Presentation
The Challenges of Law in Cyberspace - Fostering the Growth and Safety of E-Commerce
Commissioner Mozelle W. Thompson, Federal Trade Commission

Professor Robert Bone:[†]

We are very honored today to have Federal Trade Commissioner Mozelle Thompson speaking with us on a topic of very current and very keen interest: electronic commerce and how to deal with some of the problems that can arise in e-commerce interactions.

I want to say a few words by way of background introducing the Commissioner to you, and then I'll turn it over to him. Commissioner Thompson is a graduate of Columbia Law School. He also received a Master's in Public Administration from Princeton's Woodrow Wilson School of Public International Affairs. He has had a distinguished legal career, starting as a law clerk and practicing with Skadden, Arps, Slate, Meagher & Flom in New York. He taught at Fordham Law School and was also Senior Vice-President and General Counsel to the New York State Finance Agency. More directly relevant to the talk today, he has served the Federal Government in several capacities. He was Principal Deputy Assistant Secretary of the Treasury, and since December of 1997, he has served as a Commissioner of the Federal Trade Commission.[1] We are very pleased and very honored to have him address us today.

Commissioner Thompson:

I appreciate this opportunity to speak to you about the challenges and opportunities presented by the growth of electronic commerce. I want to thank Dean Cass, Professor Bone and members of the *Journal of Science & Technology Law* for inviting me here.

Boston is an area that has long been recognized for high tech. I am reminded of that every time I talk to my brother, who is a professor at the University of Massachusetts, Lowell, and is Co-Director for the Massachusetts Center for Advanced Computation. It is a truly exciting time to be here to talk about this topic. A good way to start is to talk a little about the FTC - who we are and what we do.

The Federal Trade Commission is a smaller agency in that there are so few of us. We are comprised of about 1100 people and we have two principal missions. One of our missions is to ensure competition as an antitrust agency. This is a jurisdiction that we share with the Department of Justice. We look at mergers, acquisitions, and predatory practices. Right now, we are trying to decide whether to approve a merger of two "small" companies - Exxon and Mobil.[2] We are also the U.S. government's principal consumer protection agency. In that vein, we have been at the forefront of high technology issues from a consumer standpoint.

This new marketplace is expected to grow exponentially over the next few years. ActivMedia predicts that Web revenue will reach $95 billion in 1999 and more than double to $226 billion in 2000.[3] By 2003, Internet sales will reach $1.3 trillion and $2.8 trillion by 2005.[4] Particularly important are predictions about the globalization of this new medium. For example, according to a recent study, by 2005, fifty-seven percent of Internet users world-wide will speak a language other than English.[5] All of this growth has caused a high likelihood that future relationships between buyers and sellers will change.

In light of all this, we now face the challenge of balancing two significant and linked policy goals:

First, we want to ensure that consumers who shop on the Internet are afforded effective

consumer protection and meaningful access to dispute resolution. Achieving this goal will build consumer confidence in the new marketplace and help it flourish.

Second, and simultaneously, we want to create an environment for online businesses that is predictable and not so burdensome as to hinder the growth of the new marketplace. Achieving this goal will ensure consumers have access to a wide range of benefits, including access to more goods, services, and information from around the world and that businesses enjoy a broader customer base.

The FTC already has engaged industry, consumers, academics, and law enforcement in a dialogue about how to foster e-commerce and provide basic consumer protection online.[6] Last December, the Commission issued a notice calling for public comments, and we have received almost seventy submissions.[7] More recently in June, the Commission convened a public workshop which brought together consumer advocates, industry members, government representatives, and academics to discuss these issues.[8]

I would like to speak to you today about what the FTC has learned so far from our efforts and to lay a framework to address these policy goals.

Consumer Law Enforcement in Cyberspace

I have been asked to opine on the role of government regulation in cyberspace. For many, those are loaded words implying intrusive government action. The FTC does not view its role as "regulating the Internet." Rather, the Commission has taken a new approach by working in an interactive way with industry and consumers to establish a framework of good business practices and stop perpetrators of fraud and deception. We think that most businesses agree with those goals. We envision that achieving solutions to consumer protection will not just involve law enforcement – because we can't be everywhere – but also the industry itself, in developing and implementing effective self-regulatory tools. Consistent with this mission, the Commission has thus far brought over 100 federal actions against companies and individuals engaged in Internet fraud and deception.[9]

Most Commission actions have attacked fraudulent practices that are not unique to the online world; they are schemes or problems that have been around for years – for example, pyramid schemes, credit repair scams and fraudulent business opportunities. At the same time, however, the Commission has also attacked new types of fraud that draw upon the unique aspects of Internet technology – speed, anonymity, and audiovisual sophistication. New techniques we have seen include modem hijacking,[10] fraudulent solicitations sent using e-mail (i.e. "spam"),[11] and deceptive online auctions.[12]

