Center for American Progress

The Internet and the Future of Consumer Protection

By Peter P. Swire*, Senior Fellow, Center for American Progress

July 24, 2006

Executive Summary

In 1996, the Federal Trade Commission (FTC) held hearings on consumer protection, privacy and the Internet. This November, the FTC will hold new hearings on consumer protection, the Internet and globalization. To help prepare for those hearings, this paper puts forward a new framework for what the Internet means for consumer protection.

The current paper is the initial part of a larger research project. The goal of this project is to clarify a consumer protection regime that will help the Internet do well for consumers, businesses, and other stakeholders. We need to enhance consumer trust, help legitimate businesses flourish, and deter or punish illegitimate practices such as fraud and theft. A better Internet will promote economic growth, and also support individual creativity, a spirit of community, and political communication.

The framework uses the metaphor of "elephants" and "mice" to explain what is changed with the Internet. For large organizations, or "elephants," the basic regulatory and enforcement process is much the same offline and online. By contrast, the Internet leads to many consumer harms caused by small actors, or "mice," that hide from enforcers, often in nests outside the United States. To respond, consumer protection agencies will face an unprecedented need for international and technological capabilities, in order to catch the mice and reduce the harms they cause.

There are also three clusters of consumer protection issues that become much more salient with the rise of the Internet. The discussion here briefly describes those clusters:

1. "The Last Mile." Consumers need to connect to the Internet to use it. Connectivity is a new utility, complete with the possibility of monopoly power that has long been a theme of utility regulation.

2. Personal information. Personal mainframes and high connectivity mean that information about named individuals flows in unprecedented ways. Major consumer protection issues arise for privacy, data security, and personal identity.

---

* Peter Swire is the C. William O'Neill Professor of Law at the Ohio State University and a Senior Fellow at the Center for American Progress. The views in this document are his own, and other documents released by the Center, including on topics discussed in this paper, do not necessarily reflect the views of Professor Swire.

3. Consumers as producers. Equipped with a personal mainframe, an individual can often compete with industrial producers, or at least create content based on industrial production. Bloggers compete with newspapers. Home video hobbyists compete with movie studios, or at least can alter the original movies. The law has historically treated consumers and producers differently, but new rules will be needed when individuals have the computing power to be effective producers.

By understanding the differences in enforcement against elephants and mice, and by recognizing the three clusters of key issues, this paper provides an agenda for the 2006 FTC hearings, and a framework for understanding the changes in consumer protection brought about by the rise of the Internet.

I. Introduction

This paper sets forth the initial version of a framework for thinking about consumer protection and the Internet. "Consumer protection" here has a common-sense meaning, roughly tracking the scope of consumer protection bureaus in local, state, and federal agencies in the United States. The term also has a somewhat broader meaning — the ways that individuals and families ("consumers") can suffer harm due to monopoly power, unfair and deceptive trade practices, and theft and other criminal acts in a commercial context.

This paper uses the term "the Internet" as shorthand for the dramatic changes in information technology that have taken place since commercial activity began on the actual Internet around 1993. Many people are familiar with Moore's Law, which states that the processing power of the computer chip will double approximately every 18 months. For consumers, Moore's Law means that the family desktop or laptop today has the storage and processing power of a mainframe from not long ago. For consumers, the spread of ever-faster broadband means that many families are approaching a condition of ever-on, unlimited connectivity.

The task, essentially, is to understand the implications for consumer protection from having personal mainframes and unlimited connectivity. A useful goal in this research is to explore the meaning of the "common good" — what is the overall set of rules, practices, and institutions that will have the Internet work well for consumers, businesses, and other stakeholders.[1] The Internet experience should shift in directions that enhance consumer trust, help legitimate businesses flourish, and deter or punish illegitimate practices such as fraud and theft. A better Internet will promote economic growth. It will also promote other values, such as support for individual creativity, community, and political communication.

Before presenting the framework, a few disclaimers are in order. First, this paper is the down payment on a larger research project about how consumer protection should

[1] For an insightful recent exploration of the meaning of the "common good," see John Halpin & Ruy Teixera, "The Politics of Definition," http://www.prospect.org/web/page.ww?section=root&name=ViewWeb&articleId=11435.

proceed for the Internet. The research effort will proceed through the planned hearings at the Federal Trade Commission (FTC) in November, 2006, and into planned presentations of the full document in the winter and spring of 2007. Interested persons are most welcome to contact the author with thoughts about the larger project.

