November 29, 2005
Cybercrime and Other Pests

- Computer Fraud and Abuse Act, 18 U.S.C. § 1030
- *U.S. v. Morris*, 928 F.2d 504 (1991)
- *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003)
- CAN-SPAM, S.877, 108th Congress, <http://www.spamlaws.com/federal/108s877.shtml>
- MAPS, *Introduction to the Realtime Blackhole List (RBL) servers*, <http://www.mail-abuse.com/wp_introrbl.html>
- Yahoo!, DomainKeys, <http://antispam.yahoo.com/domainkeys>
- *Code*, chapters 15-17, appendix

For further reading (optional):

- David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. Rev. 325 (2001), <http://www.spamlaws.com/articles/usf.html>
- David Johnson, Susan Crawford, and John Palfrey, *The Accountable Net: Peer Production of Internet Governance*, 9 Va. J.L. & Tech. 9 (2004) <http://cyber.law.harvard.edu/home/uploads/336/AccountableInternet.pdf>
- Electronic Frontier Foundation, *Noncommercial Email Lists: Collateral Damage in the Fight Against Spam*, <http://www.eff.org/wp/?f=SpamCollateralDamage.html>

For every good thing, there are those who try to mess it up; the Internet is no exception. Put communications online and some will try to intercept or disrupt them; enable online commerce, and some will try online theft (not only of funds, but of data or identities). In many of our prior discussions, we have seen existing law applied or adapted to online activity. Here, we look into some areas of *sui generis* law, legislation aimed specifically at online problems: cybercrime and spam. Are these in fact areas where pre-Internet law, code, and markets fail? If so, does the new law address the failure or add to the confusion?

The Computer Fraud and Abuse Act (CFAA) is the major "anti-hacking" law. CFAA criminalizes "access[ing] a computer without authorization" or "exceeding authorized access" to a computer system or network. Over its history, the statute has been expanded from a narrow class of federal and financial institution computers to any computer used in interstate or foreign commerce. What is the difference between "accessing without authorization" and "exceeding authorized access"? Where is that distinction between outsiders and insiders relevant?

Consider how "authorization" for access is given or denied, especially in the context of a publicly accessible computer system. Many websites post "terms of service," and many interactive systems show "banners" when a user logs in, e.g. "By logging onto this machine you agree to the TOS posted here: <http://www.speakeasy.net/content/internetservices/shelltos.html>." Are these sufficient

to make unwelcome use or access a crime? If it depends on the notice given to the system's user, how might this notice compare with that sufficient to form a contract?

While junk mail is not new, it has expanded to new dimensions online. Businesses find email a cheap means of contacting targets, some of whom want some of the communications, many of whom do not. Unsolicited communications clog mailservers and inboxes. In response, service providers and end-users have turned to self-help: filters; blacklists (rejection based on keywords or IP addresses); whitelists (acceptance based trusted sender addresses or signatures such as DomainKeys); user verification (see, e.g., www.spamarrest.com); and blackhole lists. Skim MAPS, *Introduction to the Realtime Blackhole List (RBL) servers,* <http://www.mail-abuse.com/wp_introrbl.html> and Yahoo!, DomainKeys, <http://antispam.yahoo.com/domainkeys>.

Consider the transparency of these spam-blocking measures, especially when they operate at the ISP level. Do you know what spam-blocking, if any, is active on your email accounts?

The CAN-SPAM Act of 2003 was Congress's response to increasing public complaint and to a patchwork of state laws. CAN-SPAM is often derided by its critics as the "You Can Spam" Act, many of whom complain that it preempted more powerful state laws. What does CAN-SPAM actually prevent? What are its enforcement mechanisms? Does the law solve problems code did not?

Computer Fraud and Abuse Act (CFAA)
18 USCS § 1030 (2005)

§ 1030. Fraud and related activity in connection with computers

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph (y) of section 11 of the Atomic Energy Act of 1954 [42 USCS § 2014(y)], with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5,000 in any 1-year period;

(5) (A) (i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in

the case of an attempted offense, would, if completed, have caused)--

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $ 5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; [or]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1) (A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section; or an attempt to commit an offense punishable under this subparagraph;

(2) (A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $ 5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3) (A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this section;

(4) (A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and

(5) (A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title [18 USCS § 3056(a)].

