October 29, 2008

Chairman William E. Kovacic
Federal Trade Commission

Ms. Maureen Ohlhausen
Director, Office of Policy Planning
Federal Trade Commission

Dear Chairman Kovacic and Director Ohlhausen:

This written statement is submitted in connection with your invitation for me to participate in your conference on "The FTC at 100: Into Our Second Century."

The "FTC at 100" project is designed to get a big picture of the past, present, and future of the Federal Trade Commission. The overarching theme of my testimony is that the FTC is, and should remain, the preeminent consumer protection agency in the world. In an era of limited resources, the focus of the agency should be where two criteria are met: (1) a topic has important effects on consumers; and (2) the FTC has a significant advantage in effectiveness compared with other possible ways to address the topic. Those other ways, for instance, might include state enforcement, enforcement by agencies in other countries, self-regulation, or reliance on market forces.

A key area for FTC leadership is online commerce. My testimony reports on recent research that shows reasons for expecting underenforcement against online harms unless the FTC continues, and quite possibly expands, its leadership role. To date, the FTC has acquired impressive expertise in technology issues relevant to online commerce. My recommendation is that such information technology expertise should be an important priority for the commission in the coming years.

In order to achieve leadership in IT issues for online commerce, I propose the following recommendations, explained more fully below:

1. **Appoint a chief technology officer for the FTC.** A chief technology officer at the commission would provide vision and leadership for IT issues affecting consumers' online activities.
2. **Assess policy initiatives by functional area, not geography.** For online harms, local and state consumer protection agencies will face major challenges in playing their historical role in enforcement. The FTC should step forward with initiatives defined by function, such as fighting spam, protecting against identity theft, and combating spyware and other malware.
3. **Use technology to implement an effective mix of federal and federated enforcement.** The Consumer Sentinel program is a promising step toward using new technologies to share information and link enforcement agencies both nationally and internationally.
4. **Use new technologies effectively in consumer education.** The commission should increase its use of multimedia and other emerging technologies to conduct consumer

education. In addition, participating in emerging technologies will provide insights to improve the commission's policy and enforcement activities for new media as they evolve.

5. **Create and implement a research agenda for consumer protection online.** An important part of being the leading consumer protection agency for online activities is to create a research agenda on issues of major concern to consumers and consumer protection. Topics for research include how to provide notice about online activities, the growing role of behavioral and experimental economics, and a special role the commission can play in computer security research to protect consumers.

As the FTC prepares for its second century, this agenda for leadership on online commerce should be a priority part of the commission's protection of consumers.

Background

I am the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University, and a Senior Fellow at the Center for American Progress. From 1999 until early 2001, I served as the chief counselor for privacy in the U.S. Office of Management and Budget. In that role I coordinated administration policy in the use of personal information in the public and private sector, including working closely with the FTC on issues such as online privacy, the Safe Harbor negotiations with the European Union, computer security, and online advertising.

My background for discussing the Bureau of Consumer Protection, or BCP, comes in part from my general background on issues that the Federal Trade Commission addresses. This fall semester, I am teaching antitrust law and a seminar on the regulation of online advertising. I have often taught courses on privacy law, cyberspace law, cybersecurity law, and banking regulation. I have spoken at numerous FTC events, met often with commissioners and staff, and submitted testimony on a range of topics facing the commission.

My scholarly and policy writings cover a wide range of privacy, computer security, and other consumer protection issues. I am faculty editor of "The Privacy Year in Review," published by *I/S: A Journal of Law and Policy for the Information Age*, which is distributed to all members of the International Association of Privacy Professionals. I am lead author of the book that is used as the official study reference for the Certified Information Privacy Professional examination. In addition to privacy and computer security generally, my writings have addressed many issues facing the BCP, such as phishing, spam, spyware, identity theft, advertising regulation, international aspects of consumer enforcement, the Fair Credit Reporting Act, the intersection of antitrust and consumer protection, and so on. My publications and list of relevant presentations are available at www.peterswire.net and www.americanprogress.org.

