Protecting Consumers Online

Key Issues in Preventing Internet Privacy Intrusions, Fraud and Abuse

By Reece Rushing, Ari Schwartz and Paula Bruening[1]

The explosion of Internet commerce has delivered enormous benefits for consumers. Prices have dropped due to the ease of Internet comparison-shopping. The marketplace has expanded as barriers to entry have diminished and buyers and sellers easily link up through Web sites such as eBay. And transactions are now quickly and conveniently conducted from a home computer, without the hassle of waiting in a line, holding on the telephone or mailing a check.

These benefits, however, are being undermined by the rise in Internet privacy intrusions, fraud and abuse. An entire sub-industry has grown that aims to gather personal information on Internet users, often surreptitiously through invasive means such as spyware. This information is frequently used for unwanted marketing, but in the wrong hands it also may be used for more malicious purposes, such as identity theft, the fastest growing crime in the United States.

Consumers also are subjected to a constant barrage of annoying and frequently offensive spam e-mail. Some of this spam is sent by fraudsters posing as legitimate businesses, such as a bank where the consumer may have an account. These "phishing" e-mails typically try to con the consumer into visiting a fake Web site and then providing personal information, such as a Social Security number, which again can be used for identity theft. Even worse, many of these scams originate overseas, out of reach of U.S. law enforcement.

Unfortunately, policymakers have been slow to respond to these online threats. Congress is still debating new legislation to prevent privacy intrusion and identity theft, while the Federal Trade Commission (FTC) — the federal agency with foremost responsibility for protecting online consumers — and other law enforcement agencies have not been adequately funded or staffed to meet their new online responsibilities.

As a result, Internet privacy intrusions, fraud and abuse continue to expand, causing increasing alarm among consumers. In an April 2006 poll for the Center for American Progress, for example, 69 percent of respondents indicated they were very or somewhat worried about having their identities stolen, more than any other risk category surveyed, including getting cancer, being victimized by violent crime or being hurt or killed in a terrorist attack.[2]

---

[1] Reece Rushing is associate director for regulatory policy at the Center for American Progress. Ari Schwartz is deputy director of the Center for Democracy and Technology. Paula Bruening is staff counsel at the Center for Democracy and Technology.

[2] Poll conducted April 13-20, 2006, by Greenberg Quinlan Rosner Research for the Center for American Progress; Center for Responsible Lending; National Military Family Association; and AARP.

This rising concern has potentially severe consequences for Internet commerce. Indeed, a recent *Consumer Reports* poll found 43 percent of consumers have already "reduced their overall use of the Internet" due to concern about identity theft.[3] If consumers abandon e-commerce out of fear of being victimized, the enormous consumer benefits of the Internet will be negated.

Action is urgently needed to head off this danger. This fall, from November 6-9, the FTC will host hearings on global marketing and technology, which will present an important opportunity to identify online threats to consumers and explore policy remedies.[4] This paper highlights some of the critical issues that should be addressed and offers general recommendations for moving forward. In particular, we recommend:

- *New consumer protections for the digital age***.** First and foremost, we need comprehensive privacy legislation to safeguard personal information and protect against identity theft. In crafting this legislation and other online consumer protections, Congress should allow states freedom to innovate and adopt stronger standards — as states frequently have been more nimble in heading off online consumer threats — while also addressing the need for uniform standards in a national and global marketplace.

- *Proactive enforcement of consumer protections.* This means providing the FTC and other law enforcement agencies the authority and resources necessary to investigate and prosecute Internet crime, including fraud perpetrated outside our borders against American citizens. State attorneys general also should be recognized as vital partners in enforcement actions.

- *New tools to empower consumers.* Consumers themselves can provide one of the best defenses against Internet privacy intrusions, fraud and abuse. But first they need clear, concise information to recognize and avoid fraud and to determine which companies are safe to do business with, as well as ways to seek redress should they be victimized, including access to the courts and mechanisms for alternative dispute resolution.

These issues are explored in greater depth below.

Privacy Legislation

Privacy is at the heart of online consumer protection. Since the advent of widespread computing, the Internet and distributed databases, it has become far easier for businesses to collect, store and trade information about their customers. Frequently, the information collected includes sensitive or personally identifying data, which if not properly secured could fall into the wrong hands and lead to identity theft. Companies also may use this data to track consumer preferences and behavior, often without the consumer's knowledge or permission.

