requires that ScanScout take steps to improve disclosure of their collection practices and to provide a user friendly mechanism that allows consumers to opt out of being tracked.

So why do I care so much about this issue? After all, isn't behavioral advertising simply about giving consumers advertising that is more relevant, which benefits consumers as well as the advertiser? And indeed pays for much of the free content that benefits consumers. What's the fuss about?

From my perspective, there are some real harms that consumers might experience from the vast quantities of data being collected about them through behavioral advertising and through other means.

Let me tell you about three types of harms that consumers can experience.

First, the collection of vast amounts of data can unintentionally—or even intentionally—include sensitive information, such as health and financial information or information about sexual orientation. The collection of sensitive information should trigger heightened protections—more robust notice and choice. It is not clear that this is happening now, although there seems to be widespread agreement that the collection of sensitive information requires such heightened protection.

Many data collectors claim that there is no harm here, since the data is deidentified. I am not assuaged. Researchers have shown how easy it is to take deidentified data and reassociate it with specific consumers.[3] And a great deal of so-called non-personally identified information is linked to a specific smartphone or laptop. Given how closely these devices are now associated the each of us—many of us sleep more closely to our cell phones than we do our spouses!—data that is linked to specific devices through UDIDs and other means are, for most intents and purposes, personally identifiable.

Second, a harm that we are all very familiar with occurs when there is a data breach. The more data that is collected and retained, the greater the risk when a data breach occurs. Holding on to vast stores of data flies in the face of one of the fundamental principles of "privacy by design" – data minimization. If you hold on to data you don't need, for purposes that you can't now articulate but might be able to at some point in the future, you and your consumers are at much greater risk in the event of a breach. Instead, it would be wise to safely destroy that data.

Third, there are very real potential harms that might not be as feasible on a small scale, but become possible on a large scale. I'm referring to the combination of data from multiple

[2] *See* In the Matter of ScanScout, FTC File No. 1023185 (Nov 2011) (consent order).

[3] *See e.g.* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010).

sources, including off line and social networks. We have seen researchers and some companies pull these data points together to make predictions about consumers' future behavior. I am concerned about data that are used in place of traditional credit reports, to make predictions that become part of the basis for making determinations regarding a consumers' credit, or her ability to secure housing, gainful employment, or various types of insurance.

I have been keenly interested in press stories about how life insurers are using consumer consumption patterns to predict life expectancy, and are used to help set rates and coverage being offered for insurance policies.

Might there be a day when a consumer's geolocation information—a history indicating where a consumer has physically been over a period of time—can be purchased by your current employer or potential employers? Or the bank where you've applied for a loan?

We have pretty strict rules designed to protect consumers in connection with traditional credit reports. Consumers have certain notification rights, as well as the right to access and correct information compiled about them. It is critical that we ensure these protections are implemented and honored for all types of reports amassed about consumers and used for sensitive purposes, like credit, employment, housing and insurance.

COPPA

While behavioral advertising and the discussions surrounding Do Not Track have our attention, these issues are not the only ones that we are closely considering. One critical piece of the agency's overall privacy agenda is our commitment to children's privacy. As you all know, the FTC enforces a rule promulgated pursuant to the Children's Online Privacy Protection Act.[4]

We began our review of the COPPA rule in 2010—five years ahead of schedule. This acceleration was necessary because technology has rapidly revolutionized the way we—and our children—communicate. It became very clear that we had to reconsider the COPPA rule on an expedited basis.

Two months ago, the Commission issued its proposed changes to the COPPA rule.[5] The comment period remains open until November 28, 2011 and we of course will be closely reviewing all submissions.

Among the changes we are proposing, the most significant make it clear that COPPA applies to new media, including the mobile space.

We are proposing to expand the definition of personal information covered by COPPA to include photos, videos, and audio files containing children's images or voices. The expanded

[4] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (1998); Children's Online Privacy Protection Act Rule, 16 C.F.R. Part 312 (1999).

[5] Press Release, FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule, (Sept. 15, 2011) *available at* http://www.ftc.gov/opa/2011/09/coppa.shtm.

definition of personal information also addresses online behavioral advertising to children. The proposed changes will require parental notification and consent prior to compiling data on a child's online activities, or behaviorally targeting advertising to a child.

We are proposing that the COPPA rule be modified to provide more streamlined, meaningful information to parents. As we said in our big privacy rethink, lengthy privacy notices just don't get the job done. That's why here, in connection with COPPA, we propose eliminating the Rule's current requirement that the direct online notice contain a lengthy recitation of an operator's information collection, use, and disclosure practices. Instead, we propose that operators give parents a simple statement of: (1) what information the operator collects from children, including whether the website or online service enables a child to make personal information publicly available; (2) how the operator uses such information; and (3) the operator's disclosure practices for such information.

We are also proposing significant changes in how verifiable parental consent can be achieved. COPPA only works if parents are in fact contacted so they can make choices. We bring the technological revolution to the concept of verifiable consent by proposing some additional ways to obtain it, such as electronic scans of signed parental consent forms, video conferencing, and the use of government-issued IDs. And we recognize that additional innovations may be possible, so we are allowing for industry to propose new means of obtaining verifiable parental consent.

While we are optimistic that new methods will be developed, we have to face reality about the ones that we have relied on in the past. We previously permitted operators to use the "Email Plus" method of verifiable parental consent when collecting personal information for the operator's internal use. Because of its simplicity, it has been widely used by kid-oriented websites. But Email Plus had always been a temporary verification method that we allowed when consent methods had not been sufficiently developed. Now, it seems to be standing in the way of developing more robust verifiable consent methods. And of course, we have long recognized that Email Plus is simply not as reliable as some of the other methods, because kids can so easily work around it.