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section--

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage

functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means--

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934 [15 USCS § 78o];

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978 [12 USCS § 3101(1) and (3)]); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive department enumerated in section 101 of title 5;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is

unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection [enacted Sept. 13, 1994], concerning investigations and prosecutions under subsection (a)(5).

United States v. Morris,
928 F.2d 504 (2d Cir. 1991)

OPINION: NEWMAN, Circuit Judge.

This appeal presents two narrow issues of statutory construction concerning a provision Congress recently adopted to strengthen protection against computer crimes. Section 2(d) of the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a)(5)(A) (1988), punishes anyone who intentionally accesses without authorization a category of computers known as "federal interest computers" and damages or prevents authorized use of information in such computers, causing loss of $ 1,000 or more. The issues raised are (1) whether the Government must prove not only that the defendant intended to access a federal interest computer, but also that the defendant intended to prevent authorized use of the computer's information and thereby cause loss; and (2) what satisfies the statutory requirement of "access without authorization." …

In the fall of 1988, Morris was a first-year graduate student in Cornell University's computer science Ph.D. program. Through undergraduate work at Harvard and in various jobs he had acquired significant computer experience and expertise. When Morris entered Cornell, he was given an account on the computer at the Computer Science Division. This account gave him explicit authorization to use computers at Cornell. Morris engaged in various discussions with fellow graduate students about the security of computer networks and his ability to penetrate it.

In October 1988, Morris began work on a computer program, later known as the INTERNET "worm" or "virus." The goal of this program was to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered. The tactic he selected was release of a worm into network computers. Morris designed the program to spread across a national network of computers after being inserted at one computer location connected to the network. Morris released the worm into INTERNET, which is a group of national networks that connect university, governmental, and military computers around the country. The network permits communication and transfer of information between computers on the network.

Morris sought to program the INTERNET worm to spread widely without drawing attention to itself. The worm was supposed to occupy little computer operation time, and thus not interfere with normal use of the computers. Morris programmed the worm to make it difficult to detect and read, so that other programmers would not be able to "kill" the worm easily.…

Morris identified four ways in which the worm could break into computers on the network:
(1) through a "hole" or "bug" (an error) in SEND MAIL, a computer program that transfers and receives electronic mail on a computer;
(2) through a bug in the "finger demon" program, a program that permits a person to

obtain limited information about the users of another computer;
(3) through the "trusted hosts" feature, which permits a user with certain privileges on one computer to have equivalent privileges on another computer without using a password; and
(4) through a program of password guessing, whereby various combinations of letters are tried out in rapid sequence in the hope that one will be an authorized user's password, which is entered to permit whatever level of activity that user is authorized to perform.

On November 2, 1988, Morris released the worm from a computer at the Massachusetts Institute of Technology. MIT was selected to disguise the fact that the worm came from Morris at Cornell. Morris soon discovered that the worm was replicating and reinfecting machines at a much faster rate than he had anticipated. Ultimately, many machines at locations around the country either crashed or became "catatonic." When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent reinfection. However, because the network route was clogged, this message did not get through until it was too late. Computers were affected at numerous installations, including leading universities, military sites, and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $ 200 to more than $ 53,000. …

DISCUSSION

…Section 1030(a)(5)(A) penalizes the conduct of an individual who "intentionally accesses a Federal interest computer without authorization." Morris contends that his conduct constituted, at most, "exceeding authorized access" rather than the "unauthorized access" that the subsection punishes. Morris argues that there was insufficient evidence to convict him of "unauthorized access," and that even if the evidence sufficed, he was entitled to have the jury instructed on his "theory of defense."

We assess the sufficiency of the evidence under the traditional standard. Morris was authorized to use computers at Cornell, Harvard, and Berkeley, all of which were on INTERNET. As a result, Morris was authorized to communicate with other computers on the network to send electronic mail (SEND MAIL), and to find out certain information about the users of other computers (finger demon). The question is whether Morris's transmission of his worm constituted exceeding authorized access or accessing without authorization.

The Senate Report stated that section 1030(a)(5)(A), like the new section 1030(a)(3), would "be aimed at 'outsiders,' *i.e.*, those lacking authorization to access any Federal interest computer." Senate Report at 10, U.S. Code Cong. & Admin. News at 2488. But the Report also stated, in concluding its discussion on the scope of section 1030(a)(3), that it applies "where the offender is completely outside the Government, . . . *or where the offender's act of trespass is interdepartmental in nature." Id.* at 8, U.S. Code Cong. & Admin. News at 2486 (emphasis added).