Assessing the success of the consumer protection mission

The "FTC at 100" project is designed to get a big picture of the past, present, and future of the Federal Trade Commission. The Bureau of Consumer Protection has a broad mandate to protect consumers generally, and especially to guard against the unfair and deceptive practices that are enforceable under Section 5 of the FTC Act. You have asked for comments on the deployment of

the agency's resources in the consumer protection area. You specifically asked for comment on the following topics: (1) the most effective means for developing consumer protection policy; (2) the optimal use of the agency's enforcement, research, advocacy, and education tools; (3) the use of industry self-regulation as a complement to enforcement; (4) setting a consumer protection research agenda; and (5) evaluation of the effectiveness of the FTC's enforcement and other efforts in the consumer protection area.

The overarching theme of my testimony is that the FTC is, and should remain, the preeminent consumer protection agency in the world. In an era of limited resources, the focus of the agency should be where two criteria are met: (1) a topic has important effects on consumers; and (2) the FTC has a significant advantage in effectiveness compared with other possible ways to address the topic. Those other ways, for instance, might include state enforcement, enforcement by agencies in other countries, self-regulation, or reliance on market forces.

The FTC's distinctive role for online commerce

An enormous area for FTC leadership is in the area of online commerce.[i] Since the rise of commerce on the Internet in the mid-1990s, the FTC has been a clear leader in assuring that consumer protection concerns are addressed by the major online players. Examples of this leadership include the 1996 Public Workshop on Consumer Privacy in the Global Information Infrastructure, the rapid adoption of privacy policies in response to FTC efforts in the late 1990s, and the 2006 hearings on Protecting Consumers in the Next Tech-ade.

There are strong reasons to believe that the FTC should retain and quite possibly expand its role as a leader in protecting consumers in online commerce. I have written a new law review article called, "No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime."[ii] The article gives new reasons why we should expect underenforcement for E-commerce, cybercrime, and Internet harms more broadly. It also recommends a strategy for addressing that underenforcement, focusing on more federal or federated enforcement.

The article stresses an information problem and a commons problem that have largely been overlooked to date. In brief, the information problem arises because only a tiny fraction of complaints and knowledge about an online fraudster or criminal comes from each jurisdiction. Historically, most consumer protection occurred at the local or state level, and local enforcers had relatively good information about which actors were "good guys" as opposed to repeat violators. Online, however, local enforcers lack the informational basis for telling good guys from bad guys. Priority bad guys thus are less likely to become the targets for enforcement.

This information problem is compounded by a commons problem. In light of the incentives facing enforcement agencies, priority will typically go to cases where many or all of the victims are local. No one will have the incentive to give priority to harms that occur across borders. This is a classic commons problem, because cross-border harms will be left to someone else. In short, no one will own these problems, and there will be underenforcement. As one example, it has often been difficult for victims of identity theft in one state to get strong enforcement against a data theft that occurs in another state.

These information and commons problems exacerbate the "forensics" problem that has been the focus of greatest legal attention to date. This forensics problem is that it is often technically and legally difficult to gather evidence where the perpetrator is physically distant from the victim. The SAFE WEB Act of 2006 is an admirable step in the direction of giving the FTC important legal tools to enforce across national borders. As the FTC develops additional experience using these new tools, its comparative advantage will become greater for addressing online harms to consumers.

In response to these information, commons, and forensic problems, the basic response should be to shift toward more federal and federated enforcement. Federal enforcement means a greater role, compared to offline activity, for the Federal Trade Commission in consumer protection. "Federated" enforcement means building new structures, compared to offline activity, to share information among local enforcers and to encourage local enforcers to bring more enforcement actions even when the perpetrator and many of the victims are outside of their jurisdiction.

In short, the FTC has already been recognized as a leader in addressing harms to consumers in online commerce. As online commerce continues to expand in complexity and share of the total economy, the information, commons, and forensic problems indicate that the relative role of the commission should likely become even greater.

Expertise in information technology issues

Compared with other consumer protection agencies, both inside the United States and globally, the FTC has acquired impressive expertise in technology issues relevant to online commerce. My recommendation is that information technology, or IT, expertise should be an important priority for the commission in the coming years.

This IT expertise has developed in part due to specific direction from Congress and the executive branch for the FTC to take action in areas including children's online privacy, spam, identity theft, and updates of data-intense issues under the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act. On the enforcement side, the FTC has been the key consumer protection agency for topics including computer security, online privacy, phishing, and spyware, and has been the federal agency most involved in issues of data breach. FTC workshops, guidelines, and other policy processes have been the leading forum for consideration of other IT-related issues, such as the current focus on online behavioral advertising.