Those of you who have been keeping up with the news know that last month we brought an action internationally, in cooperation with the Australians against a "page-jacking" scheme.[13] Some clever individuals in Australia bought domain names and codes that were very close to other popular sites and manipulated those codes so that if you clicked on, for example, the web site for "Saving Private Ryan," you would immediately be transferred to a pornographic site.[14] They did the same thing with Harvard Law Review.[15] The offenders then used the practice called "mouse trapping," where once consumers entered their site, consumers could not get out unless they shut down their browsers and restarted.[16] The goal of these individuals maintaining pornographic sites was to increase traffic to their sites so that they could show a tremendous number of hits on their web sites. They could therefore get more advertising revenue (because the more "hits" that a web site has, the more advertising they can sell).[17]

Similarly, we have taken action against online auctions that seemed legitimate, but did not deliver any goods.[18] There was one a few months ago that made fraudulent solicitations using "spam."[19] These fraud artists sent e-mail to tens of thousands of people, claiming to confirm an "order" for $250 to $899 charged to their Visa Card; if the information was not correct, the recipient had to call the number provided in the email.[20] The number had a normal three-digit prefix that looked like a normal U.S. area code.[21] What the fraud artists did not tell the recipients of the email was that the number was in Dominica, a small island in the Caribbean.[22] To call that number, the consumer would be charged approximately ten dollars a minute.[23] They would induce people to call, and would make money from the consumers' telephone charges.[24]

Notwithstanding our important law enforcement activities, the Commission recognizes that lawsuits alone cannot adequately protect consumers. Consumers must be empowered to protect themselves in the new interactive world. As such, the Commission develops and encourages consumer education efforts and has prompted industry to develop new technologies that afford consumers more control over their transactions.

Privacy and Data Protection

Data protection was among the first policy issues to surface as e-commerce started to become a reality. Studies have consistently shown that consumers are highly concerned about data privacy, whether online or off, and that their concern has actually increased over time. In fact, in a national survey conducted in February for Privacy and American Business by Alan Westin, a resounding eighty-two percent of the 1014 adults surveyed indicated that having a privacy policy would matter in deciding whether they would participate at a website that collected information about them.[25]

The FTC issued a 1998 report to Congress on online privacy in which we expressed "disappointment" about industry progress on self-regulation.[26] During the past year, however, industry leaders have expended substantial effort to build self-regulatory programs. Although leading online companies understand the business case for protecting consumer privacy, the implementation of fair information practices is not widespread among commercial web sites. In fact, a mere ten percent of companies surveyed this summer have implemented the entire complement of fair information practices we have suggested.[27]

Accordingly, the most important challenges to be addressed include reaching those businesses which have not taken steps to protect consumer privacy, especially small and medium-sized businesses which will provide the base for real growth in e-commerce; and encouraging widespread adoption of all of the fair information practices, including educating consumers about the value of these self-regulatory efforts.

We have found that there are still some problems, and recent testimony raises two very good issues, one of which concerns Congress. One thing we've been seeing is that the most popular web sites post some sort of privacy policy about how they will use data. There is still a core of companies out there – presumably responsible companies who are not doing anything to ensure consumer privacy. Consumers, to feel confident, need to know that they are going to have some minimum level of data protection no matter where they are. Industry needs to work on coverage - how to get at those other companies who really aren't doing the right thing to address the issue.

Second is a series of fair information practices that have five elements that we've consistently talked about for at least three-and-a-half years.[28] Large segments of the industry

have adopted these elements. However, according to a recent survey, although a large number of the most popular web sites have some sort of hard privacy policy, less than ten percent actually meet the five information practices:

1) Notice/Awareness: providing notice to consumers that their data is being collected;
2) Choice/Consent: providing a choice for consumers as to whether they want to participate;
3) Access/Participation: so that on a reasonable basis, depending on the industry, the consumers could reliably know that the information being collected is correct;
4) Integrity/Security: security that the information consumers are giving to that web site is actually going to that site; and
5) Enforcement/Redress: if companies fail to meet their representations on the first floor, consumers know that they have some remedies.[29]

We have concluded in this past year that, despite the fact that there is proliferation of proposed legislation on Capitol Hill to deal with this issue, we thought it was premature to enact legislation. We have planned some additional workshops and task forces for the coming months to pinpoint specific problem areas for action. But this issue is not going away. Those of you who are interested in banking have been following the Financial Modernization Bill,[30] and one of the key issues that we have discussed there is to what extent banks can share information with other affiliates. While there is movement in this direction, there are some people who have thought it was inadequate. There are also concerns about medical data privacy. While these issues are not going away, the industry has a real opportunity to address them now.

