

Testimony of
Ari Schwartz, Deputy Director
Center for Democracy and Technology
before
The Financial Services and General Government Subcommittee
of the House Committee on Appropriations
on
“Consumer Protection Issues”
February 28, 2007

Chairman Serrano and Ranking Member Regula, thank you for holding this public hearing on Appropriations for the Federal Trade Commission (FTC). The Center for Democracy and Technology (CDT) is pleased to have the opportunity to participate.

CDT is a non-profit, public interest organization dedicated to preserving and promoting privacy, civil liberties and other democratic values on the Internet. CDT has been a widely recognized leader in the policy debate about the issues raised by spyware, phishing and related privacy threats to the Internet.¹ As we have worked to build trust on the Internet, we have participated ever more closely with the activities of the Consumer Protection Bureau at the Federal Trade Commission.

Summary

There are several new dynamics that will affect the way that the FTC pursues its consumer protection mission in the online world over the coming years. These include new laws in their jurisdiction, challenges in locating the perpetrators of online schemes, the rapid pace of technological evolution, the increasing financial motivation of malicious Internet users, and the increasingly complicated nature of international cooperation.

The FTC has taken the lead law enforcement role in fighting spyware, one of the most serious threats to the Internet's continued usefulness, stability and evolution. The Commission must be commended for recognizing early on the profound threat posed by

¹ See, e.g., CDT leads the Anti-Spyware Coalition (ASC), a group of anti-spyware software companies, academics, and public interest groups dedicated to defeating spyware; In 2006, CDT Deputy Director Ari Schwartz won the RSA Award for Excellence in Public Policy for his work in building the ASC and other efforts against spyware; "Eye Spyware," *The Christian Science Monitor*, Apr. 21, 2004 ["Some computer-focused organizations, like the Center for Democracy and Technology, are working to increase public awareness of spyware and its risks."]; "The Spies in Your Computer," *The New York Times*, Feb. 18, 2004 ["Congress will miss the point (in spyware legislation) if it regulates specific varieties of spyware, only to watch the programs mutate into forms that evade narrowly tailored law. A better solution, as proposed recently by the Center for Democracy and Technology, is to develop privacy standards that protect computer users from all programs that covertly collect information that rightfully belongs to the user."]; John Borland, "Spyware and its discontents," *CNET News.com*, Feb. 12, 2004 ["In the past few months, Ari Schwartz and the Washington, D.C.-based Center for Democracy and Technology have leapt into the front ranks of the Net's spyware-fighters."].

the rising tide of spyware and for actively moving to limit its spread. Congress should know that threats are growing in number and virulence, and that, if the FTC is going to continue to act as an critical bulwark against spyware it will need adequate funding to expand training, education, oversight and enforcement efforts.

As consumer Internet fraud increases, the FTC's ability to work with its international counterparts becomes ever more important. At the request of the Commission and with support from groups like CDT, Congress passed the SAFE WEB Act late last year to provide the FTC powers to promote international cooperation. Yet, while the Commission clearly recognizes the importance of the new law, its budget request and planning documents do not seem to adequately increase funding, staffing and expectations for international work over the next two years to move this goal forward.

Finally, CDT would like to impress upon the Committee the important role that the FTC has played in promoting good privacy practices online. For the last decade, CDT has actively urged Congress to take a more comprehensive approach to privacy. Last year, we were joined in this effort, not only by privacy advocates, but also by 14 major companies. The FTC's experience on privacy will be essential as this effort moves forward. In particular, the Commission will need adequate resources to participate in the discussion and to implement whatever legislation emerges from the process.

Many of these new dynamics have been precipitated by the Internet revolution and the growth of digital technologies. However, when adjusted for inflation, the Commission's staff in 2008 will only be 62% of the size that it was almost 30 years earlier in 1979, well before the Internet explosion.² For online consumer protection to be effective, Congress will need to appropriate resources commensurate with the FTC's new responsibilities.

I. Growth of Internet Commerce Has Led to New Roles for FTC

The exponential growth of Internet commerce has delivered enormous benefits to consumers. With low barriers to entry and a profusion of tools for comparing various sellers, e-commerce has lowered prices and expanded consumer choice. Users also benefit from the enormous convenience e-commerce provides, conducting transactions from their home offices, laptop computers and increasingly even mobile devices like PDAs and phones.