[3] *Consumer Reports* WebWatch, "Leap of Faith: Using the Internet Despite the Dangers," Oct. 26, 2005, available at http://www.consumerwebwatch.org/pdfs/princeton.pdf.
[4] For more information, see http://www.ftc.gov/bcp/workshops/techade/index.html.

Despite this unprecedented threat, there is still no single comprehensive law that spells out consumer privacy rights. Instead, a confusing patchwork of distinct, and sometimes inadequate or nonexistent, standards has grown over the years, producing more than a few oddities. For example, we reserve our strongest privacy protections for cable and video records, while travel records and online purchasing data are left disturbingly vulnerable, financial privacy laws have major exceptions, and some important uses of "public records" are left unregulated.

Congress should enact comprehensive privacy legislation based on fair information principles.

Congress should put in place a single consistent regime, based on fair information practice principles, to add some teeth and coherency to privacy protections. Specifically, consumers should be able to:

- know which companies are collecting information from them;
- provide only information necessary for a transaction;
- find out what, outside of the original transaction, companies are doing with this information;
- know who else might have access to their personal data;
- check to ensure that the data held about them is timely, accurate and complete; and
- obtain assurance that their information is held securely by all third parties.

These protections are crucial to address the new threats faced by online consumers. Consumers need to be put back in control of their personal information, so that privacy is preserved and fraud and abuse prevented.

State Protections

State privacy protections have helped fill gaps in federal law. For example, in early 2004, it was revealed that sham businesses, some intent on identity theft, had purchased the personal records of 145,000 consumers from the information services company ChoicePoint. The public learned about this security breach because of a California law that requires disclosure of data thefts. No similar federal law existed at the time, nor has one been passed since.

A major sticking point to federal privacy legislation, of course, is the issue of preemption. Business interests are currently lobbying Congress to preempt state laws with a single federal law, which they argue will make compliance simpler and easier. The problem is that the federal preemption some seek would be weaker than existing state protections.

States should be provided room to innovate and develop enhanced protections for consumers, but strong, consistent standards are important given the national and global nature of the Internet.

If federal standards are sufficiently strong, there is less need for a proliferation of new state laws. States are more likely to act where federal law is inadequate to protect consumers — as California did in requiring disclosure of security breaches involving

personal records.

Our preference would be to establish a standard of consumer protection that is a floor and not a ceiling, and to allow states to create stronger protections, so long as they do not result in inconsistency or confusion. When this is not feasible, the goal for consistent Internet legislation should be the creation of a federal standard high enough to provide consumers with robust safeguards at least as protective as the stronger existing state standards.

As with other issues in the privacy debate, the preemption issue requires honest dialogue among all affected parties to ensure both that consumer protection standards are increased nationally while businesses are not burdened with inconsistent requirements. In some cases, we may find that variations in state laws cause undue burden on business or confusion for consumers. In such cases, it may be preferable to preempt states with strong federal standards. Where preemption is applied, however, it should be narrowly focused and should not wipe out broad categories of state protections. The goal is to avoid acting prematurely in ways that unnecessarily stifle the ability of states to innovate and protect their residents.

Proactive Enforcement

Laws protecting online consumers cannot succeed without strong, proactive enforcement. Currently, however, law enforcement is poorly equipped to police Internet crime, as evidenced by the slow response to growing threats to online consumers. Only within the past several years, for example, have the FTC and Justice Department launched anti-spyware cases.[5] As a result, an illicit industry has been allowed to grow. Today, most Internet users have had spyware surreptitiously installed on their computers.

Strong enforcement requires additional funds for the FTC and other law enforcement agencies; enhanced technical expertise and computer forensics; and active engagement by state attorneys general.

To prevent problems such as spyware from mushrooming, there must be a commitment to aggressively investigate and prosecute Internet crime. This begins by providing sufficient resources to enforcement agencies, in particular the FTC. The FTC is the lead federal agency responsible for protecting consumers against spam, spyware, identity theft and other Internet fraud. However, when adjusted for inflation, the commission's budget is still about the same as 1987, well before the Internet explosion. For online consumer protection to be effective, Congress must appropriate resources commensurate with the FTC's new enforcement responsibilities.

Currently, the FTC and other federal agencies lack the necessary technical expertise and capabilities to investigate any but a relative handful of the Internet privacy intrusion, fraud and abuse cases that arise regularly. Training of law enforcement officials and investment in

[5] Center for Democracy and Technology, "Spyware Enforcement," June 2006, available at http://www.cdt.org/privacy/spyware/20060626spyware-enforcement.pdf.

computer forensics are needed so that investigators are able to uncover violations and verify consumer complaints. Partnerships with research universities can be especially helpful in this effort. The Department of Homeland Security, for instance, relies on the CERT research lab at Carnegie Mellon University for information and training on Internet security vulnerabilities. A similar arrangement with a university on Internet fraud and privacy could provide a cost-effective way to augment the federal capability.