The shelf life on Email Plus has run its course and we are proposing to let this one go. I am confident that industry will develop more reliable methods—methods that work and that we can be assured are representing actual choices made by parents so they can exert the control over information about their kids that Congress intended when it enacted COPPA.

At the same time that we are considering how the COPPA Rule can be improved, our enforcement of the Rule continues in full force. In May of this year, the Commission reached a settlement with Playdom, a developer of online virtual worlds, many of which cater to children.[6] The Commission charged Playdom with collecting and disclosing personal information obtained from children—information which included their names, email addresses, instant messenger IDs, and even their locations—all without parental consent. Hundreds of thousands of children had registered on Playdom's various sites and exposed their personal, private information without

[6] *United States v. Playdom, Inc.*, No. SA CV-11-00724 (C.D. Cal., May 24, 2011) (consent decree).

their parent's knowledge. The Commission's settlement with Playdom—$3 million in civil penalties—set a new high water mark for COPPA.

And in August of this year, the Commission brought its first COPPA case against a mobile app developer.[7] We charged W3 Innovations with illegally collecting and maintaining thousands of young girls' email addresses. The "dress up" and "girl world" mobile apps developed by W3 also allowed girls to publicly post personal information to in-app message boards that were accessible to the public. In all, there were 50,000 downloads of W3 Innovations apps directed at children.

Privacy, whether it relates to our children, the security of our personal information, or control over whether our online behavior is being tracked, is about trust in the marketplace.

Endorsement Guides

Trust is the backbone of any consumer experience—this holds true not only with respect to consumers' concerns about their personal information, but also with respect to advertising consumers see and rely upon.

The FTC announced revisions to the Endorsement Guides in 2009[8]—prior to that, they had not been updated since 1980. In the intervening thirty years, we saw tectonic shifts in the advertising world and its movement to the online and mobile space. This changing environment called for updated guidance.

Our Endorsement and Testimonial Guidance continues to be based on three important principals.

- Endorsements must be truthful and not misleading.
- If the advertiser doesn't have proof that the endorser's experience represents what consumers will achieve by using the product, the ad must clearly and conspicuously disclose the generally expected results in the depicted circumstances.
- And, if there's a connection between the endorser and the marketer of the product that would affect how people evaluate the endorsement, and it is not otherwise apparent from the communication, it should be disclosed.

So, for example, if a blogger has been paid by an advertiser in connection with writing about a product, that payment must be disclosed. And an affiliate marketer can't hold itself out as offering independent reviews of a product.

---

[7] *United States v. W3 Innovations LLC*, No. CV-11-03958 (N.D. Cal., Sept. 8, 2011) (consent decree).

[8] Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. Part 255 (2009).

In the past year we have continued our active enforcement of the guidelines. In March 2011, a company called Legacy Learning agreed to pay the FTC $250,000 to settle charges that it used misleading online consumer reviews to tout its product—in this case a series of guitar-lesson DVDs.[9] The company used an online affiliate program, through which it recruited affiliates to promote its courses through endorsements in articles, blog posts, and other online editorial material, with the endorsements appearing close to hyperlinks to Legacy's website. In exchange, affiliates received substantial commissions on the sale of each product resulting from referrals. The Commission alleged that the company engaged in deceptive advertising—it represented that online endorsements written by affiliates reflected the views of ordinary consumers or "independent" reviewers, without clearly disclosing that the affiliates were paid for every sale they generated.

Another interesting Commission action enforcing our Endorsement Guides is our litigation against Russell Dalbey, the CEO and founder of the company behind the "wealth-building" program "Winning in the Cash Flow Business."[10] In this case, the Commission—along with the Colorado Attorney General—is challenging infomercials claiming that consumers could make large amounts of money quickly and easily by finding, brokering, and earning commissions on seller-financed promissory notes. The litigation is currently pending.

Along with the Dalbey complaint, the FTC and the Colorado AG announced a settlement with one of the consumers who offered a testimonial in a Dalbey infomercial. We alleged that this endorsement was deceptive. Marsha Kellogg claimed that she earned almost $80,000 from just one promissory note transaction using Dalbey's program. And she claimed that her total earnings were more than $134,000. The complaint alleges that Kellogg made this statement even though she earned $50,000 less than what she claimed. Kellogg agreed to an order settling the FTC charges against her. The order is the FTC's first against a consumer charged with making misrepresentations in a testimonial.

I've spent my time with you this morning talking about consumer trust. Trust in what consumers see, trust in what they hear, and trust in what is being done with information about them.

As a Commissioner at the Federal Trade Commission, consumers rely on me to maintain that trust. And I am relying on you to continue to do the right thing by consumers, your customers.

Thank you for giving me the opportunity to spend some time with you this morning.

---

[9] *See* In the Matter of Legacy Learning Systems, Inc.; FTC File No. 1023055 (June 2011) (consent decree).

[10] *Federal Trade Commission and State of Colorado, ex rel. John W. Suthers, Attorney General, Plaintiffs v. Russell T. Dalbey; DEI, LLLP; Dalbey Education Institute, LLC; IPME, LLLP; Catherine L. Dalbey and Marsha Kellogg, Defendants* No. 11-CV-1396-RBJ-KLM (D. CO. Oct. 11, 2011) (Order for Preliminary Injunction).