Second, a few words are helpful on "market failures" and "government failures." Those experienced in Washington debates know that market failures are a standard justification for government action. In the classic example, a factory sends harmful waste into the river. This pollution is an externality — the benefits of the production go to the factory while the costs are suffered by those downstream. Because it does not internalize the costs, the factory has an incentive to over-produce and over-pollute. The government thus may require pollution controls to fix the externality.

Also familiar in Washington debates, especially in recent years, is the idea of government failure. Critics of government regulation point out that additional regulation might make a problem worse, or enforcement actions may be costly and done in less-than-optimal ways. I entirely agree with a core point — we should examine both market failures and government failures before concluding that a particular government action is justified. With that said, this initial paper will identify a number of market failures that may exist on the Internet, but will not repeat the government failures point each time. Full analysis of these issues requires attention to the imperfections of both markets and of government interventions.

A third disclaimer is that this early version of the research identifies areas of concern for consumers, but does not always say which institutions would best address each issue. Consumer protection has often proceeded in the United States at the local, state, and federal levels. At the federal level, the FTC has the broadest jurisdiction over consumer protection, but numerous other agencies have specialized jurisdiction that may be relevant to the Internet, including the Federal Communications Commission (FCC), the Food and Drug Administration (FDA), the various banking agencies, and many others. Much of the detail about which institutions should do what will be left for the longer research report.

Summary: This initial paper seeks to present a framework for consumer protection as we approach a world of personal mainframes and unlimited connectivity. The emphasis in this initial paper is on identifying areas where market failures may be significant and new measures or institutions may be needed to assure effective consumer protection.

II. What is Changed or Unchanged about Consumer Protection on the Internet: Of Elephants and Mice

In earlier writing, I have used the metaphor of the elephants and mice to explain when legal regulation is likely to work well on the Internet.[2] The same metaphor is used

[2] Peter P. Swire, "Elephants and Mice Revisited: Law and Choice of Law on the Internet," *153 U. Penn. L. Rev. 1975* (2005); Peter P. Swire, "Of Elephants, Mice, and Privacy: International Choice of Law and the

in this paper's framework to explain what is essentially the same or different about consumer protection as it shifts to the Internet. In summary, consumer protection enforcement is much the same against offline and online "elephants," or large actors. New problems arise, against the numerous small actors, or "mice," that create consumer protection issues on the Internet.

The Metaphor of Elephants and Mice.

Elephants — the actual animals or the big corporations — are large, powerful, and practically impossible to hide. The large size of elephants is a vulnerability — they can't hide if they break the law, and they have large assets that can be seized under a court judgment. The large size of elephants is also an advantage, however. Elephants are enormously strong and have all sorts of effects on the local ecosystem (potentially crushing trees, smaller animals, and so forth.). If a particular regulation angers an elephant, it may be able to lobby to change the rule. If an enforcement action is brought, it has a thick skin, and defense lawyers may protect it from harm.

The situation is quite different for mice, which are small, nimble, and multiply annoyingly quickly. A good example on the Internet is phishing, where fraudsters send e-mails pretending to be from legitimate banks or other businesses. The phishing e-mails typically say there is a problem with the account, and ask the consumer to go to a Web site and provide name, Social Security number, or other personal information. Phishing e-mails and Web sites breed quickly — new phishing scams pop up daily and a typical Web site is up for a few weeks or less. If one Web site is closed down, the fraudster soon opens up a new one. Many phishing attacks come from overseas, where the fraudsters often have a cozy nest that U.S. regulators cannot easily find. For mice, the main strategy is to stay hidden. Once the fraudster is identified, civil and criminal penalties may quickly follow.

What the Metaphor Means for Consumer Protection.

