Remarks by Commissioner Julie Brill
United States Federal Trade Commission

Conference of Western Attorneys General Annual Meeting
Privacy 3.0 Panel

Santa Fe, New Mexico
July 20, 2010

Good afternoon and thank you for that very kind introduction. "Privacy 3.0" is a good title for this panel. I have spent a lot of time thinking about privacy over the past twenty years. From my perspective, during the last year or so, it seems we have entered a third realm of privacy regulation, the "3.0" stage. What I would like to do this afternoon is spend a little bit of time talking about the different stages of privacy regulation from the perspective of the Federal Trade Commission as well as from the states.

Please note that the things I say this afternoon are my personal views. I am not here representing any of the other Commissioners or the Commission as a whole.

Let us go back and think about the early stages of privacy regulation in the 1990s. "Privacy 1.0," from my perspective, was the "Notice and Choice" Model. We called it the "Fair Information Practices" principles. Although you might not be familiar with that title, everyone is familiar with the underlying principles. During this stage, the FTC and the states looked at privacy issues through a regulatory framework that called for notice, choice, access, and security with respect to information. We evaluated privacy policies that way: privacy policies on the web, practices of companies, and various self-regulatory regimes were all examined through the lens of Fair Information Practices.

The FTC, the states, and many consumer advocates called on Congress to enact these Notice and Choice principles into law. However, Congress did not enact sweeping legislation on these broad principles. But it did enact the Gramm-Leach-Bliley Act, which many of you are familiar with.[1] The GLB Act embodies Notice and Choice principles. Consumers are given a one-time notice. They are required to read it, understand it, and make an intelligent choice that often will last for a long time. It is an interesting model and I am going to have some thoughts and critiques about it in a moment.

Shortly after GLB was enacted, the Federal Trade Commission, as some of you know, switched gears, and moved from "Privacy 1.0" to "Privacy 2.0." It moved from a regulatory framework focused on Fair Information Practices to one focused on principles of harm. The Harm Model was first launched by former FTC Chairman Tim Muris, but it since has been embraced by many people, including in the states. The Harm Model focuses on harmful privacy practices that present risks of physical security or economic injury. As a result, the Federal Trade Commission, and the states, started focusing on

[1] 15 U.S.C. §§6801-6809 (1999).

data security, data breaches, identity theft, and children's online privacy, as well as issues such as spam, spyware, and telemarketing, including the Do Not Call list.

Let me expand a bit on the first two issues, data security and data breaches. During the Privacy 2.0 timeframe, regulators focused on enhancing tools to address data security and data breaches. First and foremost, the states, led by California but followed by many other states, enacted data security laws that required notification to consumers about data breaches. The Federal Trade Commission and other federal regulators adopted the Safeguards Rule under the Gramm-Leach-Bliley Act.[2] The GLB Act focused on financial institutions, and in that context included data security issues.

Within the Privacy 2.0 framework, the FTC started looking at various cases that came to light as a result of the states' breach notification laws. The FTC and the states analyzed the matters under Section 5 of the FTC Act and similar state laws, which prohibit unfair and deceptive acts and practices in commerce. In investigating security breach matters, the FTC asked "Was there deception or unfairness in the way that the companies were notifying consumers about their privacy practices, and in the way that they were implementing their privacy practices?" This analysis fell within the Harm Model—we were looking for harm to consumers—and it employed the FTC Act and the states' unfair or deceptive acts and practices laws to examine privacy issues within that rubric.

There were many enforcement cases brought during this era by the states and the FTC. Cases like *ToySmart*, *BJs*, *ChoicePoint*, *TJX* (parent of TJ Maxx), *LifeLock*, and most recently the Commission's settlement with Twitter fall under Privacy 2.0 and the Harm Model.[3] With respect to the recent *Twitter* case, we asked: "what did Twitter say it was going to do with respect to customers' information, what were its actual practices, and did the deviations between its promises and practices present potential harm to consumers?" This was typical of the type of Harm Model issues we examine in the Privacy 2.0 framework.

In addition to security breaches, there has also been an emphasis on identity theft issues, with attention paid to enhancing tools regulators have with respect to identity theft. The Fair and Accurate Credit Transaction Act (FACTA),[4] for example, allows consumers to obtain free credit reports once a year from each credit reporting agency, to allow consumers to determine whether or not they have been victimized by identity theft. Consumers can look at their credit report and make a determination on their own as to whether suspicious accounts have been opened in their name, or whether other suspicious activity appears in their credit report.

---

[2] 16 C.F.R. Part 314.

[3] *See, e.g.*, FTC v. Toysmart.com, LLC and Toysmart.com, Inc., No. 00-11341-RGS (D. Mass. 2000); In the Matter of BJ's Wholesale Club, Inc., FTC Dkt. No. C-4148 (2005) (consent order); United

The tools and principles of the Harm Model have been very important over the past decade, and have been employed to good use by regulators. But industry has been moving forward in ways that are not necessarily addressed by this Harm Model. There have been substantial developments with respect to the Internet and electronic technology, which have become much more sophisticated in terms of how consumers' information is gathered, retained and used. Very rich ecosystems of data are being created and deployed, paving the way for some very sophisticated forms of advertising.

I would like to talk about one of these forms of advertising, which is known as behavioral advertising. In my view, our two prior privacy models—"Privacy 1.0" and "Privacy 2.0"—do not really address the concerns that are now aris