Morris relies on the first quoted portion to argue that his actions can be characterized only as exceeding authorized access, since he had authorized access to a federal interest computer. However, the second quoted portion reveals that Congress was not drawing a bright line between those who have some access to any federal interest computer and those who have none. Congress contemplated that individuals with access to some federal interest computers would be subject to liability under the computer fraud provisions for gaining unauthorized access to other federal interest computers. *See, e.g., id.* (stating that a Labor Department employee who uses Labor's computers to access without authorization an FBI computer can be criminally prosecuted).

The evidence permitted the jury to conclude that Morris's use of the SEND MAIL and finger demon features constituted access without authorization. While a case might arise where the use of SEND MAIL or finger demon falls within a nebulous area in which the line between accessing without authorization and exceeding authorized access may not be clear, Morris's conduct here falls well within the area of unauthorized access. Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers.

Moreover, the jury verdict need not be upheld solely on Morris's use of SEND MAIL and finger demon. As the District Court noted, in denying Morris' motion for acquittal,

> Although the evidence may have shown that defendant's initial insertion of the worm simply exceeded his authorized access, the evidence also demonstrated that the worm was designed to spread to other computers at which he had no account and no authority, express or implied, to unleash the worm program. Moreover, there was also evidence that the worm was designed to gain access to computers at which he had no account by guessing their passwords. Accordingly, the evidence did support the jury's conclusion that defendant accessed without authority as opposed to merely exceeding the scope of his authority.

In light of the reasonable conclusions that the jury could draw from Morris's use of SEND MAIL and finger demon, and from his use of the trusted hosts feature and password guessing, his challenge to the sufficiency of the evidence fails.…

EF Cultural Travel BV v. Zefer Corp.,
318 F.3d 58 (1st Cir. 2003)

OPINION: BOUDIN, Chief Judge.

Defendant Zefer Corporation ("Zefer") seeks review of a preliminary injunction prohibiting it from using a "scraper tool" to collect pricing information from the website of plaintiff EF Cultural Travel BV ("EF"). This court earlier upheld the injunction against co-defendant Explorica, Inc. ("Explorica"). EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) ("EF I"). The validity of the injunction as applied to Zefer was not addressed because Zefer's appeal was stayed when it filed for bankruptcy, but the stay has now been lifted.

EF and Explorica are competitors in the student travel business. Explorica was started in the spring of 2000 by several former EF employees who aimed to compete in part by copying EF's prices from EF's website and setting Explorica's own prices slightly lower. EF's website permits a visitor to the site to search its tour database and view the prices for tours meeting specified criteria such as gateway (e.g., departure) cities, destination cities, and tour duration. In June 2000, Explorica hired Zefer, which provides computer-related expertise, to build a scraper tool that could "scrape" the prices from EF's website and download them into an Excel spreadsheet.

A scraper, also called a "robot" or "bot," is nothing more than a computer program that accesses information contained in a succession of webpages stored on the accessed computer. Strictly speaking, the accessed information is not the graphical interface seen by the user but rather the HTML source code--available to anyone who views the site--that generates the graphical interface. This information is then downloaded to the user's computer. The scraper program used in this case was not designed to copy all of the information on the accessed pages (e.g., the descriptions of the tours), but rather only the price for each tour through each possible gateway city.

Zefer built a scraper tool that scraped two years of pricing data from EF's website. After receiving the pricing data from Zefer, Explorica set its own prices for the public, undercutting EF's prices an average of five percent. EF discovered Explorica's use of the scraper tool during discovery in an unrelated state-court action brought by Explorica's President against EF for back wages.

EF then sued Zefer, Explorica, and several of Explorica's employees in federal court. n1 Pertinently, EF sought a preliminary injunction on the ground that the copying violated the federal Copyright Act, 17 U.S.C. § 101 et seq. (2000), and various provisions of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 (2000). The district court refused to grant EF summary judgment on its copyright claim, but it did issue a preliminary injunction against all defendants based on one provision of the CFAA, ruling that the use of the scraper tool went beyond the "reasonable expectations" of ordinary users. …

What appears to have happened is that Philip Gormley, Explorica's Chief Information Officer and EF's former Vice President of Information Strategy, e-mailed Zefer a description of how EF's website was structured and identified the information that Explorica wanted to have copied; this may have facilitated Zefer's development of the scraper tool, but there is no indication that the structural information was unavailable from perusal of the website or that Zefer would have known that it was information subject to a confidentiality agreement.