These benefits, however, are being undermined by the rise in privacy intrusions, fraud and abuse. An entire shadow industry has arisen with the sole purpose of gathering personal information on Internet users -- often surreptitiously through invasive means such as spyware. Most of this information ends up being used to bombard users with 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.

² According to the FTC, the Commission had 1,746 FTEs in 1979 (see <http://www.ftc.gov/ftc/oed/fmo/ftc2.htm>) and is requesting 1,019 in 2008 (see <http://www.ftc.gov/ftc/oed/fmo/budgetsummary08.pdf>).

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 banks or e-commerce sites where targeted consumers are likely to have live accounts. These “phishing” e-mails typically try to dupe consumers into visiting fake Web sites where they are prompted to submit passwords and personal information, such as a Social Security numbers, which can, in turn, be used for identity theft. Making matters worse, many of these scams originate overseas, out of reach of U.S. law enforcement.

Consumers are increasingly alarmed about these kinds of scams, Internet privacy intrusions, fraud and abuse. In an April 2006 poll for the Center for American Progress 69 percent of respondents indicated they were very or somewhat worried about having their identities stolen, making it the most widely cited risk category surveyed, including getting cancer, being victimized by violent crime or being hurt or killed in a terrorist attack.³

Spyware has proven especially costly for consumers. Consumer Reports estimates that the problem cost consumers \$2.6 billion last year and affected 1 in 8 Internet users.⁴ As disturbing as those figures are, even they cannot give an adequate picture of the harm caused by spyware-related privacy invasions, which can wreak havoc on Internet users lives.

To prevent problems such as spyware from mushrooming, there must be a systemic 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.

The FTC enforces the:

- Childrens Online Privacy Protection Act
- CAN-SPAM Act
- Fair and Accurate Credit Transactions Act
- Do Not Call List
- Gramm-Leach Bliley Act

And plays a lead role in addressing the growing threats related to:

- Identity theft
- Spyware
- Phishing

³ 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.

⁴ “State of the net 2006,” *ConsumerReports.org*, Sept. 2006, http://www.consumerreports.org:80/cro/electronics-computers/online-protection-9-06/state-of-the-net/0609_online-prot_state.htm.

- General Internet fraud

When we take into account the scope of the FTC's responsibilities it becomes obvious that maintaining this aggressive enforcement on behalf of American consumers requires additional funds for the FTC. The online marketplace will become both more complex and more essential over time, and the FTC has been and will continue to be a critical force in maintaining consumer trust in the Internet. Increased resources are a vital part of making that happen.

II. New Challenges in Investigating Malicious Internet Actors

In the early days of Internet crime, a vast number of offenses amounted to little more than virtual vandalism. Hackers would often circumvent Internet security as a way of showing off to their friends and proving their skills. That trend has long been on the decline, as malicious actors on the Internet are increasingly going after financial gain first and foremost.⁵ This means that more consumers are losing more money than ever before either as a direct or indirect result of malicious activity online, and that malicious hackers have more financial resources than ever before. As a result, the FTC's consumer protection mission is at its most vital moment. Compensating consumers who have been harmed and putting a stop to fraudulent schemes becomes ever more important as fraud and monetary loss become more widespread.

As the FTC's role in fighting new fraud increases, its job becomes more complicated. One of the great paradoxes of the Internet is that while most Internet users are having their movements tracked and traced in ways never before imagined, those that are willing to take the time and energy can hide the tracks of their online activities in ways that make them very difficult to find. While this is a huge boon for free expression around the world, it also can help criminals and malicious Internet operations to evade the grasp of law enforcement. Using just a few simple tools, criminals and scammers can quickly and easily cloak their identities and locations. Tracking them down may require the assistance of multiple network operators, applications providers and technical experts to unravel a complex web of online identities and cloaking services.

Tracking individuals online is made more complicated by the fact that many malicious Internet schemes involve groups of companies, affiliates, and individuals acting together to defraud consumers. Not only must the identities and locations of all of these actors be traced, but the business arrangements and relationships between them must also be sorted out before law enforcers can act. The Internet's distributed nature lends itself to arrangements wherein multiple parties each contribute to form a complete operation or business plan. This characteristic has helped to provide all kinds of new services, but it may be exploited just as easily for malevolent purposes as for benevolent ones. The complexity of these arrangements will likely continue to grow as malicious Internet users realize that working with many different parties complicates enforcement and spreads liability to multiple entities.

