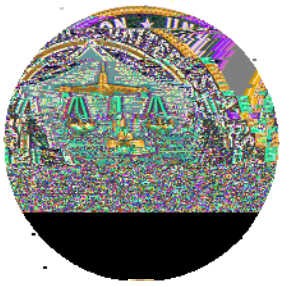

Federal Trade Commission

[1] The views stated here are my own and do not necessarily reflect the views of the Commission or other Commissioners. I would like to express my gratitude to my attorney advisors, Elizabeth Delaney and Holly Vedova, for their contributions to this paper.

what I think are the principal ones.

I. Product markets are increasingly worldwide in their scope.

There are exceptions, to be sure. "Polly Pockets" still wear national garb, and therefore the markets for those products tend to be national in their dimensions. Vehicles still drive on the left in the U.K. and Japan, and vehicles that ar

[2] *See Dialing for Dollars*, Online NewsHour, Nov. 5, 2002, transcript available at www.pbs.org/newshour/bb/asia/july-dec02/telemarketing_11-05.html; Anthony Mitchell, *The Call Center Compliance Mess*, E-Commerce Times, Oct. 14, 2004, available at www.ecommercetimes.com/story/37330.html.

[3] *See, e.g., FTC v. 3R Bankcorp, et al.*, No.: 04C 7177 (E.D. N. Ill,. filed May 17, 2006)(call centers located in Canada and India falsely promised consumers a "guaranteed" low-

interest credit card for an advance fee); *FGH International et al.*, No. CV04-8103-AHM (JWJx)(C.D. Cal., filed Sept. 27, 2004)(corporate defendant and telemarketing boiler room based in Peru); *4086465 Canada, Inc., a corporation d/b/a International Protection Center, et al.*

Second, there are practices that disincentivize use of the Internet altogether.[7] These include things such as identity theft and other forms of invasion of privacy that can occur when Internet transmissions are highjacked or computer systems are hacked. And, this also includes instances where unreasonable and inappropriate security practices result in flaws and vulnerabilities in data security systems.[8]

Third – and this pertains specifically to efforts by firms to transmit employee and customer information to their various offices located in other countries – disparate national standards and rules governing whether and how such data transmissions can lawfully occur may

---

available at www.ftc.gov/os/caselist/0423205/0423205.htm; *In re Zango, Inc. et al.*, File No. 052 3130 (issued Nov. 2, 2006) (consent order) available at www.ftc.gov/os/caselist/0523130/index.htm*; In re Direct Revenue, LLC et al.*, File No. 052 3131 (issued Feb. 20, 2007) (consent order) available at www.ftc.gov/os/caselist/0523131/index.htm.

[7] One survey, for example, found that, as a result of fears about protecting their identities, 30 percent of consumers polled were limiting their online purchases, and 24 percent were cutting back on their online banking. *See* Jennifer Cummings, *Substantial Numbers of U.S. Adults Taking Steps to Prevent Identity Theft*, Wall St. J. Online, May 18, 2006, available at www.harrisinteractive.com/news/newsletters/WSJfinance/HI_WSJ_ PersFinPoll_2006_vol2_iss05.pdf.

[8] In a number of cases, the Commission has alleged that security inadequacies led to breaches that caused substantial consumer injury and were challenged as unfair practices under the FTC Act. *See, e.g., In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sep. 5, 2006); *In the Matter of DSW, Inc*., FTC Docket No. C-4157 (Mar. 7, 2006); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sep. 20, 2005).

In other cases, the Commission has alleged that a company has misrepresented the nature or extent of its security procedures in violation of the FTC Act's prohibition on deceptive practices. *See, e.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Apr. 23, 2007); *In the Matter of Nations Title Agency, Inc*., FTC Docket No. C-4161 (Jun. 19, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of MTS Inc., d/b/a/ Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (Jul. 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

[9] *See* Miriam Wugmeister, Karin Retzer, and Cynthia Rich, "*Global Solutions for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules*," 38 Geo. J. Int'l L. 449, 469-77 (2007).

[10] FTC Staff Report, *Broadband Connectivity Competition Policy*, Jun. 2007, available at Broa/v07or30raff R.pdfe atET Rag130.1j/50c0gs6.41431 g6001 re0

computer network technology, and DVD encryption technology are just a few examples of the fruits of standard-setting processes.

In the computer memory chips industry for example, manufacturers have utilized the JEDEC Solid State Technology Association (previously known as the Joint Electron Device Engineering Council) to develop standards for computer memory chips. JEDEC develops standards for dynamic random access memory (DRAM), the most common type of memory used by computers, among other things. JEDEC was first created in 1960 and today some 290 companies that either make or use semiconductors and related services and equipment participate together in 50 different committees within JEDEC to develop standards for all different aspects in the industry. The standards they generate are adopted all over the world.