Additionally, the Commission just last week issued a final rule implementing legislation passed in 1998 to provide additional privacy protections for children online.[31] In looking at the Internet and a variety of web sites, we have found that there were some practices that were geared toward children that presented some problems and questions. We generated a rule based on a great deal of consultation that we actually thought was fairly creative. The rule prohibits solicitation of personal data from children ages thirteen and under unless parental consent is obtained. We recognize though, that there are a variety of uses for information, so there is a provision for essentially a sliding scale. If a child is being asked for information that can be posted on the web, in a chat room, or enable people to contact them offline, there must be a more "hard" parental consent. In other words, it may require that the web site ask the parents to submit something in writing giving their child permission to play. There are other sites, though, where kids aren't identified. While they solicit information, it is not information to be used for marketing purposes, in which case there are other filters that can be used. For example, in one filter a parent's e-mail address must be provided, and an e-mail is sent back to the parents stating that a reply has to be sent back within twenty-four hours. This way, it is more likely that within that time period, the child would not just give out private data himself. The parent would have an opportunity to receive and confirm the e-mail. In this way, it is a sliding scale varying with the degree to which information is released.

Unfortunately, the privacy problem takes on a special significance because of the data protection directive issued by the European Union ("EU").[32] That directive dictates strict legal protections for the personal data of EU citizens and, if enforced, could in some cases hamper the flow of data between the U.S. and the EU. The EU's strict regulatory approach differs from our own. A key element of reaching agreement on a compromise will be ensuring EU countries that U.S. self-regulation backed up by strong enforcement at the FTC can provide a consistent level

of protection for both Europeans and Americans. The Department of Commerce has been working with industry on their self-regulatory issues and with the FTC, to the extent that we can provide some sort of regulatory backdrop for fraud and deception, to develop a safe harbor for the EU directive. They have made progress and are in the final stages; the proposal will likely come out by the end of the year.[33]

E-Commerce Poses a Broad Set of Challenges for Consumers and Business

Insuring privacy and data protection is just one of the challenges associated with the switch to a digital economy. The globalization of e-commerce provides businesses with access to customers worldwide, and consumers have access to a vast array of choice, speed, convenience, and potentially lower costs.

However, despite the vast benefits the new marketplace offers, we know that industry, consumers, and law enforcement all have concerns about what rules and laws will govern Internet transactions. For businesses, access to potential customers in every single country, province, and city that has access to the Internet means that they may be subject to the laws of every jurisdiction. Consumer protection laws around the world vary significantly, particularly with respect to such issues as comparative advertising, advertising to children, and rights of withdrawal from contracts, otherwise known as "cooling off" rules.

It is fairly easy to come up with examples about conflicts of law that give pause to many businesses trying to navigate the global market. Understandably, businesses want regulatory predictability, certainty and guidance. These issues are equally if not more problematic for consumers. Traditionally, the U.S. domestic legal framework on choice-of-law and jurisdiction favors consumers, affording them the core protections available where they live and granting them the right to have disputes resolved in courts close to home.

Consumers are already concerned about the implications of dealing with unfamiliar e-businesses. The National Technology Readiness survey indicated that 67 percent of consumers are not confident conducting business with a company that can be reached only online.[34] Traditional law enforcement concerns are also clear. The Internet is an attractive medium for fly-by-night scam artists, located throughout the global marketplace, who can reach all online consumers.

Meeting the Challenge

We are not in completely uncharted territory, however. We already have in place a legal framework for consumer protection and for choice of law and jurisdiction. Applying those principles to e-commerce poses special challenges.

Simple rules are appealing, but hard to achieve. For example, some advocate a "rule-of-origin" approach (country of the seller) as a threshold way to establish certainty – both for choice of law and choice of forum. Though attractive to businesses for obvious reasons, this approach is unlikely to be successful because of the inconvenience (and cost) to consumers and because government consumer protection agencies are not likely to forgo the ability to protect their own consumers in their own courts to remedy injury inflicted by a foreign web site. We must also recognize that if companies were subject only to the rules where the company was established, scam artists would "race to the bottom," setting up shop in countries with lax protections.

At the same time, a pure "rule-of-destination" approach (the buyer's place of residence) may sound attractive to consumers and law enforcers, but we must be realistic since consumers don't benefit if judgments they win in their home courts cannot be enforced against a foreign seller. Moreover, can or should we expect an online business to be prepared to defend itself in court anywhere in the world and comply with unpredictable and potentially inconsistent

regulations?

In our work at the FTC and in discussions with our international colleagues, the Commission is taking a two-prong approach toward resolution of these issues:

(1) laying the groundwork for international recognition of consumer protection laws and creating international treaties defining rules for jurisdiction and choice of law; and

(2) self-regulatory initiatives that yield good business practices and facilitate alternative dispute resolution.

Both strive to balance our two policy goals: ensuring that consumers receive effective consumer protection and at the same time ensuring that the online medium provides sufficient certainty to businesses to foster commercial growth and development. Any ultimate solution likely will require some combination of these approaches.

Can We Articulate Widely Accepted Principles in International E-Commerce?