If the FTC were considered as a company engaged competitively with other companies for leadership on IT issues, then business strategists would say that there are "first-mover advantages" and "synergies" from this pattern of FTC activity on IT-related issues. The first-mover advantages exist because the first consumer protection agency to act on an emerging topic often becomes the focus of the most intense education about the relevant facts and policies. The synergies exist because experience with one set of IT issues makes the FTC more effective with other sets of IT issues.

I would go further and argue that the FTC has a duty to continue to develop its leadership in IT issues relevant for online commerce. Except for the FTC, I am not aware of any other consumer

protection agency that has anything approaching the same level of experience, reputation, and ability to foster improved protections for consumers online. Innovations in data practices and information technology will raise a constant stream of new potential problems for online consumers. The FTC can and should play a unique role in assuring that consumers are treated well as markets and technologies shift. Often the right answer will not be to regulate. The participation of the FTC as a potential enforcer or regulator, however, will frequently make industry consider consumer concerns far more seriously.[iii] Before harmful patterns get locked into business practices, participation by the FTC can help assure that consumers' needs are built into emerging business models.

Recommendations for IT Leadership

In order to achieve leadership in IT issues for online commerce, I propose the following recommendations:

1. Appoint a chief technology officer for the FTC. A chief technology office can play a helpful role in creating and implementing the strategy for assuring that the FTC is as effective as possible in protecting consumers in online activities. One role of the CTO would be to help envision where problems for consumers are likely to arise, and help the FTC advocate for the rights of consumers in emerging business practices. A second role would be to help assure that the FTC takes advantage of technology as it seeks to carry out its own activities.

2. Assess policy initiatives by functional area, not by geography. As discussed above, the enforcement against online harms will often not be achieved successfully by local enforcers. Because many online harms happen on the national or international scale, the FTC has a key institutional role to play in enforcement.

In terms of assessing the success of the commission—a question posed by the FTC at 100 process—the logical way to assess programs is by functional area. For instance, there can be periodic reviews in areas such as spam, phishing, spyware, online privacy, behavioral advertising, computer security, ID theft, and others. For each functional area, there will often not be the preponderance of local enforcement that has happened for traditional consumer frauds and other harms. Instead, the question becomes the extent to which strategic goals are achieved for each of these policy areas. Staffing and other resource decisions should be made in connection with the priorities among the functional areas. Resource decisions will depend on a mix of enforcement and non-enforcement activities, including research, workshops, and other policy formation efforts.

3. Use technology to implement an effective mix of federal and federated enforcement. The Internet allows fraudsters to cause harm at a distance, such as when spam comes from overseas or an identity thief infiltrates a database thousands of miles from a consumer's home. The Internet and evolving technology also greatly benefit the FTC and other consumer protection actors. The Consumer Sentinel project, led by the FTC, has greatly improved information sharing among enforcement agencies about online harms. Looking ahead, the CTO and other FTC leaders should think strategically about where evolving technology can improve coordination among consumer protection agencies, self-regulatory groups, the media, public interest groups,

and others who help combat online harms. To save costs, wikis, other online forums, and teleconferences can reduce the amount of expensive physical travel that would otherwise accompany this level of effort at coordination.

4. Use new technologies effectively in consumer education. One important role of the commission is consumer education. For instance, the commission has been very active in creating resources for consumers affected by identity theft. Going forward, it makes sense for the commission actually to use emerging technologies in order to reach consumers. For instance, multimedia is likely to become far more important in coming years, with text no longer being the only way to give disclosures or memorialize a contract online. The commission can explore when and how to use multimedia in its outreach efforts. The commission should consider if and how to have employees participate in blogs and other Web 2.0 activities, and the type of disclaimers about whether the posting is by an individual or on behalf of the commission. The commission should explore automatic translation to Spanish and other languages, to help assure that consumers who receive marketing in non-English languages are protected effectively.

This sort of active engagement in new communications and advertising technologies makes sense simply as a matter of effective consumer education—the commission should try to use the techniques that actually reach consumers. In addition, participating in emerging technologies will provide insights to improve the commission's policy and enforcement activities in evolving media.