In the computer network technology industry, standards are particularly important because they help ensure that equipment manufactured by different manufacturers works together on the same network, thereby increasing competition in the industry. The Institute of Electrical and Electronics Engineers (IEEE) is the leading body that writes standards governing the physical aspects of local area networks (LANs).

Another example involving standard setting (or at least an industry trade association's development of something akin to a standard) is in the DVD industry. DVD encryption technology developed by the DVD Copy Control Association (DVD CCA) allows movie studios to offer their copyrighted films to consumers in digital format without risk of illegal copying. To prevent the illegal copying of DVDs, manufacturers encrypt, or scramble the digital signal. Technology known as Content Scramble System (CSS) developed by the DVD Copy Control Association unscrambles the content so it can be viewed on DVD players or personal computers.

complementary products or to disfavor the complementary products of a competitor. This was alleged in the *Microsoft* cases involving its operating system and browser.[14]

Another form of resistance is simply a refusal to configure products so that they are interoperable. All of you are familiar with the developments to date with respect to digital music. Apple, Microsoft, Sony, and others have developed different digital rights management (DRM) technologies to encrypt digital content, and these competing standards limit interoperability.

Apple has sparked the most controversy largely because of the huge success of iTunes and iPod. Apple has refused however to license its DRM solution – FairPlay – to third parties and its refusal to use anything but FairPlay – has meant that there is limited interoperability between Apple's products and competitor's products. This has made it difficult for the average consumer to transfer music from iTunes to third party devices. It also means that it is difficult to play music encrypted with third-party DRM on an iPod.[15]

As many of you are aware, this has led some to argue that Apple's tactics violate the antitrust and consumer protection laws. For example, in the United States, a class action

---

[14] *United States v. Microsoft*, 253 F.3d 34 (D.C. Cir. 2001); Commission Decision, COMP/C-37.792 Microsoft, Case T-201/04R, art. 1(1), art. 5(a) (Mar. 24, 2004).

[15] However, iPod owners are not necessarily locked into iTunes for music – there are a number of others sources including CDs and sites like eMusic that do not encrypt their music files. This has led some, including the head of the Antitrust Division, to cast a skeptical eye on claims that Apple is violating the antitrust laws. *See* Thomas O. Barnett, *Interoperability Between Antitrust and Intellectual Property*, Presentation to the George Mason University School of Law Symposium Managing Antitrust Issues in Global Marketplace, Sep. 13, 2006, Washington, D.C. *See also* Marcel van de Hoef, *Apple Didn't Break Antitrust Law, Dutch Watchdog Says*, Bloomberg.com, Sep. 6, 2007 (noting that the Dutch regulator reviewing this case found that "[c]onsumers who buy music through the Internet store of Apple can and may also play this music on devices other than the iPod").

complaint brought in the Northern District of Ca

[16] *Slattery v. Apple Computer, Inc.*, No. C 05-00037 JW (N.D. Cal. filed Jan. 3, 2005). On March 21, 2007, the Court consolidated the *Slattery* case with related cases and ordered that all future filings bear the caption "The Apple iPod iTunes Anti-Trust Litigation." *See Tucker v. Apple Computer, Inc.*, Case No. C 06-04457 JW, Related Case No. C 05-00037 JW, Order Consolidating Related Cases; Appointing Co-Lead Counsel (N.D. Cal. filed Mar. 21, 2007).

[17] BNA World Intellectual Property Report, *Apple Must Make iTunes Downloads Playable on Other MP3 Players*, Volume 21, Number 3, Mar. 2007.

[18] *Id.*

[19] Estelle Dumout, *Consumer Groups Wage War on Apple DRM*, BusinessWeek, Jan. 25, 2007, available at www.businessweek.com/globalbiz/content/jan2007/gb20070125_115474.htm.

[20] The Berkman Center for Internet and Society at Harvard Law School has released an interesting paper which does a good job of describing the potential antitrust problem with Apple's strategy. *See*

[22] Apple has said that it is in talks with other major music companies and expects half of its offerings to be available in DRM-free format by the end of the year. *See* Jo Best, Apple, *EMI Ink DRM-Free Music Plan*, BusinessWeek, Apr. 2, 2007.

[23]

improve the quality of data in environments where there may be significant interference, and to

[26] *Id.*

[27] *See* J. Thomas Rosch, *Has the Pendulum Swung Too Far? Some Reflections on U.S. and EC Jurisprudence*, Remarks before the Bates White Fourth Annual Antitrust Conference, Washington, D.C., Jun. 25, 2007, available at www.ftc.gov/speeches/rosch/070625pendulum.pdf; J. Thomas Rosch, *The Three Cs: Convergence, Comity, and Coordination*, Remarks before the St. Gallen International Competition Law Forum, St. Gallen University, Switzerland, May 10-11, 2007, *available at* www.ftc.gov/speeches/rosch/070510stgallen.pdf.

the next decade is how we handle the conflicting regulatory regimes that cover the flow of personal information. Our economies depend in large part on nearly instantaneous transmission of data. Increasingly, this data is traveling across country lines, sometimes several countries in seconds. If we don't get it right – and by "we," I mean the FTC as well as other international regulatory bodies – we could end up crippling international commerce and perhaps stifling innovation. International businesses find it extraordinarily difficult to transmit personal information across borders – whether it be employee or customer-related – without running afoul of other countries' privacy laws.