The metaphor of elephants and mice helps explain what the Internet changes and doesn't change for consumer protection. The main point here is that the shift to the Internet matters much less for issues concerning elephants. For instance, imagine that there is a deceptive trade practice claim against a national chain retailer in the physical world or a leading e-commerce retailer. Enforcement of the claim would be similar offline and online. The state or federal consumer protection agency would bring the complaint. Under current law, there would almost certainly be jurisdiction, because the defendant knew it was conducting business in that state. If the agency could prove the facts, then a consent decree or judgment can readily result.[3]

Internet," *32 The International Lawyer 991* (1998). These and other publications are available at http://www.peterswire.net/pspublications.htm.

[3] When I spoke this spring at a consumer protection conference of the National Associations of Attorneys General, I asked enforcement officials from small states whether they were able to bring effective enforcement actions against national chain retailers and large e-commerce sites. The officials said that such actions are quite manageable, if the facts sustain the claim.

Enforcement is much more difficult against mice. The Internet is a more fertile breeding ground for mice than the offline world. The reason is that Web and e-mail communications are international and essentially free. With roughly a billion people online today, that means that each of us has roughly a billion next-door neighbors, not all of whom are very nice. The online world gives mice a lot of places to hide.

Many consumer problems on the Internet are caused by mice. Examples include: spam e-mails; phishing attacks; the money-transfer scams that seem to have started in Nigeria; and viruses, worms, and other attacks on the consumers' systems. Purveyors of pornography, especially kiddie porn, hide like mice. So do those who download copyrighted content. As officials have tried to bring enforcement actions against these mice, they have faced serious obstacles.

Some problems involve a combination of elephants and mice. Consider the example of spyware (the computer tells someone about the consumer's activities), and adware (special software shows ads to consumers based on their activities). The adware companies turn out, perhaps surprisingly, to be elephants. The business model for an adware company, such as Claria, is to be visible enough to sell advertisements for major companies. That visibility means that Claria can be found by consumer protection agencies as well. As a result, Claria has substantially changed its practices. Meanwhile, other spyware attacks are done by mice. The purveyors of spyware hide their activities, such as by using "drive-by downloads" to put software stealthily on a consumer's computer and try to gain control of it. In this instance, the metaphor of the elephants and mice indicates that adware may be a much easier problem to resolve than spyware attacks by hidden actors.

Policy Implications of Elephants and Mice.

By clearly describing what is different about the Internet, we can better assess what should be done. For consumer protection issues related to elephants, the basic enforcement process remains much the same. There will be difficult substantive issues, such as whether a particular practice is anticompetitive or deceptive. Some of the key substantive issues for the Internet are described below in Part III. But the fundamental regulatory and enforcement processes resemble those for the offline world.

The biggest enforcement changes for the Internet arise from its international and technical dimensions. Historically, many consumer protection disputes were local, and were resolved in the city or county where the merchant was located. Over time, consumers increasingly purchased through the mail or by telephone. State Attorneys General, along with the FTC, often stepped in to enforce against merchants in the national market. With the Internet, the number of international communications for consumers has soared. Problems caused by mice — often from overseas — are pervasive, from spam to phishing to other fraud schemes.

The U.S. system of consumer protection thus faces a much greater need for effective international enforcement. This internationalization is directly attributable to the Internet and the sorts of consumer harms that result. U.S. enforcement agencies will need to work together with foreign enforcement agencies and overseas businesses at a much higher rate than ever before. This need for overseas enforcement is the rationale for proposals such as the Undertaking Spam, Spyware and Fraud Enforcement With Enforcers Beyond Borders Act "The U.S. Safeweb Act," S. 1608, which the Senate passed earlier this year.

In addition to having expanded international enforcement authorities, consumer protection agencies will need effective, ongoing links with enforcement-related entities in other countries. These international activities will be in addition to traditional consumer protection problems and mice-related harms conducted within the United States. Local and state consumer protection agencies will likely find it difficult to fund and staff such international efforts. Expanded international activities will thus likely require new staffing and funding at the national level.

Along with international capabilities, consumer protection agencies will need an unprecedented level of technology expertise. Effective enforcement, such as tracking down spammers or phishers, increasingly requires forensic skills of a highly technical nature. Mice hide, and it takes skilled technical people to find the pests. Agencies also need greater in-house technology expertise to cope with the rapid rate of change. From my involvement in anti-spyware and anti-phishing efforts, I know that categories of attacks shift every few months and often even more quickly. In addition, the public education role of consumer protection agencies means that the agencies must have the technical ability to understand current problems and communicate to the public about how to respond.

