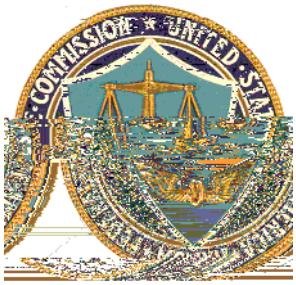

Federal Trade Commission

Consumer Protection 2015: Back to Basics for the New Media

Jessica Rich[1]
Director, Bureau of Consumer Protection, FTC

Kelley Drye & Warren LLP – Advertising and Privacy Law Summit
June 11, 2015

I'm delighted to be here to kick off this interesting event. I'd like to use my time this morning to talk about the FTC's latest work in advertising and privacy. That's much broader than the Internet of Things, the unifying theme for this event. But the Internet of Things is indeed a fitting backdrop since it encapsulates many of the broader consumer protection challenges we face today.

For starters, data is collected from and about consumers wherever they go – through their smartphones, wearables and fitness devices; in their smart homes and smart cars; as they shop in stores and online; as they check and update their many social networks; as they walk down the street; everywhere.

[1] The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner.

Advertising, too, is coming at consumers from every angle, through their many smart devices, in every conceivable format. Fantastical products make fantastical claims. Companies send you ads about cures for colds that you just caught yesterday. Those shoes you viewed online five minutes ago follow you everywhere. Ever

the risk of allergies, but we alleged that it didn't have sound scientific evidence to back that up. The case is pending in federal court.

In a similar vein, we took action against shipment broker uShip and freight in February for failing to disclose that it provided discounts and awards to customers who posted reviews of its service.

Finally, to provide guidance in this important area, we recently updated the FAQs for our Endorsement Guides.[3] The revised FAQs take a deeper dive into forms of promotion that were relatively new when we did our last update – for example, Twitter, affiliate marketing, "like" buttons, employee endorsements, solicited endorsements, and uploaded videos, to name just a few.

Clear and Conspicuous Disclosures

Finally, I want to address a significant issue that runs through all of our work – disclosures. By disclosures, I mean information needed to prevent an ad from being deceptive. The law is pretty basic here too: Disclosures must be clear and conspicuous. To accomplish this, advertisers should use direct and unambiguous language and make the disclosure stand out. If a disclosure is hard to find, tough to understand, buried in unrelated details, or obscured by other elements in the ad, it's not clear and conspicuous. This is true not just in print, but online and on mobile. We have an excellent guidance piece on this – *Dot Com Disclosures*, which we recently updated to provide specific guidance for making disclosures on mobile devices, Twitter, and other new media.[4]

Many of our cases involve problems with omitted or buried disclosures. So last year, we launched a project called *Operation Full Disclosure* to remind companies of the

[3] *The FTC's Endorsement Guides: What People Are Asking* (May 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking

[4] *.com Disclosures: How to Make Effective Disclosures in Digital Advertising* (Mar. 2013), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/com-disclosures-how-make-effective-disclosures-digital.

importance of clear and conspicuous disclosures. We contacted over 60 companies, including 20 of the biggest advertisers in the country, to alert them to problems with disclosures in their TV and magazine ads. The response to our outreach has been very positive but you can expect more work in this area.

On the Horizon

That's a snapshot of our advertising work this year, and I haven't even talked about our extensive work on green claims and auto ads, or our big case against DIRECTV. For the upcoming year, we'll continue to focus on health claims of all sorts, especially cognitive claims, as well as endorsements and disclosures. In the fall, we'll host a workshop on over-the-counter homeopathic products to examine how these products are being marketed and advertised. And we'll issue guidance on Native Advertising by the end of the year.

II. Privacy

Now I'll move to our privacy program. Earlier, I talked about the ubiquity of data collection. But it's also invisible in many ways. Most of the companies that collect consumers' data online and through their mobile devices are behind the scenes and never interact with consumers. And as we move into the era of the Internet of Things, data collection will become even more invisible.

Our privacy program focuses on three related areas designed to protect consumers in this environment – Big Data, Sensitive Data, and New Technologies.

Big Data

First is Big Data, by which I mean the vast collection of detailed data about consumers for use in making predictions about their behavior or likely outcomes.