EF also claims that Gormley e-mailed Zefer the "codes" identifying in computer shorthand the names of EF's gateway and destination cities. These codes were used to direct the scraper tool to the specific pages on EF's website that contained EF's pricing information. But, again, it appears that the codes could be extracted more slowly by examining EF's webpages manually, so it is far from clear that Zefer would have had to know that they were confidential. The only information that Zefer received that was described as confidential (passwords for tour-leader access) apparently had no role in the scraper project.

- - - - - - - - - - - - - - Footnotes - - - - - - - - - - - - - -
n2 As an example, the website address for an EF Tour to Paris and Geneva leaving from Boston is
http://www.eftours.com/public/browse/browse_detail.asp?CTID=PTG%20V&GW=BOS
Looking closely at the website address, one can determine that the destination code for the Paris and Geneva tour is PTG, while the gateway code for Boston is BOS.
- - - - - - - - - - - - - End Footnotes- - - - - - - - - - - - - -

…The issue … is whether use of the scraper "exceeded authorized access." A lack of authorization could be established by an explicit statement on the website restricting access. (Whether public policy might in turn limit certain restrictions is a separate issue.) Many webpages contain lengthy limiting conditions, including limitations on the use of scrapers. However, at the time of Zefer's use of the scraper, EF had no such explicit prohibition in place, although it may well use one now.

The district court thought that a lack of authorization could also be inferred from the circumstances, using "reasonable expectations" as the test; and it said that three such circumstances comprised such a warning in this case: the copyright notice on EF's homepage with a link directing users to contact the company with questions; EF's provision to Zefer of confidential information obtained in breach of the employee confidentiality agreements; and the fact that the website was configured to allow ordinary visitors to the site to view only one page at a time.

We agree with the district court that lack of authorization may be implicit, rather than explicit. After all, password protection itself normally limits authorization by implication (and technology), even without express terms. But we think that in general a reasonable expectations test is not the proper gloss on subsection (a)(4) and we reject it. However useful a reasonable expectations test might be in other contexts where there may be a common understanding underpinning the notion, cf. Terry v. Ohio, 392 U.S. 1, 9, 20 L.

Ed. 2d 889, 88 S. Ct. 1868 (1968) (Fourth Amendment), its use in this context is neither prescribed by the statute nor prudentially sound.

Our basis for this view is not, as some have urged, that there is a "presumption" of open access to Internet information. The CFAA, after all, is primarily a statute imposing limits on access and enhancing control by information providers. Instead, we think that the public website provider can easily spell out explicitly what is forbidden and, consonantly, that nothing justifies putting users at the mercy of a highly imprecise, litigation-spawning standard like "reasonable expectations." If EF wants to ban scrapers, let it say so on the webpage or a link clearly marked as containing restrictions.

This case itself illustrates the flaws in the "reasonable expectations" standard. Why should the copyright symbol, which arguably does not protect the substantive information anyway, Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 344-45, 113 L. Ed. 2d 358, 111 S. Ct. 1282 (1991), or the provision of page-by-page access for that matter, be taken to suggest that downloading information at higher speed is forbidden. EF could easily include--indeed, by now probably has included--a sentence on its home page or in its terms of use stating that "no scrapers may be used," giving fair warning and avoiding time-consuming litigation about its private, albeit "reasonable," intentions.

Needless to say, Zefer can have been in no doubt that EF would dislike the use of the scraper to construct a database for Explorica to undercut EF's prices; but EF would equally have disliked the compilation of such a database manually without the use of a scraper tool. EF did not purport to exclude competitors from looking at its website and any such limitation would raise serious public policy concerns. Cf. Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505, 516-18 (4th Cir. 1999); Desnick v. Am. Broad. Cos., 44 F.3d 1345, 1351 (7th Cir. 1995).

[W]e conclude that the district court's rationale does not support an independent preliminary injunction against Zefer, [but] there is no apparent reason to vacate the present injunction "as against Zefer." Despite being a party to the case, Zefer is not named in the ordering language of the injunction; it is merely precluded, like anyone else with notice, from acting in concert with, on behalf of, or at the direction of Explorica to use the scraper to access EF's information.

…[F]or future litigation among other litigants in this circuit [we] indicate that, with rare exceptions, public website providers ought to say just what non-password protected access they purport to forbid.

