Federal Trade Commission

Asia Pacific Economic Cooperation
Electronic Steering Group Meeting, Data Privacy Subgroup
January 24, 2007
Canberra, Australia

Next Steps for Cross-Border Enforcement Cooperation

Remarks of Pamela Jones Harbour
Commissioner, Federal Trade Commission

I. INTRODUCTION

Good afternoon. I am Pamela Jones Harbour, a Commissioner at the United States Federal Trade Commission. I begin with the usual disclaimer: the views I express here are my own, and are not necessarily those of the Federal Trade Commission or any other individual Commissioner.

I am delighted to be here in Canberra at the APEC ECSG's Data Privacy Subgroup meeting. I would like to thank the Australian Government for hosting us here today and a special thanks to Colin Minihan from the Australian Government Attorney-General's Department for chairing this meeting. I am not sure if I can thank Colin for this, but I am grateful for the summer weather - a welcome reprieve from the winter coat, hat and gloves that I was wearing in Washington, DC.

I applaud the Data Privacy Subgroup on all the work it has already

accomplished. We all agree that the APEC Privacy Framework is an important vehicle to accommodate the different privacy approaches within the vast Asia-Pacific region. And I know that we all acknowledge that our work is not done. We just had a very productive two days at the implementation workshop and several interesting sessions on implementation today. As we have been discussing, these cross-border privacy rules would provide a mechanism to transfer data across the region, which is only becoming more and more crucial in the globalized economy that we live in today.

As a Commissioner at the Federal Trade Commission, the U.S. agency charged with protecting consumers, my perspective is one that always leads to the following question: "What does this mean for consumers?" I spent a number of years as a partner at a large law firm, and when you are at a law firm, you always think, "What does this mean for my client?" And so now, I look at it this way. I have quite a large client base in my current position as a Commissioner at the Federal Trade Commission. Consumers are my clients. And what do cross-border privacy rules mean for them?

Cross-border privacy rules, **if** implemented effectively, have the potential to provide more consistent and reliable privacy protections for personal information across the region. And, overall, such increased privacy protections could benefit consumers. In addition, consumers could also benefit in a number of ways from unrestricted information flows under cross-border privacy rules, which is another goal of the implementation of the APEC Privacy Framework. Unrestricted transfers

reduce costs to businesses that can be passed on to consumers. In short, cross-border privacy rules have tremendous potential, and we all recognize the importance of this work. The challenge ahead is to figure out a way to develop rules while accommodating differing legal systems, privacy frameworks, and enforcement approaches. It is against this background that I now describe new developments in the FTC's cross-border law enforcement authority.

II. THE U.S. SAFE WEB ACT AND INTERNATIONAL ENFORCEMENT COOPERATION

A. SAFE WEB Act Background[1]

I am pleased to report that the FTC has obtained new and expanded powers that will allow it to cooperate more fully with foreign law enforcement authorities in a variety of areas. The U.S. SAFE WEB Act, which was signed into law only last month – on December 22nd – provides the FTC with updated cooperation tools for the 21st century. And better cooperation will help the FTC to fight a range of practices that harm consumers.

There are a number of provisions of the SAFE WEB Act that are most relevant to international enforcement cooperation. Before outlining those, some background on this new law will provide you some additional insight on its importance.

As you may know, the FTC has the authority to take action against companies that engage in deceptive or unfair acts or practices. This broad authority is pursuant to Section 5 of the FTC Act. We have used the general authority of Section 5, as well as some other more specialized laws to take action against companies engaging in

unfair or deceptive practices relating to privacy and data security.[2] If a company misrepresents its privacy and data security policies and protections to the public, we can allege that they are engaging in a deceptive practice; and if a company does not have reasonable safeguards to protect sensitive consumer information, we can allege that they are engaging in an unfair practice if that practice causes substantial injury. Using these legal theories, the FTC has brought a number of high profile cases against large multinational corporations as well as cases against smaller entities.[3]

The broad and flexible language of Section 5 has allowed the FTC to confront practices that harm consumers – such as spam and spyware – that were unthinkable in 1938, when the FTC first obtained authority over "unfair and deceptive acts or practices." Other sections of the FTC Act – particularly those that relate to information-sharing and investigative assistance – have not been as adaptable.

