

I. Background

Let me begin with a very brief overview of the FTC's history of privacy protection. Privacy has been a core component of the FTC's consumer protection mission for decades. The Commission's work in this arena began with its implementation of the Fair Credit Reporting Act of 1970, which promotes the accuracy and privacy of credit reporting information. With the emergence of the Internet and e-commerce in the mid-1990s, the FTC's privacy agenda expanded to encompass online privacy issues. Of course, the rise of e-commerce meant that privacy issues became truly global in nature. For that reason, international outreach and cooperation has long been critical to our privacy work, and our involvement here in APEC has been and remains an important part of those efforts. In fact, just became one of the first participants in the APEC Cross-border Privacy Enforcement Arrangement.

While the FTC's commitment to consumer privacy has remained constant over the years, its enforcement efforts have reflected two conceptual approaches: the "notice and choice" and "harm-based" models. These approaches are well-known to you, as they are also reflected in the APEC Privacy Framework. The notice and choice model gained ascendancy in the mid-1990's, when the FTC began to focus on consumer privacy in the online context. As you know, this model emphasizes that businesses should provide notice of the information they collect from consumers and how they will use it so that consumers can provide informed consent to the collection and use of their information. The harm-based model gained ascendancy at the FTC in the early part of the last decade. In contrast to the notice and choice model, the harm-based model focuses on tangible harm to consumers resulting from misuse of their information. The harm-based

approach targets uses of information that create financial risks — such as identity theft; threats to physical security — such as stolen credit cards; and unwanted intrusions into consumers' daily lives — such as spyware, spam, and telemarketing.

II. Lessons Learned

The FTC's privacy reexamination is taking place against that backdrop. What has the FTC learned from its privacy roundtables? Several key themes have emerged.

At the outset, it is important to recognize that the free flow of information that consumers fosters the flow of free content and services to consumers online. Consumers derive tremendous benefits from the free content and services available online, which are made possible by online advertising. Privacy policy should take this into account.

But it has also become clear that current approaches to privacy have significant limitations. The notice and choice model puts too much burden on consumers to read and understand lengthy and complicated privacy policies that seem designed more to limit companies' liability than to communicate with consumers. To be sure, privacy policies play an important role in ensuring accountability, but they do not ensure meaningful consumer choice or inspire consumer confidence in a world in which data may be shared among numerous organizations for multiple, unanticipated purposes.

The harm-based model, on the other hand, has sometimes focused too much on financial harms to consumers and on harms when they occur, rather than taking preventive measures before the information is collected, used, or shared. That is not to say that tangible, financial harms are not important — they are, of course. But even where there may be no risk of economic harm, there are situations in which consumers may be injured when their personal information is shared. For example, a consumer may not want

company procedures, systems, and technologies at the outset, so that they are an integral part of a company's business model. This would include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, and implementing reasonable procedures to promote data accuracy. These measures would provide consumers with substantive protections without placing the burden on them to read long notices and make detailed choices. The FTC is therefore exploring how to encourage companies to incorporate these protections into their practices, whether there are other such protections that companies should consider, and how to balance the costs and benefits of such protections.

B. Simplifying Choice

Second, the FTC is considering how to simplify the privacy choices presented to consumers. One way would be to recognize that consumers do not need to exercise choice for certain commonly accepted business practices that consumers expect — for example, consumers naturally expect that an online vendor will share a consumer's address to the shipping company that will deliver the consumer's purchase. By eliminating the need to obtain a consumer's consent to this transfer of information, consumers can focus on the choices that really matter to them, and on uses of data that they would not expect when they engage in a transaction. Simplifying choice should also reduce the burdens on businesses. The FTC is considering how to define these commonly accepted business practices.

The FTC is also exploring — in cases where choice would be needed — how to make consumer privacy choices more meaningful. For example, rather than discussing

thoughts and ideas on the questions that the report raises. We value the input of our fellow APEC economies and invite your views.

Let me stop here and thank you for the opportunity to give you this update.