Summary: For large organizations, or "elephants," the basic regulatory and enforcement process is much the same offline and online. By contrast, the Internet leads to many consumer harms caused by small actors, or "mice," that hide from enforcers, often in nests outside the United States. To respond, consumer protection agencies will face an unprecedented need for international and technological capabilities. States and localities are unlikely to be as effective at the new challenges as federal agencies, and greater federal staffing and funding may therefore be needed to respond to Internet-related challenges.

III. Key Categories of Consumer Issues for the Internet

The discussion of elephants and mice provides a general way to understand when consumer protection will be different and difficult on the Internet. Mice breed quickly on the Internet, and enforcement against them poses new challenges.

There are also at least three clusters of consumer protection issues that become much more salient with the rise of the Internet. The discussion here briefly describes those clusters:

1. “The Last Mile.” Consumers need to connect to the Internet to use it. Connectivity is a new utility, complete with the possibility of monopoly power that has long been a theme of utility regulation.

2. Personal information. Personal mainframes and high connectivity mean that information about named individuals flows in unprecedented ways. Major consumer protection issues arise for privacy, data security, and personal identity.

3. Consumers as producers. Equipped with a personal mainframe, an individual can often compete with industrial producers, or at least create content based on industrial production. Bloggers compete with newspapers. Home video hobbyists compete with movie studios, or at least can alter the original movies. The law has historically treated consumers and producers differently, but new rules will be needed when individuals have the computing power to be effective producers.

The Last Mile and Connectivity as the New Utility.

Going forward, consumers will expect to have reliable and fast connections to the Internet. Connectivity becomes a new utility, similar to electricity and water as an expected part of the American household.

Connectivity thus will be a significant consumer issue. For other utilities, there has been a long tradition of public regulation. The high fixed costs of laying the “last mile” of electricity, water, or Internet connection means that there are high barriers to entry into those consumer markets. There is thus a major risk of monopoly power, and a solid intellectual rationale for concern that monopoly problems will emerge for the last mile of Internet connections.

In response, opponents of regulation have highlighted two features of the current connectivity market. First, there is the reality or potential for effective competition in the last mile, such as where cable, telephone, and other companies all might supply a house with broadband. Second, Internet connectivity is a more complex good than basic electricity or water service. We expect Internet connection speeds to continue to increase rapidly, and we expect continued innovation in the technologies for connecting users to the Internet. Under conditions of rapid change, traditional utility regulation may do a poor job of assuring consumers of good service at competitive prices.

There is a related risk of content control or discrimination by the organizations providing the last mile of connection. At its core, the current “Net neutrality” debate highlights the possibility that the companies that supply the last mile will leverage market power in the connection market into market power in content and other markets.

The history of utility regulation in the United States has included a significant role for municipal and other public provision of services. In the current era, the question is the extent to which municipalities or other government units should encourage the use of

public networks, such as municipal provision of wireless throughout a large geographic area. A recent article by Robert McChesney and John Podesta argues that public provision of utility services has historically been a key ingredient in improving results for consumers of electricity and other utilities.[4]

Summary: This preliminary paper does not assess the degree of monopoly power in the current market for the "last mile" of connectivity. Because connectivity is the new utility, however, economic growth and consumer protection depend on avoiding the monopoly problems that can develop for utility markets. Overall approaches to the last mile should include effective institutions that place checks on the emergence of monopoly power over time.

Personal Information – Privacy, Security, Identity

In a world of personal mainframes and unlimited connectivity, personal information moves over the Internet in ways that are utterly new. A compelling example is the recent loss of a laptop by an employee of the Veterans Administration (VA). With the loss of a standard laptop — what this paper calls a "personal mainframe" — the data of more than 20 million veterans was placed at risk. Even though that particular laptop was later recovered, the event serves as a vivid reminder. Unprecedented quantities of personal information are on many computers and can be transferred instantly to other computers.