For the most part, consumer protection used to be a domestic concern, and these information-sharing and investigative assistance provisions were part of a legal framework that developed in earlier days. In those days, the concept of cross-border commerce, and 24/7 cross-border computerized information flows was unimaginable. When the FTC Act first was written, American consumers did business directly with American firms, and American companies generally directed sales to American consumers. Of course, globalization of trade, improvements in telecommunications, and the Internet have changed this domestic focus. The growing use of network technologies and the rise of electronic commerce have created a global marketplace.

The consequences of the FTC Act's domestic focus first surfaced in our

mission to tackle cross-border fraud – problems like pyramid and lottery schemes, travel and credit-related ploys, and high-tech scams such as phishing and spyware. Because of antiquated consumer protection laws, government enforcement authorities around the world were constricted in their ability to keep up with con artists who were able to manipulate technology and national borders to strike quickly, victimize thousands of consumers in a short period of time, and disappear with their ill-gotten gains without a trace. These con artists were often able to escape prosecution because the authorities simply were unable to pursue them across national borders, or were unable to share crucial evidence with fellow enforcement partners in other jurisdictions.

To address these surmounting challenges, in 2003, the OECD, the Organisation for Economic Co-operation and Development, established guidelines on cross-border fraud enforcement cooperation.[4] These guidelines set forth a detailed framework for international cooperation to combat cross-border fraud. They include recommendations on notification, information sharing, assistance with investigations, and confidentiality. In April 2006, the OECD followed up on this initiative with new guidelines for enhanced cross-border law enforcement cooperation to combat spam.[5] And now, the OECD is currently working on similar guidelines for privacy enforcement cooperation.

At the same time that the OECD 2003 Guidelines were released, the FTC recommended that Congress provide the FTC with enhanced powers to combat cross-border fraud that closely tracked the OECD cross-border fraud guidelines. The result,

the U.S. SAFE WEB Act, will expand international cooperation in the area of cross-border fraud and other practices that are increasingly global in nature.

B. SUMMARY OF SAFE WEB PROVISIONS

We feel a great sense of accomplishment now that this law has passed, but our work is hardly done – it is just beginning. We need to take advantage of our new cooperation tools consistent with our policy goals and resources. I will now highlight for you some of the main features of SAFE WEB.

1. Sharing Compelled and Confidential Information with Foreign Law Enforcement Authorities

First, SAFE WEB authorizes the FTC to share compelled or confidential information – including documents and testimony – with its foreign law enforcement counterparts.[6] Before SAFE WEB, the FTC could only share such information with other federal, state, and local enforcers - not with foreign enforcers. Now, with SAFE WEB, the FTC can exercise its discretion to disclose this information, particularly when such sharing would help the FTC's own law enforcement efforts and help U.S. consumers. A good example of this is when the FTC and a foreign agency investigate the same targets.

Of course, certain conditions must be met before we are able to pass on compelled and confidential information about a common target. For example, we must first be provided with assurances that the information will be maintained in confidence. Also, we must also be provided assurances that the information will be used only for investigating or enforcing against a company engaging in possible

violations of foreign laws prohibiting fraudulent or deceptive commercial practices, or other practices substantially similar to practices prohibited by any law administered by the FTC. Essentially, this means that the FTC will look to see whether the foreign agency is acting under authority similar to the FTC's authority.

If these conditions are met, the FTC can now exercise its discretion to disclose compelled or confidential information. In the scenario where the FTC and a foreign agency are both investigating the same target, the FTC's ability to share more complete information about the target can streamline parallel investigations, help avoid duplication of efforts, and possibly speed up investigations. It could also be used to increase the quantity and improve the quality of evidence against the target.