Working with our international colleagues to afford similar consumer protections under law affords a "big picture" approach to global problems and moves in a manner consistent with efforts to resolve issues through international treaties.

I lead the U.S. delegation to the OECD Consumer Policy Committee, which has drafted guidelines for governments to consider as they work with businesses and consumers to establish rules for consumer protection in e-commerce.[35] Those guidelines will be ratified by the OECD Council next month.[36] However, the differences between many European countries' systems of law and our own made for considerable difficulties in developing consensus of difficult issues like choice of law and jurisdiction.

In light of these difficulties, the U.S. delegation has encouraged the OECD to articulate broad principles that could serve as the underpinnings of international cooperation. Such principles include:

(1) online consumers should not get any less protection than offline consumers; and

(2) everyone benefits from reasonable disclosures, business practices, and initiatives that serve to facilitate informed decision-making and build consumer confidence in e-commerce.

We have reached agreement that companies should provide consumers with sufficient information to enable them to know with whom they are dealing and to understand the terms and conditions of a contract before it is concluded. The guidelines also provide guidance on fair advertising and marketing practices. In order to facilitate further cooperation, there are some other principles on which I think we need to reach consensus.

First, with respect to jurisdiction, we should distinguish between companies purposefully and knowingly engaged in a transaction with a consumer domiciled in a certain country versus companies that have merely posted a website and not transacted business. Second, with respect to choice of law, we should isolate for international consensus those truly fundamental consumer protections – most obviously those that prohibit fraud – and we should be more careful that consumers do not lose these.

Also, drawing distinctions between "private" and "public" law should significantly

facilitate how we approach issues of jurisdiction and choice of law. An approach that works for private contracts between business and consumers, including private rights of action, may not make sense for public law enforcement agencies. Simply put, international approaches should not undermine any government's ability to protect its own consumers through the prosecution of businesses engaged in fraud or clear deception.

Of course, other forums, including the ABA,[37] UNCITRAL,[38] and the Hague Convention on Jurisdiction and the Effects of Judgments in Civil and Commercial Matters[39] seek to address this issues, and the FTC has also been providing input on all fronts with respect to the effects on consumer protection.

Self-Regulation

In thinking about the big picture, we have to acknowledge certain realities. Relatively few consumer disputes are resolved in court, even in those cases when consumers do have the option of suing close to home under their own law. In addition, obtaining a judgment at home against a foreign business often times will not yield the sought-after remedy because of the difficulty in enforcing it. Finally, as the marketplace continues to grow exponentially, it will become increasingly more difficult for law enforcement agencies to remedy all problematic transactions.

For these reasons, the FTC is giving serious consideration to alternative frameworks for international consumer protection and dispute resolution. We have reached the conclusion that the pressure to answer every question related to choice of law and forum will be lessened significantly if most consumer disputes can be handled through inexpensive, easy-to-understand private arbitration mechanisms.

The FTC appreciates the virtues of self-regulatory programs, if effective and grounded in real commitment, especially in rapidly developing industries such as the Internet. Industry members should be brainstorming about how they can convert current domestic programs into effective vehicles for prevention and resolution of cross-border disputes. Some of these mechanisms are already being developed, such as seal programs like WebTrust[40] and BBBOnline;[41] consumer rating programs, such as Bizrate.com;[42] third party mediation and arbitration; and escrow and insurance services, such as those provided through eBay.[43]

The OECD Guidelines recognize the importance of such mechanisms, and, in fact, the U.S. delegation is leading a working group on a related project to encourage the development of a harmonized system of credit card chargebacks, a protection enjoyed by U.S. consumers but not shared by many of our international colleagues.

Conclusion

When it comes to electronic commerce, our brave new world of the future blends the familiar with the innovative. These issues pose special challenges that warrant international cooperation. Even in the U.S., the FTC and other government agencies must join industry and consumer representatives to develop private-sector initiatives that ensure informed consumer decision-making and a vibrant, competitive new economy.

Question and Answer Session

Audience Member:

My research is focused in the area of electronic privacy. Not as much in the area of fraud and detection, but in terms of the uses of information. There are a lot of conflicting views

between businesses, consumers and government on what are appropriate or inappropriate uses of information.

Commissioner Thompson:

There is one fundamental view right now. The EU-U.S. dispute actually highlights that view. The issue is whether the data that you generate belongs to the individual or whether it belongs to the person gathering it.

Audience Member:

Let me focus on the regulatory aspect of it. Obviously, the businesses want a self-regulatory environment. Until recently, I thought the FTC was moving in the opposite direction and I heard you say that you had decided not to call for any legislation in this area.

Commissioner Thompson:

At this time.

Audience Member:

You've also said that less than ten percent of the web sites have in place appropriate privacy policies.

Commissioner Thompson:

With the full five elements.[44] That is what the latest study showed us.