For consumer protection, issues of personal information have become a much larger project. In 1996, the FTC administered one privacy law, the Fair Credit Reporting Act of 1970 (FCRA). The FCRA was focused on traditional mainframe databases, especially the credit histories held by the three market leaders. A decade later, the list of personal information rules administered by the FTC alone has mushroomed, including: the Children's Online Privacy Protection Act of 1998; the Gramm-Leach-Bliley Act of 1999; the Safe Harbor with the European Union, established in 2000; the CAN-SPAM Act of 2003; major FCRA amendments in 1996 and 2003; and identity theft laws passed in 1999 and at other times. In addition to these new legal authorities, privacy and data security have become major topics for enforcement under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive trade practices. Other sectors have also seen a large increase in attention paid to data privacy and security, such as the health privacy rules under the Health Insurance Portability and Accountability Act. In recognition of this changing landscape, the FTC in 2006 created a new Division of Privacy and Identity Protection, within its Bureau of Consumer Protection.

This overview paper will not go into great depth on how best to govern use of personal information for the Internet. I have written extensively elsewhere on the topic. Instead, the goal here will be to describe briefly four types of market failure associated with personal information and the Internet.

---

[4] Robert McChesney & John Podesta, "Let There be Wi-Fi," *Washington Monthly*, Jan.-Feb. 2006, available at http://www.washingtonmonthly.com/features/2006/0601.podesta.html.

(i) *Intrusion failure.* The unregulated market quite likely results in more telemarketing calls and spam e-mails than consumers desire or are economically efficient. Consider the incentives of a telemarketer who makes 100 calls, and breaks even with three purchases out of the 100. For those three purchases to occur, there is a classic externality — the telemarketer does not internalize the burdens on those who don't want to receive the calls. For telephone calls and spam, the burdens include the time spent by individuals dealing with unwanted intrusions. For spam, in addition, the overall usefulness of e-mail can be substantially reduced due to the effort needed to separate helpful e-mails from unwanted advertisements, fraudulent phishing e-mails, and security threats such as viruses. The response has included the FTC's National Do Not Call Registry and anti-spam legislation.

(ii) *Data breach failure.* It is very difficult for individuals to monitor how well organizations keep their personal data secure. Suppose an organization suffers a data breach, losing customers' Social Security numbers. The organization has a strong incentive to keep that fact quiet, so that it does not suffer a reputational or other loss. There is thus a potentially significant externality — the organization stays silent, but the harm is suffered by the individuals whose data has been compromised. In response, many states now require organizations to disclose data breaches, and federal legislation may pass as well.

(iii) *Privacy failure.* The same sort of monitoring problem applies to organizations' use of personal information more generally. A consumer may reveal personal information to an online company, perhaps under a company privacy policy that says the data will not be shared. If consumers cannot monitor data sales effectively, then the company has an incentive to over-use the personal data — the company profits by selling the information but the consumer suffers any loss that results from disclosure. One response to this problem has been FTC enforcement against companies that break their privacy promises to consumers.

(iv) *Unique identifier failure.* One less-widely appreciated problem arises from the incentives of organizations to over-use unique identifiers such as Social Security numbers ("SSNs") or biometrics. As computer security experts know, a secret degrades with use — the more people who know the SSN, for instance, the more likely that a fraudster will also know it. For a particular company, the SSN may be the most cost-effective way to uniquely identify a customer today. Use of the SSN by each company, however, creates an external cost to the individual. The risk to the individual of identity theft goes up as the secret is used repeatedly. The company that asks for the SSN does not suffer that risk of identity theft, but the individual does. The response, over time, should be systems of authentication that reduce the likely harm to consumers of identifying themselves in daily situations.

Summary: For uses of personal information, this paper does not advocate a particular mix of market, self-regulatory, or regulatory responses to the new challenges. Instead, it explains four categories of market failures that logically follow from the shift to personal mainframes and unlimited connectivity. Personal

information issues have already become a far greater issue for consumer protection agencies than they were historically.