2. Using Investigative Powers to Aid Foreign Law Enforcement Authorities

Second, SAFE WEB permits the FTC to use its investigative power on behalf of foreign law enforcement agencies.[7] In some cases, effective enforcement cooperation demands that the FTC reach beyond information already in its files and gather new information on behalf of foreign law enforcement authorities. Before SAFE WEB, the FTC could not have provide such assistance to a foreign agency – even if the foreign agency's investigation would ultimately benefit U.S. consumers. Now, if the FTC determines that the requested cooperation is consistent with its policy goals and resources, it can issue a civil investigative demand – essentially a subpoena – for documents and testimony to an entity located in the United States and share the information with the foreign agency. Before we use our investigative

powers, however, the FTC must – in addition to the criteria I mentioned concerning information sharing – consider whether: 1) the foreign agency would provide reciprocal assistance to the Commission; 2) the use of our investigative powers would prejudice the public interest; and 3) the foreign agency's investigation concerns practices that have caused injury to a significant number of persons.[8]

Under this section of the Act, the FTC also may initiate a proceeding under an existing federal statute to obtain testimony, documents, or things for use in a foreign or international proceeding.[9] This statute is frequently used when foreign proceedings are already in progress, and the foreign litigant needs to obtain evidence from the U.S. expeditiously.

3. Protecting the Confidentiality of Information from Foreign Sources

Third, the U.S. SAFE WEB Act enables the FTC to obtain information it would not otherwise receive from foreign entities. On the government-to-government level, it protects the confidentiality of information provided to the FTC by a foreign government agency if the foreign authority requests confidential treatment as a condition of providing the information.[10] This addresses the concern expressed by some foreign government agencies that materials they share with the FTC might be publicly disclosed in response to an inquiry under the U.S. Freedom of Information Act, FOIA, which allows any interested person to request the FTC's records on any matter. Now, under SAFE WEB, the FTC will be able to guarantee confidentiality and thereby obtain some extremely valuable information.

This exemption from public disclosure also applies to consumer complaints that the FTC receives from foreign government and private sector sources, as well as consumer complaint information submitted to joint consumer complaint projects such as the international website *econsumer.gov*. This type of consumer complaint information can be extremely useful in investigating cross-border matters, and we believe that our ability to protect this information from disclosure will increase the volume of the information that we receive.

4. Strengthening Enforcement Relationships

Finally, the U.S. SAFE WEB Act contains several provisions that will strengthen the FTC's enforcement relationships both bilaterally and within multilateral organizations such as APEC. For example, SAFE WEB permits the FTC to spend funds, within specified limits of course, on projects and consultations with cooperative foreign law enforcement organizations.[11] It also permits the FTC to enter into international cooperation agreements when such agreements are required as a condition of reciprocal assistance.[12] SAFE WEB also allows the FTC to participate in meaningful staff exchanges with foreign counterparts.[13]

As these examples show, SAFE WEB provides the FTC with expanded tools for international enforcement cooperation that the FTC can use, when appropriate, to address the consumer protection challenges of our increasingly global and technological world.

I appreciate the opportunity to speak with you today and I look forward to the remainder of the program tomorrow. Thank you.

ENDNOTES

1. U.S. SAFE WEB Act of 2006, Pub. L. No. 109-455.

2. Specialized statutes include the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, and the Fair Credit Reporting Act, 15 U.S.C. § 1681.

3. *See e.g.*, *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006) (FTC alleged that data broker failed to use reasonable procedures to screen prospective subscribers resulting in sale of consumer information to data thieves; settlement reached with an order of $10 million in civil penalties, $5 million in consumer redress, and injunctive provisions); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (FTC alleged that retailer of pet products and services misrepresented the security measures it took to safeguard consumer information; settlement reached requiring the company, among other things, to implement a comprehensive information security program for its web site). More information about these two cases, as well as the FTC's other privacy and security related cases, are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

4. Recommendation of the Council concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders [C(2003)116)], available at http://www.oecd.org/dataoecd/24/33/2956464.pdf.

5. Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws against Spam[C(2006)57], available at http://www.oecd-antispam.org/article.php3?id_article=237.

6. SAFE WEB, *supra* note 1, at § 4(a), 6(a).

7. *Id.*, § 4(b).

8. *Id.*, § 4(b).

9. 28 U.S.C. § 1782.

10. SAFE WEB, supra note 1, at § 6(b).

11. *Id.*, § 4(b).

12. *Id.*, § 4(b).

13. *Id.*, § 9.