5. Create and implement a research agenda for consumer protection online. As a global leader for thought leadership online commerce, the commission should create and implement a research agenda to promote consumer protection online. Historically, the Bureau of Economics has often played an important role in research about economic and related antitrust issues. Looking ahead, the Bureau of Consumer Protection can be a leader in researching how emerging IT practices affect consumer protection. Creation of a research agenda should be done in collaboration, of course, with leading researchers. Examples of areas for attention could include the following:

- **Notice in online commerce.** An important FTC initiative in the 1990's was to encourage web sites to post privacy policies. Violations of those privacy policies, in turn, have been enforceable as deceptive practices under Section 5 of the FTC Act. This notice-based enforcement, however, is being put in jeopardy by developments in web technology. A typical commercial web page today, for instance, may have 15 to 40 or more "server calls" to different servers, often operated by different companies. There is a serious question how notice should operate when so many different companies can derive information from a consumer's visit to a single web page.

- **Behavioral economics and online commerce.** The modern economic understanding of consumer behavior has stressed results from behavioral and experimental economics. These economic approaches stress important ways in which consumers depart from the "rational actor" model that has often underpinned consumer protection law. The FTC has begun to look for insights from behavioral economics, but policy initiatives going

forward should likely be based on a more thorough examination of the behavioral and experimental economics literature.

- **Computer security research.** Consumers suffer from a range of serious computer security problems. Millions of computers are infected with viruses or have become part of "bot" farms that can be operated remotely by cybercriminals. Spyware, phishing, and other problems put consumers at risk of identity theft and reduce trust in online banking and other areas of online commerce.

  In response, the commission might play a uniquely helpful role in fostering computer security. The anticircumvention provisions of the Digital Millennium Copyright Act place strict limits on the ability of computer security researchers to test many common technologies and publicize the security flaws they discover. There is a statutory exception to the DMCA, however, which allows federal agencies to conduct or sponsor research about those same technologies. As a federal agency, therefore, the FTC can explore whether and how to use its statutory powers to sponsor research on computer security matters that are vital to consumers.

Conclusion

In considering the future role of the Bureau of Consumer Protection, my comments have focused on the role of the FTC as a global leader in protecting consumers in online commerce. Online commerce is clearly highly important—it is a large and growing share of the economy. It is also an area where the FTC has already developed comparative expertise and should continue to take on the responsibility of being a global leader.

These comments about online commerce, however, should not detract from other important missions of the Bureau of Consumer Protection in coming years. For instance, we are likely on the cusp of a massive effort to address climate change. "Green marketing" is therefore likely to be a tremendously important topic in coming years, and deceptive claims about greenhouse gases or carbon dioxide emissions, for instance, require great attention. As another example, the current mortgage and financial crises have revealed severe problems in consumer protection in the banking and related sectors. If there is a reorganization of bank regulatory agencies, it is vital that the new structure have more effective safeguards for consumers than we have seen in recent years. The FTC has been an especially effective consumer protection agency, in my view, and quite possibly deserves to retain or expand its current role in protecting consumers in the financial realm.

In short, the FTC has earned its current strong reputation for protecting consumers as it approaches its one hundredth anniversary. My congratulations to all those who have contributed to this success, and I hope the comments here can contribute to the process for building on that success in the coming years.

Peter P. Swire
Senior Fellow, Center for American Progress
C. William O'Neill Professor of Law

Endnotes

[i] For more discussion of the important role of the FTC in the area of online commerce, see the proceedings of the Center for American Progress conference on "The Internet and the Future of Consumer Protection," available at http://www.americanprogress.org/events/2006/7/b593305ct2758595.html.

[ii] Peter P. Swire, "No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime," J. Telecomm. & High Technology L. (forthcoming, 2008), available at http://ssrn.com/abstract=1135704.

[iii] I have long believed the credible threat of government action is an important factor in helping self-regulatory approaches become more effective. Peter P. Swire, "Markets, Self-Regulation, and Legal Enforcement in the Protection of Personal Information," U.S. Department of Commerce, Privacy and Self-Regulation in the Information Age (1997), available at http://ssrn.com/abstract=11472.