CAN-SPAM Act of 2003

S.877, 108th Congress

An Act

To regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the `Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003', or the `CAN-SPAM Act of 2003'.

SEC. 2. CONGRESSIONAL FINDINGS AND POLICY.

(a) FINDINGS- The Congress finds the following:

(1) Electronic mail has become an extremely important and popular means of communication, relied on by millions of Americans on a daily basis for personal and commercial purposes. Its low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce.

(2) The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited commercial electronic mail is currently estimated to account for over half of all electronic mail traffic, up from an estimated 7 percent in 2001, and the volume continues to rise. Most of these messages are fraudulent or deceptive in one or more respects.

(3) The receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail, or for both.

(4) The receipt of a large number of unwanted messages also decreases the convenience of electronic mail and creates a risk that wanted electronic mail messages, both commercial and noncommercial, will be lost, overlooked, or discarded amidst the larger volume of unwanted messages, thus reducing the reliability and usefulness of electronic mail to the recipient.

(5) Some commercial electronic mail contains material that many recipients may consider vulgar or pornographic in nature.

(6) The growth in unsolicited commercial electronic mail imposes significant monetary costs on providers of Internet access services, businesses, and educational and nonprofit institutions that carry and

receive such mail, as there is a finite volume of mail that such providers, businesses, and institutions can handle without further investment in infrastructure.

(7) Many senders of unsolicited commercial electronic mail purposefully disguise the source of such mail.

(8) Many senders of unsolicited commercial electronic mail purposefully include misleading information in the messages' subject lines in order to induce the recipients to view the messages.

(9) While some senders of commercial electronic mail messages provide simple and reliable ways for recipients to reject (or `opt-out' of) receipt of commercial electronic mail from such senders in the future, other senders provide no such `opt-out' mechanism, or refuse to honor the requests of recipients not to receive electronic mail from such senders in the future, or both.

(10) Many senders of bulk unsolicited commercial electronic mail use computer programs to gather large numbers of electronic mail addresses on an automated basis from Internet websites or online services where users must post their addresses in order to make full use of the website or service.

(11) Many States have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but these statutes impose different standards and requirements. As a result, they do not appear to have been successful in addressing the problems associated with unsolicited commercial electronic mail, in part because, since an electronic mail address does not specify a geographic location, it can be extremely difficult for law-abiding businesses to know with which of these disparate statutes they are required to comply.

(12) The problems associated with the rapid growth and abuse of unsolicited commercial electronic mail cannot be solved by Federal legislation alone. The development and adoption of technological approaches and the pursuit of cooperative efforts with other countries will be necessary as well.

(b) CONGRESSIONAL DETERMINATION OF PUBLIC POLICY- On the basis of the findings in subsection (a), the Congress determines that--

(1) there is a substantial government interest in regulation of commercial electronic mail on a nationwide basis;

(2) senders of commercial electronic mail should not mislead recipients as to the source or content of such mail; and

(3) recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from the same source.

SEC. 3. DEFINITIONS.

In this Act:

(1) AFFIRMATIVE CONSENT- The term `affirmative consent', when used with respect to a commercial electronic mail message, means that--

(A) the recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative; and

(B) if the message is from a party other than the party to which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient's electronic mail address could be transferred to such other party for the purpose of initiating commercial electronic mail messages.

(2) Commercial electronic mail message-

(A) IN GENERAL- The term `commercial electronic mail message' means any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose).

(B) TRANSACTIONAL OR RELATIONSHIP MESSAGES- The term `commercial electronic mail message' does not include a transactional or relationship message.

(C) REGULATIONS REGARDING PRIMARY PURPOSE- Not later than 12 months after the date of the enactment of this Act, the Commission shall issue regulations pursuant to section 13 defining the relevant criteria to facilitate the determination of the primary purpose of an electronic mail message.

(D) REFERENCE TO COMPANY OR WEBSITE- The inclusion of a reference to a commercial entity or a link to the website of a commercial entity in an electronic mail message does not, by itself, cause such message to be treated as a commercial electronic mail message for purposes of this Act if the contents or circumstances of the message indicate a primary purpose other than commercial advertisement or promotion of a commercial product or service.

(3) COMMISSION- The term `Commission' means the Federal Trade Commission.

(4) DOMAIN NAME- The term `domain name' means any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.