Audience Member:

I've also heard Orrin Hatch, a conservative Republican, and Ed Markey, a liberal democrat, both say that privacy legislation is inevitable,[45] so I'm wondering can you give me some background on how the FTC arrived at its decision not to pursue legislation, hoping for advances in technology perhaps?

Commissioner Thompson:

One is that over the past several months there have been some real improvements in technology and there are people out there right now who are beginning to provide, for consumers, technological ways for them to control where their data goes. That is one issue. Second, we wanted to see a little more about the value of businesses and business issues. One significant initiative took place several months ago and other companies are beginning to follow. IBM, Microsoft, and others have said that if an e-business does not have a privacy policy on its site, they will not advertise on that merchant's site. That kind of business-to-business response should be very important to condition businesses to understand that the Internet is not the "wild west" - that there are some basic things that they have to do for consumers as one of the barriers to entry. These merchants have the wonderful advantage of not having buildings or warehouses to maintain, but they have other requirements that they have to meet. This is what consumers tell us they want.

Audience Member:

You had mentioned at the beginning that sales on the Internet are increasing incredibly. I'm wondering if you have any sense of what costs are incurred by the offline [merchants] that aren't experienced by the online group.

Commissioner Thompson:

The Commerce Department is looking at that issue right now, and it is sort of a mixed bag in the sense that they are sure some companies should be represented in the pie, to have a bigger slice in the pie. But in some areas, it's a real growth of the pie. In other words, we have people conducting business who would not normally be able to do so. A farmer in Idaho who wanted to buy a diamond watch for his wife, chances are, would not go to Tiffany's to buy it. He might not buy at all. But if he could get to Tiffany's on the web, he might. It is not just that the shares in the pie shift, but it is also that the pie is growing. Do not forget that there are also a variety of services on the web that did not exist before. For example, groceries.com and downloads of certain kinds of information simply didn't exist before. In that sense, we've created new markets as well. For that matter, online auctions, an entirely new business model, didn't exist until recently.

Audience Member:

Regarding your discussion on the challenges of data protection, you discussed how parents have to respond to authorize their children's participation in certain online activities. Assuming that children are fairly intelligent, why can they just not enter false e-mail addresses, which can be done with any of a variety of Internet sites, have it sent back to them, and avoid the mechanism?

Commissioner Thompson:

Realistically, I have to tell you it is impossible to create a perfect system. We recognize that. Some children are targeted more than others. We recognize that too. The real question is, are there reasonable measures that can be taken to protect the majority of children out there? There are some measures that at least give parents the opportunity to participate. Sometimes it is a time requirement, sometimes it is something as simple as a web site stating in order to participate in this web site, parents have to respond within 24 hours with their driver's license number or VISA card. Surely there are some children who are going to rummage through their mothers' pocketbooks looking for VISA cards, in which case, I think the parents have a little bit of a bigger problem than whether their children want to visit the Disney online site or not. I think the key is that in this particular instance, there are solutions that have to do with both issues. That is what we are trying to do. Part of the solution is also, as I said, setting an appropriate climate for how businesses wind up treating children. This requirement sends a very clear message in that regard.

Audience Member:

Have you seen any alternative dispute resolution models that actually work? By "work," I mean models that are inexpensive, are fair to both sides, and are fast.

Commissioner Thompson:

They are only beginning to come into form right now, together with codes of conduct. I think we are seeing some related areas where similar measures have worked. For example, in the United States, advertisers are governed by a self-regulatory model that has been in place for over forty years.[46] We, as the FTC, are the "last resort" enforcers of that model. Advertisers have developed their own code of conduct, have their own dispute resolution mechanism, and are able to govern their own best business practices. Europeans are able to engage in many practices regarding advertising their goods that would not be allowed in the United States. Partly, when you create a climate over time, businesses police themselves and are tougher on themselves. If it

appears that an advertiser is working outside that model, the other business can come to the FTC. There are a couple of areas where we begin to see this model, and we want to see more of that approach. In Europe (in the U.K.) work is being done on an ADR model on some consumer protection issues. Also, there is a private initiative on trust marks that essentially requires participating businesses to place a seal on their web sites that states that they agree to a code of conduct and consumer protection. This model is being developed right now.

David Byer, Testa, Hurwitz & Thibeault:

Where does the age 13 dividing line come from?

Commissioner Thompson:

The age limit of under 13 appears in federal law under a variety of circumstances, so it's consistent with other federal laws and we use that as a dividing line in determining who is a child. The rule can be found at ftc.gov. There is also a different provision that says that the presumption shifts somewhat if you fall between the ages of 13 and 18. That provision says that children those ages can participate in certain web sites, but the web site cannot solicit information from them. The site must give parents a right to opt their child out. Some of those responsible web sites also have an additional screening web site so that individuals cannot even participate in the main web site without permission unless they are over 18. These sites recognize the importance of gaining the trust of parents and children in developing a web site.