⁵ Krebs, Brian, "The Computer Bandit," *The Washington Post Magazine*, Feb. 19, 2006.

The global nature of the Internet further complicates the task of apprehending malicious online actors. Internet scams are increasingly based overseas or in multiple countries at once, adding a whole new dimension to enforcement investigations. Law enforcers must cultivate relationships with their foreign counterparts in order to increase cooperation when it comes time to conduct investigations. The same is true for domestic enforcement across multiple states. The FTC has always had the authority and the willingness to cooperate with state attorneys general on enforcement matters, and the Internet makes these cases ever more likely since consumers from many different states may be affected by a single online scam.⁶ In order to be fruitful, this cooperation requires all parties to expend extra resources.

Because of the rapid changes involved with Internet scams, investigations of Internet fraud are becoming increasingly technologically intensive. Although vast resources may not have been required when the FTC first began investigating online scams, technological advances over the past few years have heightened the level of sophistication necessary for successful investigations. If the FTC is to continue as a leader in online enforcement, it must keep pace with these changes.

The Internet revolution also complicates FTC oversight of completed cases. Before digital technologies became pervasive, it was much easier for the FTC to monitor whether former defendants were complying with the provisions of their settlement agreements or court orders. The Internet provides simple means for such actors to quickly and easily setup new schemes under new monikers in new locations, making it difficult for the FTC to draw links to former businesses or identities and determine compliance.

All of this technological evolution impacts FTC resources in four ways:

- Training and consultations with outside experts may be necessary in order to strengthen the knowledge base of FTC investigators.
- Sophisticated equipment may be needed in order to track and understand the intricacies of online schemes, and also for the purposes of evidence gathering.
- The amount of time necessary to conduct investigations may increase due to the technical complexities of determining and proving how a particular malicious enterprise works and who is behind it. The same is true for oversight, where monitoring functions may become increasingly resource-intensive.
- The pool of resources dedicated to consumer education will undoubtedly grow. Frequent and rapid changes in technology can be difficult for consumers with minimal technical expertise to comprehend, and the FTC is a major source of guidance for consumers looking to protect themselves online.

In all of these ways, the fast pace of technological change demonstrates the need for the FTC to expend new resources in order to stay up to speed.

⁶ See, e.g., “FTC, Washington Attorney General, Sue to Halt Unfair Movieland Downloads,” *Federal Trade Commission*, Aug. 15, 2006, <http://www.ftc.gov/opa/2006/08/movieland.htm>.

III. FTC's Leading Role in Spyware Enforcement: Setting An Example for the Future

Four years ago, very few people were familiar with the term “spyware.” Consumers were just beginning to witness the effects of unwanted software that appeared unexpectedly on their home computers. Since that time, consumers have been increasingly deluged with programs that they never knowingly installed on their computers. Often these programs make themselves difficult to remove, expose users’ personal data, open security holes, and undermine performance and stability of their systems. The FTC was one of the first law enforcement bodies to take note of this menace. Since then, the Commission has been leading the charge in the spyware fight in three key ways: engaging in enforcement actions, developing guiding principles for enforcers, and establishing industry standards.

The Commission filed the nation’s first spyware lawsuit in late 2004 against a network of deceptive adware distributors and their affiliates.⁷ This case struck at the heart of one of the most nefarious spyware schemes on the Internet. The scammers involved were secretly installing software that left consumers’ computers vulnerable to hackers, and then duping those same users into purchasing fake security software to help repair their systems. Not only did the FTC succeed in the case – obtaining a \$4 million order against the primary defendant and over \$300,000 in disgorgement from the other defendants – but the investigations in the case opened up several additional leads that contributed to the FTC’s pursuit of other malicious software distributors. In the more than two years since launching this first suit, the FTC has engaged in a total of 11 spyware enforcement actions, all of which have ended with settlements or court orders that benefit consumers.