(5) ELECTRONIC MAIL ADDRESS- The term `electronic mail address' means a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the `local part') and a reference to an Internet domain (commonly referred to as the `domain part'), whether or not displayed, to which an electronic mail message can be sent or delivered.

(6) ELECTRONIC MAIL MESSAGE- The term `electronic mail message' means a message sent to a unique electronic mail address.

(7) FTC ACT- The term `FTC Act' means the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(8) HEADER INFORMATION- The term `header information' means the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message.
(9) INITIATE- The term `initiate', when used with respect to a commercial electronic mail message, means to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message. For purposes of this paragraph, more than one person may be considered to have initiated a message.
(10) INTERNET- The term `Internet' has the meaning given that term in the Internet Tax Freedom Act (47 U.S.C. 151 nt).
(11) INTERNET ACCESS SERVICE- The term `Internet access service' has the meaning given that term in section 231(e)(4) of the Communications Act of 1934 (47 U.S.C. 231(e)(4)).
(12) PROCURE- The term `procure', when used with respect to the initiation of a commercial electronic mail message, means intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one's behalf.
(13) PROTECTED COMPUTER- The term `protected computer' has the meaning given that term in section 1030(e)(2)(B) of title 18, United States Code.
(14) RECIPIENT- The term `recipient', when used with respect to a commercial electronic mail message, means an authorized user of the electronic mail address to which the message was sent or delivered. If a recipient of a commercial electronic mail message has one or more electronic mail addresses in addition to the address to which the message was sent or delivered, the recipient shall be treated as a separate recipient with respect to each such address. If an electronic mail address is reassigned to a new user, the new user shall not be treated as a recipient of any commercial electronic mail message sent or delivered to that address before it was reassigned.
(15) ROUTINE CONVEYANCE- The term `routine conveyance' means the transmission, routing, relaying, handling, or storing, through an automatic technical process, of an electronic mail message for which another person has identified the recipients or provided the recipient addresses.
(16) SENDER-

(A) IN GENERAL- Except as provided in subparagraph (B), the term `sender', when used with respect to a commercial electronic mail message, means a person who initiates such a message and whose product, service, or Internet web site is advertised or promoted by the message.

(B) SEPARATE LINES OF BUSINESS OR DIVISIONS- If an entity operates through separate lines of business or divisions and

holds itself out to the recipient throughout the message as that particular line of business or division rather than as the entity of which such line of business or division is a part, then the line of business or the division shall be treated as the sender of such message for purposes of this Act.

(17) Transactional or relationship message-

(A) IN GENERAL- The term `transactional or relationship message' means an electronic mail message the primary purpose of which is--

(i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender;

(ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;

(iii) to provide--

(I) notification concerning a change in the terms or features of;

(II) notification of a change in the recipient's standing or status with respect to; or

(III) at regular periodic intervals, account balance information or other type of account statement with respect to,

a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender;

(iv) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(v) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

(B) MODIFICATION OF DEFINITION- The Commission by regulation pursuant to section 13 may modify the definition in subparagraph (A) to expand or contract the categories of messages that are treated as transactional or relationship messages for purposes of this Act to the extent that such modification is necessary to accommodate changes in electronic mail technology or practices and accomplish the purposes of this Act.

SEC. 4. PROHIBITION AGAINST PREDATORY AND ABUSIVE COMMERCIAL E-MAIL.

(a) OFFENSE-

(1) IN GENERAL- Chapter 47 of title 18, United States Code, is amended by adding at the end the following new section:

`Sec. 1037. Fraud and related activity in connection with electronic mail

`(a) IN GENERAL- Whoever, in or affecting interstate or foreign commerce, knowingly--

`(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,

`(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,

`(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,

`(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or

`(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses,

or conspires to do so, shall be punished as provided in subsection (b).

`(b) PENALTIES- The punishment for an offense under subsection (a) is--

`(1) a fine under this title, imprisonment for not more than 5 years, or both, if--

`(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

`(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

`(2) a fine under this title, imprisonment for not more than 3 years, or both, if--

`(A) the offense is an offense under subsection (a)(1);

`(B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations;

`(C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period;

`(D) the offense caused loss to one or more persons aggregating $5,000 or more in value during any 1-year period;

`(E) as a result of the offense any individual committing the offense obtained anything of value aggregating $5,000 or more during any 1-year period; or

`(F) the offense was undertaken by the defendant in concert with three or more other persons with respect to whom the defendant occupied a position of organizer or leader; and

`(3) a fine under this title or imprisonment for not more than 1 year, or both, in any other case.