Audience Member:

The Internet is so enormous - I was just wondering how you police it?

Commissioner Thompson:

You're absolutely right that the Internet is a huge place, but I wouldn't use the word "police." There are a couple of things that have to be involved. One is creating the appropriate climate for good business behavior. Businesses agree to these basic principles and they can take appropriate action. The Direct Marketing Association has said that participating online merchants must have a privacy policy by a certain date.[47] If a merchant does not comply, it will not be permitted to remain a part of the Association.[48] That is part of the climate. At the same time, we have an Internet Unit at the FTC now.[49] We actually pay them to surf the web. They find a great deal of information through their investigations online. We also have a toll-free number for consumers to call and report problems that they have experienced online. The online problems reported rank number two on the list of total complaints. We also have another unit that works through our site and allows consumers to send unsolicited email that they have received to us - our "Spam Catcher."[50] We get thousands of hits per week from people sending us email. We find the "Spam Catcher" very helpful because unsolicited emails usually are indicative of fraud schemes. To the extent that we can track patterns of behavior and con artists operating in various locations, it is very helpful. The device also allows us to cooperate with other countries so that we can talk about the instances where we see fraudulent behavior. We establish that dialogue with the presumption that we have a very open market here, and a strong market. That presumption means that we believe that this is the right, rather than the wrong, approach. That approach does not mean that theirs are institutions with which we have problems. When we see problems, we take appropriate action. It is that kind of balance that we are trying to achieve. You are right that it is impossible for us to police everyone. On the other hand, if we can get everyone who is involved in the process cooperating with us, we can create

the appropriate climate for good business behavior. What's also very helpful is that in the United States barriers to entry of the lawsuit are very low.

Audience Member:

How many people are in the unit investigating online fraud?

Commissioner Thompson:

Enough to make a difference. This issue was enough of a concern to Congress that last year they gave us $4 million more than we requested to form this unit.

Professor Bone:

I want to thank Commissioner Thompson for a very interesting and stimulating talk. The Internet and the future of e-commerce certainly intersects with every field of the law and challenges them all, including my favorite, Civil Procedure.

---

† Professor, Boston University School of Law; B.A., with distinction, Stanford University; J.D., magna cum laude, Harvard Law School. Professor Bone's teaching and research interests lie in the areas of civil procedure, intellectual property, legal history, and jurisprudence.

[1] For additional information on Commissioner Thompson, please visit the FTC web site. *Federal Trade Commission Home Page* (last modified Apr. 14, 2000) <http://www.ftc.gov>.

[2] On November 30, 1999, the FTC announced that it had "accepted a proposed settlement of charges that Exxon Corporation's acquisition of Mobil Corporation would violate federal antitrust laws." FTC, *Exxon/Mobil Agree to Largest FTC Divestiture Ever in Order to Settle FTC Antitrust Charges* (last modified Dec. 9, 1999) <http://www.ftc.gov/opa/1999/9911/exxonmobil.htm>.

[3] *See* ActivMedia Research, EXECUTIVE SUMMARY REPORT, *Real Numbers Behind 'Net Profits* 1999 SIXTH ANNUAL GUIDE TO GLOBAL E-COMMERCE 8 (1999).

[4] *See id*.

[5] *See* Computer Economics, Inc., *English Will Dominate Web for Only Three More Years* (last modified Oct. 13, 1999) <http://computereconomics.com/new4/pr/pr990610.html>.

[6] The FTC has held public workshops exploring various issues, including U.S. Perspectives on Consumer Protection in the Global Electronic Marketplace, and Consumer Information Privacy. *See* FTC, *E-Commerce & the Internet* (last modified Mar. 28, 2000) <http://www.ftc.gov/bcp/menu-internet.htm#workshops>.

[7] Public Workshop: U.S. Perspectives on Consumer Protection in the Global Electronic Marketplace, 63 Fed. Reg. 69,289 (1998).

[8] *See* FTC, *Public Workshop, U.S. Perspectives on Consumer Protection in the Global Electronic Marketplace, June 8-9, 1999* (last modified Feb. 1, 2000) <http://www.ftc.gov/bcp/icpw/index.htm>.

[9] *See e.g.*, FTC, *Commission Enforcement Actions Involving the Internet and Online Services* (last modified Dec. 20, 1999) <http://www.ftc.gov/opa/1999/9912/case121599.pdf> (describing various Internet-related FTC actions).

[10] Modem hijacking occurs when a consumer is lured into downloading and installing software which, when activated, disconnects consumers' modems and reconnects them to distant servers through long distance phone

calls. *See* FTC, *Victims of Moldovan Modem "Hijacking" Scheme to Get Full Redress Under FTC Settlements* (last modified Aug. 28, 1998) <http://www.ftc.gov/opa/1997/9711/audiot-2.htm>.

