

Connecticut State Bar Association
Antitrust and Trade Regulation, Consumer Law and Federal Practice Sections
Keynote Address
March 15, 2011

“Hot Topics at the Federal Trade Commission”

Good evening. Thank you, Bob [and Erika] for inviting me to be with you this evening, and for that kind introduction.

It is great to be here in New England. As you just heard, I came to the Federal Trade Commission from Vermont via North Carolina. When I moved to our nation’s capitol, I knew I would have to adjust a bit: to big city life, big city politics – and even a whole new lingo. In Washington, just as Steve Martin once said about the French, “they have a different word for *everything*.”

“Spin” has nothing to do with wash cycles. The “tea party” does not serve cucumber sandwiches. And “shovel ready” is not the back-up plan for when the plow truck runs out of gas.

And perhaps the hardest for me to adjust to: in D.C., “snow” means “panic” – all out, abandoned cars, closed freeways, shutdown-the-government panic. And, of course, they have their own, typically hyperbolic, words for a blizzard: “Snowmageddon” and “Snowpocalypse.” Honestly, New Englanders drive better in a white-out than Washingtonians

Change: A Proposed Framework for Business and Policymakers.” In that report, we highlight several threats to consumer privacy that most consumers don’t even know exist.

For example, if you browse for products and services online, entities that place ads on the sites you visit might collect and share information about your activities, including your searches, the websites you visit, and the content you view. If you participate in social networking, third-party applications are likely to have access to the information you or your friends post on the site. If you use location-enabled Smartphone applications, multiple entities might have access to your precise whereabouts. And if you use loyalty cards at a grocery store or send in a product warranty card, your name, address, and information about your purchase may be shared with data brokers and combined with other data.

These practices go from creepy to downright disturbing when they involve sensitive data, like medical conditions, and sensitive users, such as children. We’ve heard that some consumers refuse to seek early treatment and online information for cancer for fear that information about their condition will get out. A Wall Street Journal article reported that some data brokers list elderly patients who suffer from Alzheimer’s disease and similar maladies as “perfect prospects for holistic remedies, financial services, subscriptions and insurance.”

We hear in “scrape” information about particular consumers on the web – including on social network sites information to insurers, lenders, and other financial firms. These financial firms then use this information in making decisions about whether – and on what terms – to provide financial products to the consumers.

Last fall, the Wall Street Journal published a report about a life insurer that had developed a way to use information – bought from third party data brokers – about consumers’ consumption patterns to make decisions about their life expectancy, and hence rates and coverage. Other larger insurers are also interested in using this technology.

The insurers justify this as a convenience and cost saving measure for their customers. Maybe. But I hope that doesn’t mean that your membership in the cupcake-of-the-month club and clicking on that “lose embarrassing belly flab” link starts to identify you as at risk for diabetes, causing your insurance rates to go up.

In essence, whenever we go online, we unwittingly allow invisible cookies to follow our every perusal, post, and purchase. Again without our consent, and often without our knowledge, this information – data miner’s gold – is bought and sold in a thriving market. There is no doubt that there is big money in information about what makes the American consumer click – literally.

There is also no doubt that that same money helps keep the content on the web creative and free. Most people like that, and would be quite upset if all of the companies that provide free content on the web started to charge consumers before they could access it. And many – including me – prefer the targeted ads that behavioral advertisers generate, even when we know those ads are based on unauthorized, undetected snooping.

But what if my health insurer raises my rates when I go online to cancel my fruit-of-the-month club membership and sign up for a cake baking class instead? Or what if the rates on credit cards that I'm offered go up as a result of my online searches for debt relief services?

When we enter cyberspace, we not only lose control over what information about us is collected; we also lose control over who gets access to that information and what they do with it.

The FTC is determined to return some of th

can make some of those speedy lies and half-truths seem like the unbiased opinion of a trusted friend.

