Remarks by Commissioner Julie Brill
United States Federal Trade Commission

before the
Trans Atlantic Consumer Dialogue
27 April 2010
Washington, DC

Good afternoon. I am honored to be here today, and I would like to thank TACD for the invitation to speak to you. As you may know, I am a newcomer to the Federal Trade Commission: I was sworn in as a Commissioner just a couple of weeks ago. But I am not a newcomer to working on behalf of consumers. For more than 20 years, I have worked with state attorneys general throughout the United States to protect consumers from unscrupulous business practices, first from my position in the Vermont Attorney General's office, and more recently in the North Carolina Attorney General's office. I see quite a few long-time friends among the crowd. I look forward to working with all of our transatlantic counterparts from the European Commission and European consumer organizations in the coming months and years.

TACD is an important forum for government officials and consumer advocates to speak directly to each other about critical issues affecting consumers in today's global economy. Today's agenda has covered a lot of ground. Many of the topics discussed today — consumer finance, food marketing, and privacy — are not only important to European and American consumers. They are core areas of focus at the FTC, and they are also issues that I have worked on throughout my career. I'd like to take a few minutes to share with you some of my thoughts about these issues.

First, the financial crisis. As we are all acutely aware, the recent global economic downturn was just that: global. And it has taken a toll on consumers everywhere. At the FTC, we've learned that when hard times hit, scam artists hit harder.

One of the greatest challenges that many consumers face today is holding on to their homes when they've lost their jobs, seen their working hours cut b

The Interagency Working Group's recommendations will not be in the form of proposed regulations. But that doesn't mean the recommendations shouldn't be taken very seriously. They will represent the collective thinking of the best experts in health, nutrition, and marketing in the government. We expect that the food industry will voluntarily comply with the final standards the Working Group develops.

While the Working Group's report has not yet been issued, I'd like to share with you some of its tentative recommendations:

1.

scope of personal information Sears collected from consumers via a downloadable software application.[7] According to the FTC's complaint, Sears paid $10 to consumers who visited the company's websites and agreed to download "research" software that the company said would confidentially track their "online browsing." In fact, the software collected vast amounts of information, including the contents of consumers' shopping carts, online bank statements, prescription drug records, video rental records, passwords, and library borrowing histories. Only in a lengthy user license agreement, available to consumers at the end of a multi-step registration process, did the company disclose the extent of the information the software tracked. The FTC's settlement with Sears requires the company to stop collecting data from consumers who downloaded the software, to destroy all data it had previously collected, and not to engage in similar conduct in the future.

The challenge today is to create an online ecosystem with meaningful consent and more transparency. In the context of online behavioral advertising, we have encouraged companies to come up with innovative ways to provide greater transparency in their interactions with consumers. This does not mean privacy policies hidden somewhere on the company's web site. What is needed instead is a more dynamic form of disclosure, what some call "just-in-time" disclosure. For example, when serving a consumer an ad, a link in close proximity could say "why am I getting this ad?" The linked text could explain that the consumer's information had been collected in order to deliver the targeted ad.

Another model that we are revisiting is one concerning consumer harm that results from privacy breaches. Currently, the formulation for consumer harm only recognize a narrow set of tangible harms in assessing whether privacy violations occurred. But we know that, in today's environment, consumers experience a broader range of privacy-related harms, including reputational harm and unexpected or surprising uses of their information. In the department store case I just described, consumers suffered a harm even if their wallets didn't suffer, and even if they didn't realize it. Most of the consumers didn't know about the massive harvesting of information that was taking place.

Assessing emerging technologies and anticipating what lies ahead is critical in contemplating frameworks that might be more appropriate for evaluating whether certain practices impact consumer privacy. Online behavioral advertising, cloud computing, and mobile marketing are just a few areas that we are taking a hard look at to identify how they impact consumer privacy. For example, in connection with cloud computing, we are engaging with industry players to try to get a better understanding of how to define cloud computing, how the model is evolving, and what new or unique issues it might pose for consumers. Industry's views — and actions — around these issues will likely have an impact on whether new rules are warranted.

We are also looking closely at third party applications on social networking sites and P2P file sharing. Many consumers may not be familiar with how such applications could be used to

[7] *In the Matter of Sears Holding Corp.*, FTC Docket No. C-4264 (Decision and Order entered Sept. 9, 2009) (press release *available at*

gain access to their data. For instance, consumers may not be aware that the software they download to share music files can give strangers access to all of the personal data from their computers.

Another privacy issue we are focusing on is health privacy. The electronic processing and storage of personal health records allows that information to be shared more readily and no doubt will improve delivery of health care through greater accuracy in tracking disease, creating personalized medicine, and medical research. But more universal use of electronic health records will also entail privacy and security risks. Because of these concerns, the Recovery Act of 2009 required health record breach notification rules to be put in place. These rules, which are now effective, are enforced by the FTC and the Department of Health and Human Services.[8]

Breach notification is not a new area to me – more than 45 states have legislation requiring notification of security breaches involving personal information. Indeed, as some of you know, the states have long been the national leaders in the area of security breach notification. I am pleased to see that the federal government is catching up to the states in this area.

Another FTC priority in the privacy realm is international enforcement cooperation. As in many other consumer protection areas, we worry0 12 n mb9e(e)ealt rewif Houy otunles to8J 13.36 0