[11] "[Spam] is any commercial electronic mail message sent, often in bulk, to a consumer without the consumer's prior request or consent." *Spamming: The E-mail You Want to Can: Hearing before the Subcomm. on Telecomm., Trade, and Consumer Protection of the House Comm. on Commerce*, 106th Cong. 25 (1999) (prepared statement of Eileen Harrington, Assoc. Dir. of Marketing Practices, Bureau of Consumer Protection, FTC) [hereinafter *FTC Statement on Spamming*].

[12] For a description of deceptive online auctions, see FTC, *Internet 'Entrepreneur' Sentenced For Wire Fraud* (last modified Nov. 8, 1999) <http://www.ftc.gov/opa/1999/9902/hare3.htm>.

[13] *See* FTC, *FTC Halts Internet Highjacking Scam* (last modified Dec. 9, 1999) <http://www.ftc.gov/opa/1999/9909/atariz.htm> ("According to the agency, the scammers copy existing Web sites and insert coded instructions in the copycat sites which automatically redirects unwitting consumers to adult sites operated by the defendants.").

[14] *See* FTC, *FTC v. Carlos Pereira, et al. - Memorandum in Support of Plaintiff FTC's Motion for an Ex Parte Temporary Restraining Order* (last modified Sept. 22, 1999) <http://www.ftc.gov/os/1999/9909/atarizmemo.htm>.

[15] *See id.*

[16] *See id.* (describing how consumers attempting to use their web browsers' "back" buttons or attempting to close their browsers are instead inundated with more pornography).

[17] *See* FTC, *supra* note 13 ("[T]he high rate of traffic generated by the 'kidnapped' surfers allowed the defendants to charge premium prices for the banner ads displayed at their site. In addition, the defendants may have received income from diverting surfers to other adult oriented Web sites").

[18] *See, e.g.*, FTC, *FTC Halts Internet Auction House Scam* (last modified Mar. 14, 1999) <http://www.ftc.gov/opa/1998/9804/hare.htm> (discussing the issuance of a temporary restraining order against Danny Hare, an internet merchant doing business as Experience Designed Computers and C&H Computer Services, who failed to deliver computer systems sold through an internet auction house).

[19] *See* FTC Statement on Spamming, *supra* note 11, at 26.

[20] *See id.*

[21] Spam recipients were instructed to call a phone number with a three-digit area code, 767. *See id.* The callers were led to believe that the number was in the United States because they did not need to dial 011 or a country code in order to make the call. *See id.*

[22] *See id.*

[23] *See id.*

[24] *See id.*

[25] *See* Dr. Alan Westin, *"Freebies" and Privacy: What Net Users Think* (last modified July 13, 1999) <http://www.pandab.org/sr990714.html>.

[26] *See* FTC, PRIVACY ONLINE: A REPORT TO CONGRESS (last modified Apr. 30, 1999) <http://www.ftc.gov/reports/privacy3/priv-23.htm>.

[27] *See id.*

[28] *See id.*

[29] *See id.*

[30] *See* Gramm, Leach, Bliley Financial Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338.

[31] *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (1999) (to be codified at 16 C.F.R. pt. 312).

[32] *See* Council Directive 95/46, 1995 O.J. (L 281) 31.

[33] *See Draft International Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce* (last modified Mar. 17, 2000) <http://www.ita.doc.gov/td/ecom/RedlinedPrinciples31600.htm>.

[34] *See* Rockbridge Associates, Inc., *National Survey Assesses Consumer Acceptance of Technology: E-Commerce Faces Strong Skepticism* (visited Apr. 16, 2000) <http://www.rockresearch.com/Articles/press_release3/press_release3.html>.

[35] The Consumer Policy Committee is part of the Organisation for Economic Co-operation and Development ("OECD"), an international organization based in Paris. *See* OECD, *What is OECD*? (last modified Jan. 14, 2000) <http://www.oecd.org/about/general/index.htm>. The organization is somewhat of a "think tank" made up of 29 of the world's industrialized nations. *See id*. The Consumer Policy Committee is one of 200 specialized sub-groups. It works in part to develop guidelines for government bodies to utilize in their policy making decisions. *See id*.

[36] *See* Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce (last modified Dec. 7, 1999) <http://www.oecd.org./dsti/sti/it/consumer/prod/CPGuidelines_final.pdf>.

[37] The Section of Business Law and the Section of International Law of the American Bar Association ("ABA") have contributed to the discussion of international approaches to e-commerce law. *See, e.g.*, American Bar Association, *Subcommittee on International Transactions - Introduction and Background* (last modified June 17, 1998) <http://www.abanet.org/buslaw/cyber/archive/introbak.html> ("Our goal is to facilitate international discussion of the legal framework in which the potential of electronic commerce in international trade can be fully realized."); *see also* American Bar Association, *Public Policy Initiatives, ABA - Section of International Law* (last modified Aug. 11, 1999) <http://www.abanet.org/intlaw/about/policy/full_policy.html> (stating the goals of supporting electronic commerce and encouraging self-regulation by the private sector).