The FTC and other federal agencies also should engage and support states as vital partners in the effort to enforce online consumer protections. It is important, in this regard, that state attorneys general be able to prosecute abuses in any area where the FTC is legally allowed to take action. A number of states are already aggressively pursuing cases against Internet privacy intrusions. For example, New York Attorney General Elliot Spitzer recently brought suit against Intermix Media Inc., for using spyware and adware to target Web users with pop-up ads. Assigning enforcement to the FTC alone would leave the commission overworked and ineffective. States can bring additional resources and expertise to bear in the fight to protect online consumers.

Cross-Border Fraud

The explosion of global commerce over the Internet complicates enforcement of online consumer protections. A victim of Internet crime might reside in the United States, but the perpetrator might be overseas, outside the reach of U.S. law enforcement. To protect against global fraud, the FTC needs the authority and resources to work with its counterparts in other countries.

The FTC has sought such power, backing the U.S. SAFEWEB Act (S. 1608) introduced by Sen. Gordon Smith (R-OR), which passed the Senate earlier this year. The House now needs to pass this important legislation.

The FTC should be granted the authority and resources necessary to work with its foreign counterparts to prevent cross-border fraud and protect privacy.

Collaboration with other countries requires staff knowledgeable about cross-border issues, foreign legal regimes and processes, and broader international issues pertinent to resolution of fraud questions. Building this knowledge base may necessitate staff exchanges, so that staff become familiar with foreign operations and build relationships with overseas counterparts. Domestically, the FTC will similarly need to develop partnerships with U.S. investigative organizations — including the Department of Justice — that work on cross-border fraud.

It is important to note that these partnerships also can be applied to address privacy violations that occur both within and outside of the United States. Privacy principles developed by the Asia Pacific Economic Cooperative (APEC), for example, anticipate the resolution of privacy violations that occur between the United States and countries in Asia. The legislative authority, the resources and the staff expertise required to address cross-border fraud will be similarly required to address privacy violations across international borders.

Private Right of Action

In the absence of strong and consistent federal and state enforcement, class-action lawsuits have been an important defense against online privacy intrusions, fraud and abuse. In 1999 and 2000, a series of cases were brought against companies that surreptitiously gathered data on Internet users. The class-action process has its problems, but these cases — and the threat of litigation — persuaded many companies to seriously address online customer privacy for the first time.

Nonetheless, class-action lawsuits have faced difficulty because consumer protection laws have not been updated to fit the online world. For this reason, the courts dismissed cases against several Internet ad companies, including DoubleClick, which had been tracking individual Web browsing.

The threat of litigation, by consumers and aggrieved companies, should be recognized and used as an important deterrent to violations of online consumer protections.

Another significant issue is that plaintiffs must demonstrate actual harm to win damages for violations of online consumer protections. This can be a high bar to meet, and has allowed some companies to escape accountability. To establish an effective deterrent to lawbreaking, Congress should specify violations in which damages may be awarded even where monetary harm or injury is not demonstrated.

These damages, however, should be proportionate to the violation. Accordingly, Congress should consider setting per-incident damages for illegal spamming, adware and other online abuses. Class-action lawsuits may be brought for telemarketing violations of the National Do Not Call Registry, for example, but damages are set at $150 per incident.

A company whose customers are harmed by another company also should be able to seek damages. For example, under the recently enacted CAN-SPAM law, Internet Service Providers (ISPs) can sue spammers. This right should be extended to surreptitiously or maliciously installed adware and other online abuses to provide consumers another layer of protection. Aggrieved companies can be expected to aggressively go after lawbreakers who jeopardize their customers and undermine profits. Indeed, online service providers such as Microsoft and AOL have already used the CAN-SPAM law to launch a host of anti-spamming lawsuits. Company-initiated lawsuits also do not face the same hurdles as class-action lawsuits (which must draw together a large number of disparate individuals), and thus may prove a more effective deterrent against online crime.

Consumer Information

Ideally, consumers will not be victimized online, and litigation will be minimized. One way to prevent online abuses is to empower consumers with information, so they can make thoughtful choices about products or services they may purchase or companies with which they may do business. This requires that companies provide clear, concise information about such matters as terms of service, privacy policies and end-user license agreements.