`(c) FORFEITURE-

`(1) IN GENERAL- The court, in imposing sentence on a person who is convicted of an offense under this section, shall order that the defendant forfeit to the United States--

`(A) any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and

`(B) any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

`(2) PROCEDURES- The procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) of that section, and in Rule 32.2 of the Federal Rules of Criminal Procedure, shall apply to all stages of a criminal forfeiture proceeding under this section.

`(d) DEFINITIONS- In this section:

`(1) LOSS- The term `loss' has the meaning given that term in section 1030(e) of this title.

`(2) MATERIALLY- For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.

`(3) MULTIPLE- The term `multiple' means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period.

`(4) OTHER TERMS- Any other term has the meaning given that term by section 3 of the CAN-SPAM Act of 2003.'.

(2) CONFORMING AMENDMENT- The chapter analysis for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

`Sec.

`1037. Fraud and related activity in connection with electronic mail.'.

(b) UNITED STATES SENTENCING COMMISSION-

(1) DIRECTIVE- Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this section, the United States Sentencing Commission shall review and, as appropriate, amend the sentencing guidelines and policy statements to provide appropriate penalties for violations of section 1037 of title 18, United States Code, as added by this section, and other offenses that may be facilitated by the sending of large quantities of unsolicited electronic mail.

(2) REQUIREMENTS- In carrying out this subsection, the Sentencing Commission shall consider providing sentencing enhancements for--

(A) those convicted under section 1037 of title 18, United States Code, who--

(i) obtained electronic mail addresses through improper means, including--

(I) harvesting electronic mail addresses of the users of a website, proprietary service, or other online public forum operated by another person, without the authorization of such person; and

(II) randomly generating electronic mail addresses by computer; or

(ii) knew that the commercial electronic mail messages involved in the offense contained or advertised an Internet domain for which the registrant of the domain had provided false registration information; and

(B) those convicted of other offenses, including offenses involving fraud, identity theft, obscenity, child pornography, and the sexual exploitation of children, if such offenses involved the sending of large quantities of electronic mail.

(c) SENSE OF CONGRESS- It is the sense of Congress that--

(1) Spam has become the method of choice for those who distribute pornography, perpetrate fraudulent schemes, and introduce viruses, worms, and Trojan horses into personal and business computer systems; and

(2) the Department of Justice should use all existing law enforcement tools to investigate and prosecute those who send bulk commercial e-mail to facilitate the commission of Federal crimes, including the tools contained in chapters 47 and 63 of title 18, United States Code (relating to fraud and false statements); chapter 71 of title 18, United States Code (relating to obscenity); chapter 110 of title 18, United States Code (relating to the sexual exploitation of children); and chapter 95 of title 18, United States Code (relating to racketeering), as appropriate.

SEC. 5. OTHER PROTECTIONS FOR USERS OF COMMERCIAL ELECTRONIC MAIL.

(a) REQUIREMENTS FOR TRANSMISSION OF MESSAGES-

(1) PROHIBITION OF FALSE OR MISLEADING TRANSMISSION INFORMATION- It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading. For purposes of this paragraph--

(A) header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading;

(B) a `from' line (the line identifying or purporting to identify a person initiating the message) that accurately identifies any person who initiated the message shall not be considered materially false or materially misleading; and

(C) header information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin.

(2) PROHIBITION OF DECEPTIVE SUBJECT HEADINGS- It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message if such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message (consistent with the criteria used in enforcement of section 5 of the Federal Trade Commission Act (15 U.S.C. 45)).

(3) Inclusion of return address or comparable mechanism in commercial electronic mail-

(A) IN GENERAL- It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that--

(i) a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and

(ii) remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message.

(B) MORE DETAILED OPTIONS POSSIBLE- The person initiating a commercial electronic mail message may comply with subparagraph (A)(i) by providing the recipient a list or menu from which the recipient may choose the specific types of commercial electronic mail messages the recipient wants to receive or does not want to receive from the sender, if the list or menu includes an option under which the recipient may choose not to receive any commercial electronic mail messages from the sender.