[38] The United Nations Commission on International Trade Law ("UNCITRAL") is the "core legal body of the United Nations system in the field of international trade law." The United Nations International Commission on Trade Law, *One World of Commerce: Towards One Commercial Law* (last modified Oct. 18, 1999) <http://www.uncitral.org/english/commiss/geninfo.pdf>. Its mandate is "to further the progressive harmonization and unification of the law of international trade." *Id.*

[39] *See Draft Hague Convention On Jurisdiction and the Effects of Judgments in Civil and Commercial Matters* (last modified Aug. 15, 1999) <http://law.gov.au/publications/hagueissue2/attacha.html>.

[40] The American Institute of Certified Public Accountants ("AICPA") created WebTrust, a seal of assurance offered to commercial Web sites that meet its electronic commerce standards for electronic commerce, known as the WebTrust[sm] Principles and Criteria. *See AICPA Launches WebTrust[sm] Electronic Commerce Seal* (last modified

Oct. 20, 1998) <http://www.apollo-one.com/webtrust/webtrust.html>.

[41] The BBBOnLine seal program approves certain companies to display a seal at their web site. *See* BBBOnLine, *Privacy Program Created to Enhance User Trust on the Internet* (last modified Mar. 25, 1999) <http://www.bbbonline.org/about/press/6-22-98.html>. The seal assures consumers of the reliability of the company. *See id*.

[42] BizRate.com gathers consumer feedback and transactional information from e-businesses. *See* Bizrate.com., *Press – BizRate.com Corporate Facts* (visited Mar. 30, 2000) <http://www.bizrate.com/press/press_facts.xpml>. BizRate.com then uses this information to make unbiased store and product recommendations to consumers. *See id*.

[43] eBay, a personal online trading community, maintains SafeHarbor, a customer support and educational resource center. *See* eBay, *Help: Rules and Safety* (last modified Apr. 14, 2000) <http://pages.ebay.com/services/safeharbor/index.html>. SafeHarbor includes both an escrow service where third parties ensure safe transfer of consumers' money and a free insurance program that covers qualified users who buy qualified items on eBay. *See id*.

[44] *See supra* note 29 and accompanying text.

[45] Orin Hatch (R-UT) stated at an April 21, 1999 hearing: "There is no question that in order for the Internet to reach its maximum potential as a viable avenue for transacting commerce, consumers must be assured that personally identifiable information that is collected online is afforded adequate levels of protection." *See Privacy in the Digital Age: Discussion of Issues Surrounding the Internet: Hearings before the Committee of the Judiciary, 106th Cong.* (statement of Sen. Orrin Hatch) (visited Jan. 25, 2000) <http://www.senate.gov/~hatch/statement/state086.html>. Ed Markey (D-MA) introduced the Communications Privacy and Consumer Empowerment Act ("CPCEA"), designed to give consumers control over the use of their personal information. *See* Center for Democracy and Technology, *Representative Markey Introduces Online Privacy Legislation* (last modified Oct. 7, 1999) <http://www.cdt.org/privacy/062096_Markey.html>.

[46] *See, e.g.*, Council of Better Business Bureaus, *Do's and Don'ts in Advertising* (visited Mar. 30, 2000) <http://www.bbb.org/advertising/dd.asp> ("For over 47 years, *Do's and Don'ts* has been compiled and published by the Council of Better Business Bureaus, the national association of the Better Business Bureau system. . . . *Do's and Don'ts in Advertising* and *Advertising Topics* offer you [advertising executives] everything you need to get quick approval of ad content for yourself or your client, and eliminate costly ad revision."); *see also* Council of Better Business Bureaus, *National Advertising Review Board: Brief Summary of Procedures* (visited Mar. 30, 2000) <http://www.bbb.org/advertising/narb.asp> ("In an effort to sustain 'truth and accuracy in national advertising' through self-regulation, a two-tier system was created by the advertising community in 1971.").

[47] *See* Direct Marketing Association, *Privacy Promise Member Compliance Guide* (visited Mar. 30, 2000) <http://www.the-dma.org/library/privacy/privacypromise.shtml>.

[48] *See id*.

[49] *See Internet Highjacking Scam*, *supra* note 13 ("The [FTC's Internet] lab was established to provide agency lawyers and investigators with hi-tech tools to investigate hi-tech consumer problems.").

[50] *See* FTC, *FTC Unveils "Dirty Dozen Spam Scams"* (last modified Mar. 14, 1999) <http://www.ftc.gov/opa/1998/9807/dozen.htm> ("[C]onsumers have forwarded [more than 250,000 unsolicited commercial e-mail messages] to a special FTC mailbox (uce@ftc.gov) set up to collect 'spam.'").