Providing this kind of information can present challenges, however. For instance, financial institutions have experienced difficulty complying with new privacy notice requirements contained in the Gramm-Leach-Bliley Act of 1999. Company privacy policies contain complex, often legalistic subject matter, but must be made understandable to the average consumer, who often has little time to review such notices.

Companies should provide clear, concise information about online policies, so consumers are empowered to make thoughtful choices about whom they do business with.

Business groups have developed formats for abbreviated notices on the Web. These notices display the most pertinent aspects of a service agreement or privacy policy, while allowing the consumer to "click through" to more detailed information. But Internet-based commercial activity is migrating away from desktop computers and laptops to mobile phones and other handheld devices that present formatting challenges (i.e., limited screen space) for consumer notices. Further complicating matters is the development of radio frequency identification devices (RFIDs) and other micro-devices, which advance a vision of "ubiquitous computing."

All of these developments — and new technological advances we cannot anticipate — will require that we continually monitor and enhance the consumer's ability to make online commercial decisions. The FTC, in particular, will need to participate in and oversee decisions about what kind of information should be provided to consumers, in what format and at what point in a transaction or communication. Again, this activity will require additional resources, so the commission is able to hire and retain staff who understand the issues involved.

Self-Regulation, Safe Harbors, and Alternative Dispute Resolution

The private sector also has an important role in policing itself. A significant measure of the U.S. approach to consumer protection relies upon mechanisms not established in traditional law. In particular, this includes self-regulatory regimes in which the private sector monitors and promotes compliance with consumer protections; safe harbors that create incentives for companies to comply with the law; and alternative dispute resolution that provides tools for consumers to redress grievances. These mechanisms can be particularly useful for the Internet due to their flexible, adaptive nature. However, they require oversight from the FTC to ensure effectiveness.

While well established in the offline world, self-regulatory regimes must be constantly adapted to address emerging online technology and business models. The FTC will need the resources and know-how to test these systems to assure they are sufficiently comprehensive, respond to consumer concerns and penalize companies that violate the regime's requirements and guidelines.

Self-regulatory regimes should be encouraged, but the FTC must exercise active oversight to ensure that promised benefits are delivered to consumers.

In addition, safe harbors may be useful to provide incentives for compliance. Safe harbors limit the threat of enforcement action and litigation for companies that receive third-party certification of compliance with consumer protections. Such certification, or seal, programs can relieve some

of the resource burden on government while signaling to consumers which companies are safe to do business with. The challenge in designing safe harbor — and one that still has not been successfully met — is creating incentives for companies to join without dropping the standard of consumer protection below that provided in law.

For companies that violate consumer protections, alternative dispute resolution provides a way for consumers to, short of litigation, bring complaints before a neutral third party and seek redress for grievances. Done well, this can present a low-cost, easily accessible and effective option to solve the inevitable problems that arise when using the Internet — from serious crime such as fraud, identity theft and security breaches to more routine offenses such as undelivered merchandise, billing errors and intrusive online marketing. As with self-regulation and safe harbors, however, the FTC must provide appropriate oversight and scrutiny to ensure that promised benefits are delivered to consumers.

Going Forward

Given the growing dangers to online consumers, it is striking how many issues remain unresolved and how spotty the enforcement response has been. There is both broad recognition of the problems and agreement on the need to act, but consensus has been difficult to achieve on exactly how to move forward.

Consumer advocates have pushed for a framework like that advised in this paper, while some business interests continue to resist strong standards and robust enforcement measures. The result has been a legislative logjam, with seemingly little hope for action for the remainder of the 109th Congress. There are some indicators that this could change, however. Leading Internet companies have called for comprehensive federal privacy legislation, and congressional hearings may commence soon.

The FTC hearings this fall might also help break the logjam. These hearings are meant to inform the FTC's efforts to protect online consumers over the next decade. But the commission's conclusions should also send a strong signal to policy-makers throughout government — including members of Congress — and to the business community about the direction we should take. Our hope is that the FTC will set an agenda that protects online consumers and preserves the future of Internet commerce. Before and after the FTC hearings, we encourage all stakeholders to engage in a serious dialogue to develop workable solutions that raise the bar of privacy protection for the digital economy.

This is an opportunity that we cannot afford to miss. Online consumers are increasingly being victimized by identity theft, fraud, spyware and other privacy intrusions. If these abuses are left unchecked and allowed to mushroom, consumers may be driven offline, negating the Internet's enormous consumer benefits and undercutting business profits. The challenge now is to avoid this scenario.