We saw that just recently when the rapper 50 Cent mentioned the penny stock H&H Imports in a series of tweets. The stock price jumped 240%. 50 Cent later tweeted two further messages to his network: one said, “I own HNHI stock. Thoughts on it are my opinion. Talk to financial advisor about it.” He followed this with: “HNHI stock is the right investment for me it may or may not be right for u! Do ur homework”.

Let’s leave aside for a moment the question of whether people who take investment advice from rappers named after money – and not a lot of money at that – deserve what they get.

jobs and work-at-home opportunities. One company advertised fake jobs on careerbuilder.com and charged job-seekers fees covering supposed background checks. The company raked in at least \$8 million from defrauded consumers.

This coordinated law enforcement sweep was impressive in its scope: It included three new FTC enforcement actions, 48 criminal actions by the Department of Justice, seven civil actions by the U.S. Postal Inspection Service – and 28 actions by 10 states and the District of Columbia.

We have brought many consumer protection cases involving scams intended to take the last dime from consumers suffering from the downturn. In the past 2 years, we have brought 30 cases against scams designed to fool consumers into purchasing plans that will reduce their mortgages or prevent foreclosure, and our partners in the states have brought over 200 similar cases.

And last August, the FTC and 24 states worked together in “Operation Healthcare Hustle.” This coordinated law enforcement sweep involved a total of 54 lawsuits and regulatory actions against sellers of phony “medical discount plans” that masqueraded as health insurance.

We have also worked closely with the states in competition initiatives, including one of our highest priorities: promoting competition in health care markets. For example, in January we jointly filed suit with the State of Ohio to stop the merger of two competing hospitals in Toledo, Ohio. Our request for a preliminary injunction is pending in federal district court.

Last November, we entered a consent decree in a merger case that preserves competition among psychiatric hospitals in Delaware, Puerto Rico, and Las Vegas, Nevada. We worked very closely with state officials in that matter as well. Finally, our efforts to stop anticompetitive pay-for-delay agreements in the pharmaceutical industry continue.

Finally, I wanted to highlight a recent enforcement action that I know has made a difference here in Connecticut over this past winter. In November 2009, the Commission entered a consent decree in a merger case that preserved competition in markets for road salt in Connecticut and Maine. We worked very closely with the office of then-Attorney General Blumenthal, as well as other state attorneys general, in thnytop.6dene17been.betber 20Gi-20myecks. The c.145 7

The new Bureau is in its beginning stages. It will not be formally operational until July, and undoubtedly it will take some time after that to get to the point where it is exercising its full regulatory, enforcement, and supervisory authority. During this interim period, I believe it is critically important for the FTC – and the states – to fill the gap by continuing to use the tools and capabilities at our disposal to protect consumers during these tough economic times.

Looking further into the future, the FTC retains all of its current enforcement jurisdiction under Dodd-Frank. In fact, the FTC will have the authority to enforce certain rules promulgated by the CFPB – as the CFPB will have the authority to enforce certain FTC rules. But I don't think anyone should worry about the federal agencies playing "double team". I'm quite confident that – unfortunately – there will be plenty of work to go around. There are simply too many scam artists looking to prey on vulnerable consumers for either the FTC or the CFPB to double up on companies who violate the law. And Dodd-Frank requires the FTC and the CFPB to enter a Memorandum of Understanding to ensure that the agencies coordinate on enforcement actions and avoid wasting scarce government resources. I'm sure we will have a good working relationship with the new Bureau, just as we've had with our other partners at the federal level and in the states.

Whether it be protecting consumer privacy or shutting down deceptive advertisers, the FTC strives to speak a language more common outside the beltway. We try to speak a language of honesty and clarity.

Because at the FTC, we believe that – as long as the rules are fair and direct – as long as individuals' rights are respected – as long as bad actors and unscrupulous scammers are kept at bay – American markets work, American businesses prosper, and the American economy produces high quality jobs.

Thank you for your attention. I'm happy to answer your questions.