In prosecuting these cases, the FTC has used its broad authority to challenge unfair and deceptive practices, recognizing that many spyware behaviors are illegal under existing law. However, the FTC has not been haphazard in choosing which cases to pursue. As the common characteristics of spyware began to reveal themselves, the FTC established three principles to guide its spyware enforcement efforts:⁸

- *A consumer’s computer belongs to him or her, not to the software distributor.* This means that no software maker should be able to gain access to or use the resources of a consumer’s computer without the consumer’s consent.
- *Buried disclosures do not work.* Communicating material terms about the functioning of a software program deep within an End User License Agreement (EULA) does not meet high enough standards for adequate disclosure.
- *Consumers must be able to uninstall or disable software that they do not want.* If a software distributor places an unwanted program on a consumer’s computer, there should be a reasonably straightforward way for that program to be removed.

⁷ *FTC v. Seismic Entertainment, Inc., et al.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

⁸ *Remarks of Deborah Platt Majoras, Chairman, Federal Trade Commission*, Anti-Spyware Coalition Public Workshop, Feb. 9, 2006, <http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf>.

In addition to serving as a guide for the FTC, these principles have helped to direct state law enforcers who have begun to take on spyware cases. The spyware space is fraught with gray areas – software behaviors that may be perfectly legitimate in one circumstance may be considered highly malicious in another. Some states have passed specific spyware statutes to help clarify these distinctions, but several of the states that have been most active in spyware enforcement have no such laws in place. The FTC’s guiding principles provide a simple, understandable baseline for current and future law enforcers as they wade into spyware issues with which they may be unfamiliar. In this way, the leadership of the FTC has been a vital component in expanding the nationwide pool of law enforcement resources dedicated to combating spyware.

The FTC has also played an integral role in establishing standards for the software industry as a whole. In two of its most recent enforcement efforts, the FTC reached settlement agreements with adware distributors that required the distributors to clearly and conspicuously disclose material terms about their adware programs *outside of any End User License Agreement (EULA)*.⁹ With these requirements the FTC has set a disclosure guideline that can be applied across the software industry, for the benefit of consumers. Not only were the adware distributors themselves forced to abandon deceptive or nonexistent disclosures, but software vendors throughout the industry were also put on notice about what constitutes legitimate behavior. The FTC’s leadership in this respect has helped to curb uncertainty in the software industry while creating a better online experience for consumers.

The effectiveness of the FTC’s spyware enforcement program in all of these regards – pursuing spyware purveyors, developing guiding enforcement principles, and establishing industry standards – has been made possible by two important characteristics of FTC consumer protection operations. The first is that the Commission had the freedom to delve into uncharted territory when the threat of spyware first became apparent. This flexibility allowed the FTC to build its knowledge of spyware early enough to keep pace with the evolution of the threat that it posed. Second, the FTC was afforded sufficient resources to engage in the complex, technology-intensive investigations that were necessary to identify unfair and deceptive practices and track down the perpetrators of those practices. Having the training and technological expertise to identify and locate spyware purveyors has been critical to the FTC’s success in this area.

Freedom to chart a new course and sufficient resources to engage in technology-intensive investigations will undoubtedly be essential to the FTC’s consumer protection mission as new online threats arise. Internet scams are increasingly complex, multi-national, and financially motivated. This makes enforcement an even greater challenge that will require the FTC to think, act, and use its resources in new ways. The success of the FTC spyware

⁹ See *In the Matter of Zango, Inc., formerly known as 180solutions, Inc., Keith Smith, and Daniel Todd*, FTC File No. 052 3130 (filed Nov. 3, 2006), available at <http://www.ftc.gov/os/caselist/0523130/index.htm>; *In the Matter of DirectRevenue LLC, DirectRevenue Holdings LLC, Joshua Abram, Daniel Kaufman, Alan Murray, and Rodney Hook*, FTC File No. 052 3131 (filed Feb. 16, 2007), available at <http://ftc.gov/os/caselist/0523131/index.htm>.

enforcement program shows what a strong leader the Commission can become when it is afforded the flexibility and resources necessary to tackle an emerging enforcement problem. As the FTC budget and performance plans are set for the coming years, these two aspects of FTC consumer protection operations should be fully supported and augmented as necessary to ensure that future enforcement efforts may be as successful as the spyware program has been.

IV. International Cooperation is Essential

The profusion 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 was recently granted special authority to work with its counterparts in other countries by the U.S. SAFE WEB Act. However, in part because of unfortunate timing, the budget request from the Commission does not seem to adequately recognize this important change.