And I don't mean to imply that our hands are perfectly clean on this front – as you all know, at this point in time in the United States, instead of one federal regulatory framework, there is a patchwork of state privacy and data security legislation – where each state can have different requirements with which a company operating on a national level must comply. For example, at least thirty-five different states have enacted data breach disclosure laws, with different triggering events and notification requirements.[28]

In an environment that is becoming increasingly more globalized, we need to look for ways to encourage compatibility and coordination between various regulatory regimes. Along these lines, the FTC has actively participated in the development of frameworks to permit

---

[28] *See* National Conference of State Legislatures, *State Security Breach Notification Laws*, available at www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

In testimony before Congress, the Commission has recommended that Congress consider requiring companies to notify consumers when the security of this information has been breached in a manner that creates a significant risk of identity theft. *See* Prepared Statement of the Federal Trade Commission on Data Breaches and Identity Theft Before the S. Comm. on Commerce, Sci., & Transp., 109th Cong., at 7, Jun. 16, 2005, available at www.ftc.gov/os/2005/06/050616databreaches.pdf.

transfers of personal data into and out of the U.S. consistent with the privacy laws of other countries. For example, the U.S.- EU Safe Harbor framework, established in 2000, facilitates the transfers of personal data from Europe to the U.S. by establishing a voluntary system under which U.S. companies can certify to a set of principles for the handling of personal data. The FTC plays a key role in this framework, acting as the enforcement agency in the event that a participating U.S. company does not abide by its stated principles. Similarly, in the Asia-Pacific Economic Cooperation (APEC) region, the FTC has been actively involved in the establishment of a voluntary cross-border rules system to permit transfers of personal data. Although this system is still in the testing phase, the FTC hopes that it will result in a consistent set of rules for companies that wish to transfer data throughout the region, as well as maintaining consumers' privacy rights.

Another notable example of international cooperation is the recent Organisation for Economic Co-operation and Development's (OECD) Recommendation on Consumer Dispute Resolution and Redress. This Recommendation advises countries on steps that they should take to update their laws to take into account e-commerce and cross-border developments. It also calls on member countries to develop bi-lateral or multi-lateral arrangements in order to improve international cooperation.[29] Efforts such as these can offer benefits to companies that operate internationally by establishing threshold requirements, improving certainty and lowering operational costs. At the same time, such efforts can provide consumers with security and

---

[29] Organisation for Economic Co-operation and Development, *OECD Urges Government and Industry to Overhaul Consumer Protection for Internet and Other Shoppers*, Jul. 16, 2007, available at www.oecd.org/documentprint/0,3455,en_2649_201185_38967917_1_1_1_1,00.html.

privacy protections no matter where they do business or where their personal information flows. Consistent, reliable and effective security and privacy protections may also encourage consumers and businesses alike to take further advantage of the global marketplace.

The complement to coordinating regulation and laws is the coordination of law enforcement efforts. We need also to strengthen the international cooperation in our law enforcement efforts. The U.S. SAFE WEB Act,[30] signed into law in December 2006, allows the FTC to cooperate more fully with foreign law enforcement authorities in the area of cross-border fraud and other practices harmful to consumers that are increasingly global in nature, such as fraudulent spam, spyware, misleading health and safety advertising, privacy and security breaches, and telemarketing fraud. In particular, it allows the FTC to share confidential information in its files in consumer protection matters with foreign law enforcers, subject to appropriate confidentiality assurances. The Act also protects information provided by foreign enforcers from public disclosure if confidentiality is a condition of providing such information.

In addition to reciprocal information sharing, the SAFE WEB Act allows the FTC to conduct investigations and discovery to assist foreign law enforcers in appropriate cases. This is necessary to enable the FTC to obtain information for foreign agencies' actions to halt fraud, deception, spam, spyware and other consumer protection law violations targeting US consumers. In turn, the Act allows the FTC to obtain the same assistance from foreign investigators. The FTC already has used the powers conferred by the Act to share information with foreign agencies in several investigations. The increasing use of these new tools will remove some of the key roadblocks to effective international enforcement cooperation.

---

[30] U.S. SAFE WEB Act of 2006, Pub. L. No. 109–455, 120 Stat. 3372 (2006).

The FTC works directly with consumer protection and other law enforcement officials in foreign countries to achieve its goals. For example, in response to the amount of fraud across the U.S.- Canadian border, the Commission has worked hard to expand partnerships with Canadian law enforcement entities to fight cross-border mass marketing fraud targeting U.S. and Canadian consumers. The FTC looks forward to continuing to work with all of our foreign counterparts to protect consumers on a world-wide basis.