Big Data can, of course, drive valuable innovation across many fields – medicine, education, transportation, and manufacturing. But it also raises privacy concerns for consumers – massive collection and storage of personal information; the risk that detailed profiles will fall into the wrong hands, enabling identity theft and other harms; the release of sensitive information consumers regard as private; and the potential use of this data by employers, insurers, creditors, and others to make important decisions about consumers.

Our central message is that, even in the face of rapidly changing business models and technologies, companies still need to follow the basic privacy principles that D collect or retain more data than you reasonably need. If you must collect it, consider de-identifying it to minimize any harm if it falls into the wrong hands. Tell consumers how you plan to use and share their data. Give consumers meaningful choices about their privacy. And protect consumer data from unauthorized access. As new business models and technologies develop, these principles remain relevant and important, although they do need to be adjusted and adapted.

We've emphasized these principles through both policy initiatives and enforcement. In January, we issued a staff report setting forth a number of recommended best practices for the Internet of Things.[5] One issue we addressed was the question we

[5] FTC Staff onsumTv-/Td [4

hear again and again about whether notice and choice have continuing relevance, given the lack of traditional screens or interface to communicate with consumers. Our answer was "yes," and the report discussed the different tools that IoT companies are using to communicate with consumers – such as point of sale disclosures, setup wizards, or even codes on the device. The report also discussed the importance of reasonable collection limits, de-identification of data, and strong security measures.

In addition, last year, we hosted a workshop entitled *Big Data: A Tool for Inclusion or Exclusion?*[6] The workshop explored how the categorization of consumers may be both creating and limiting opportunities for consumers, with a focus on low income and underserved consumers. We plan to issue a report on this topic in the coming months. One of our main messages is – there are laws on the books that address many of these concerns and companies must comply with them.

For the past few years, we've also focused a lot of attention on the unique privacy challenged presented by the data broker industry. Last year, we issued a report on these entities, showing the enormous number of data points they collect on each consumer, the profiles and categories they use to characterize individuals, their many sources of data, and the clients they sell to – which *do* include employers, insurers, and creditors.[7] We also brought a number of cases against data brokers selling information for purposes covered by the Fair Credit Reporting Act without complying with that important law.

---

[6] *See generally* https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion

[7] FTC Report, *Data Brokers: A Call For Transparency and Accountability* (May 2014), *available at* https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014

We remain very concerned about the invisibility of these practices to consumers. And it's not just about privacy. Increasingly, we are seeing a link between data brokers and fraud. In fact, we often discover in our fraud cases that the scammers used highly sensitive data bought from another company – including Social Security and bank account numbers – to trick or steal from consumers. This data goes well beyond the

defendant Craig Brittain solicited sexually explicit photos from women's ex-boyfriends and others – in many cases through deception – to post on his website, isanybodydown.com. He then used another site to pose as an attorney and charge $250 for removing the information. The Commission also issued a unanimous summary decision finding law violations by Jerk.com. That case involved photos of kids and teens being labeled a "jerk," supposedly by their peers.

Data security is also a huge part of our work to protection sensitive information. Over the past 15 years, we've brought over 50 enforcement actions against companies that failed to implement reasonable security protections – including companies such as Microsoft, TJX, Lifelock, and CVS. Our 50th case, announced last August, was against GMR Transcription Service, a company whose poor security practices, we alleged, exposed the medical information of thousands of consumers on the Internet. This year, we are taking our message on the road, gearing up for a campaign called *Start with Security*, in which we will host events around on the country on security topics and best practices. We also will continue to put out business guidance, including a new piece soon on lessons learned from FTC cases. The Commission, of course, also unanimously supports new federal legislation to enhance our authority in this area.

Finally, the FTC has a special interest in protecting the privacy of kids. To date, we've brought 25 cases in this area, including two COPPA cases last fall against the mobile app for Yelp and the gaming app *TinyCo*. Each company paid substantial civil penalties.

Mobile and Tech

A third area of focus for our privacy program is mobile technologies and, indeed, tech more broadly. In the past few years, this area has become one of the main priorities at the FTC – in privacy and more generally. For example, we've brought cases against Apple, Amazon, and Google related to kids' in-app purchases; against T-Mobile and AT&T for mobile cramming; and against AT&T and TracFone for making allegedly false claims that they provided "unlimited data" to their broadband customers. These cases are all about applying basic consumer protection rules to the growing mobile platform.