Consumers as Producers

A major theme in consumer protection, going forward, is that consumers are also producers. Equipped with a personal mainframe and unlimited connectivity, individuals are newly able to produce a vast range of information-based goods. Consider activities that today are done by thousands or millions of individuals in their homes: write a blog; make and edit high-quality digital photos; transfer music and video files from one device to another, and then "sample," "mix," or otherwise alter the content; sell products worldwide from home, using eBay and other online auction sites; contribute to Wikipedia and other collaborative content; and write code for Linux and other Open Source projects. In economic terms, the barriers to entry into these markets have fallen dramatically. Ordinary individuals create information products, and distribute them worldwide through the Internet.

The fact that individuals can produce also means that an increasing portion of the value to consumers of hardware, software, and content comes from their ability to produce. Quite simply, consumers are harmed — lose value — to the extent that legal rules or market forces prevent them from producing.

When consumers also produce, they are not driven solely by the profit-maximizing model of traditional economic models. Certainly some individuals' computer use at home is motivated by profit, such as selling on an auction site. Much of the computer activity, however, has other motivations. For instance, it may be fun or relaxing to edit digital photos and share them with friends and family. Editing photos is not "work" time, and it is a mistake to see all computer use at home as "work" that should be regulated primarily as commercial activity. Computer use at home involves values that are not primarily commercial, including leisure, building community, creativity and self-expression, and reading or writing about politics and other First Amendment activity.

This new role for consumers, as producers, does not fit well into the established concepts of copyright and other intellectual property. Intellectual property has historically been written in order to encourage professional production. In movies, for instance, the chief players included professional actors and crew, the movie studios, and distribution outlets including movie theaters. Before the Internet, individuals made home movies or perhaps acted out scenes for their friends, but copyright law took little notice. With home computers and the Internet, however, many consumers want to be creative with videos — take a clip from the news or a movie, insert commentary or humor, and send the results to their friends. When consumers take clips from copyrighted movies, the industry has sharply challenged the practice as copyright violation.

The spread of personal mainframes means that society has to come to new decisions about which productions are permitted, and on what terms. If the rules are too strict — if computers are "locked down" so they can't make videos or do other things —

then consumers feel harmed. In short, there is a major consumer protection issue about the extent to which consumers will be able to produce with their new computer equipment and then use the Internet to share that production.

The combination of consumers as producers does not fit neatly into established federal agency jurisdiction. The Copyright Office and Patent and Trademark Office have historically been concerned with professional producers. The FCC may have some role to play to the extent that transmissions occur through common carriers. The FTC has not historically treated consumers-as-producers as a core mission. As a result, it is an open question, not well-discussed to date, about which institutions would best accommodate the interests of both professional producers and consumers as these issues become more salient.

A second category of issue also arises from this new role of consumers as producers. This category concerns the extent to which individual consumers should have to comply with consumer protection regimes as the individual becomes a producer. An example is that advertisers, before disseminating an advertisement, must have "adequate substantiation for all objective product claims."[5] The FTC policy on advertising claims was created during the era of the 30-second TV ad or display ad in the local newspaper. These ads were paid for by corporations. In the Internet world, however, do ads have to be substantiated when placed on individual blogs? Do individuals have to have documentation in their files before they make claims about their own Web site or other Internet activities? A similar issue arose early in 2006 when the Federal Election Commission (FEC) tried to decide the extent to which political blogs, run by individuals, had to comply with campaign finance rules. Looking ahead, there is an analogous question for data privacy and security rules, about the extent to which individuals have to comply with such rules for their Web sites, personal contacts lists, and other collections of personal information.

For this second category, there is a strong case for exempting "individuals and small businesses," in order to avoid over-regulation and red tape. On the other hand, individuals become much more significant actors when they are armed with personal mainframes and unlimited connectivity. So, the case for exemption may not exist if it turns out that harm to other consumers is being caused by the actions of individuals.

Summary: A major new fact for the Internet is the extent to which consumers are also producers. An increasing portion of the value of hardware, software, and content comes from the ability of consumers to produce — to modify information in creative ways. Limits on that ability to produce thus become a salient consumer protection issue. A second issue is the extent to which individuals must comply with generally applicable consumer protection rules when they are acting as producers.

[5] See FTC Policy Statement Regarding Advertising Substantiation, available at http://www.ftc.gov/bcp/guides/ad3subst.htm.