Collaboration with other countries requires a staff that is 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 need to develop similar 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.¹⁰ The resources, legislative authority, and staff expertise required to address cross-border fraud will be similarly required to address privacy violations across international borders.

Although the FTC made its budget request prior to the passage of SAFE WEB, CDT remains concerned that neither the FTC Performance Plan nor the Budget Summary adequately recognize the growing international challenges and the resources that will be needed to deal with them. The Performance Plan suggests that it will cooperate with international law enforcement on 20 cases in 2007 with 30 FTE working on international cooperation. The numbers for 2008 are identical. Considering the high number of Internet cases that contain international components,¹¹ setting the bar at 20 cases – out of over 400

¹⁰ *APEC Privacy Framework*, 16th APEC Ministerial Meeting, Nov. 2004, http://www.apec.org/apec/news_media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html.

¹¹ See, e.g., Stone, Brad, “Spam Doubles, Finding New Ways to Deliver Itself,” *The New York Times*, Dec. 6, 2006.

projected consumer protection cases in total – seems very low. The fact that the FTC’s expectation of cases and staffing remains stagnant into 2008 causes even greater concern, since it suggests that the Commission does not plan to exercise its new powers from SAFE WEB any further as it learns from its experience over the first year of the law’s implementation. CDT hopes that the Commission will update its plans and resource requests to adequately reflect SAFE WEB implementation.

IV. Privacy Threats Increase FTC Need for Forensic and Enforcement Resources

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, can become a tool for identity theft. Companies also may use this data to track consumer preferences and behavior, often without the consumer’s knowledge or permission.

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 developed 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.

Over the past nine years, CDT has urged Congress to enact a single consistent regime, based on fair information practice principles. Specifically, consumers should be able to:

- know which companies are collecting information from them;
- provide only information necessary for a transaction;
- find out what companies are doing with this information beyond the original transaction;
- 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.

We believe that 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.

When this law is finally passed, the FTC, with its leadership role on these issues to date, will undoubtedly be asked to enforce these new privacy protections as well. We hope that as the privacy issue is debated, a plan for enforcing the law will be considered concurrently. While the long-term streamlining of privacy law will make educational and other efforts easier, we hope that Congress will recognize that the historic effort of protecting Americans’ privacy will require significant resources to implement.

V. Addressing Common Carrier Exemption

The FTC for many years has asked that the exemption that prevents the Commission from exercising general jurisdiction over telecommunications “common carriers” be rescinded.

The idea of creating a level playing field is appealing, particularly when some communications services fall within the jurisdiction of the FTC. In particular, lifting the restriction in certain areas - such as billing, advertising and telemarketing - could ensure that the agency with the most expertise in these areas is taking a leading role.

However, rescinding the exemption completely could lead to duplication of government regulation and/or confusion for consumers in certain areas. For example, telecommunications companies are already subject to the Customer Proprietary Network Information (CPNI) rules administered by the Federal Communications Commission, which limit reuse and disclosure of information about individuals' use of the phone system including whom they call, when they call, and other features of their phone service. At this point, we are not sure it would be wise to take this issue away from the FCC. Similar questions may arise with other issues: Which agency would take the lead? By which rules would a complaint about deceptive notice be addressed? How will these decisions be made?

The Commission has been thoughtful in these areas in the past, so it is likely that any concerns could be addressed. If this proposal should move further, the Commission would need to be able to have a detailed examination and plan for dealing with similar areas of overlap including the kind of resources needed to dispatch its newly expanded duties in the telecommunications space.. Congress should also take part in studying this issue further.

V. Conclusion

CDT does not have all of the budget data nor expertise necessary to be in a position to offer suggestions on exact FTC funding and allocation amounts, however, we feel confident in recommending that FTC resources should be steadily increased given all of the new factors discussed in this testimony. The Internet has touched every sector of the FTC's consumer protection mission, and although digital innovations have simplified some tasks, they bring their own new challenges in training, education, oversight, and – perhaps most intensely – enforcement. The Commission has aptly demonstrated its leadership in online consumer protection, and yet it is surviving with pre-Internet staffing. We urge this Committee to find ways for FTC resources to match the demands of the Internet age.