(C) TEMPORARY INABILITY TO RECEIVE MESSAGES OR PROCESS REQUESTS- A return electronic mail address or other mechanism does not fail to satisfy the requirements of subparagraph (A) if it is unexpectedly and temporarily unable to receive messages or process requests due to a technical problem beyond the control of the sender if the problem is corrected within a reasonable time period.

(4) PROHIBITION OF TRANSMISSION OF COMMERCIAL ELECTRONIC MAIL AFTER OBJECTION-

(A) IN GENERAL- If a recipient makes a request using a mechanism provided pursuant to paragraph (3) not to receive some or any commercial electronic mail messages from such sender, then it is unlawful--

(i) for the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message that falls within the scope of the request;

(ii) for any person acting on behalf of the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message falls within the scope of the request;

(iii) for any person acting on behalf of the sender to assist in initiating the transmission to the recipient, through the provision or selection of addresses to which the message will be sent, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message would violate clause (i) or (ii); or

(iv) for the sender, or any other person who knows that the recipient has made such a request, to sell, lease, exchange, or otherwise transfer or release the electronic mail address of the recipient (including through any transaction or other transfer involving mailing lists bearing the electronic mail address of the recipient) for any purpose other than compliance with this Act or other provision of law.

(B) SUBSEQUENT AFFIRMATIVE CONSENT- A prohibition in subparagraph (A) does not apply if there is affirmative consent by the recipient subsequent to the request under subparagraph (A).

(5) INCLUSION OF IDENTIFIER, OPT-OUT, AND PHYSICAL ADDRESS IN COMMERCIAL ELECTRONIC MAIL- (A) It is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides--

(i) clear and conspicuous identification that the message is an advertisement or solicitation;

(ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and

(iii) a valid physical postal address of the sender.

(B) Subparagraph (A)(i) does not apply to the transmission of a commercial electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

(6) MATERIALLY- For purposes of paragraph (1), the term `materially', when used with respect to false or misleading header information, includes the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

(b) Aggravated Violations Relating to Commercial Electronic Mail-

(1) Address harvesting and dictionary attacks-

(A) IN GENERAL- It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message that is unlawful under subsection (a), or to assist in the origination of such message through the provision or selection of addresses to which the message will be transmitted, if such person had actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that--

(i) the electronic mail address of the recipient was obtained using an automated means from an Internet website or proprietary online service operated by another person, and such website or online service included, at the time the address was obtained, a notice stating that the operator of such website or online service will not give, sell, or otherwise transfer addresses maintained by such website or online service to any other party for the purposes of initiating, or enabling others to initiate, electronic mail messages; or

(ii) the electronic mail address of the recipient was obtained using an automated means that generates possible

electronic mail addresses by combining names, letters, or numbers into numerous permutations.

(B) DISCLAIMER- Nothing in this paragraph creates an ownership or proprietary interest in such electronic mail addresses.

(2) AUTOMATED CREATION OF MULTIPLE ELECTRONIC MAIL ACCOUNTS- It is unlawful for any person to use scripts or other automated means to register for multiple electronic mail accounts or online user accounts from which to transmit to a protected computer, or enable another person to transmit to a protected computer, a commercial electronic mail message that is unlawful under subsection (a).

(3) RELAY OR RETRANSMISSION THROUGH UNAUTHORIZED ACCESS- It is unlawful for any person knowingly to relay or retransmit a commercial electronic mail message that is unlawful under subsection (a) from a protected computer or computer network that such person has accessed without authorization.

(c) SUPPLEMENTARY RULEMAKING AUTHORITY- The Commission shall by regulation, pursuant to section 13--

(1) modify the 10-business-day period under subsection (a)(4)(A) or subsection (a)(4)(B), or both, if the Commission determines that a different period would be more reasonable after taking into account--

(A) the purposes of subsection (a);

(B) the interests of recipients of commercial electronic mail; and

(C) the burdens imposed on senders of lawful commercial electronic mail; and

(2) specify additional activities or practices to which subsection (b) applies if the Commission determines that those activities or practices are contributing substantially to the proliferation of commercial electronic mail messages that are unlawful under subsection (a).

(d) REQUIREMENT TO PLACE WARNING LABELS ON COMMERCIAL ELECTRONIC MAIL CONTAINING SEXUALLY ORIENTED MATERIAL-

(1) IN GENERAL- No person may initiate in or affecting interstate commerce the transmission, to a protected computer, of any commercial electronic mail message that includes sexually oriented material and--

(A) fail to include in subject heading for the electronic mail message the marks or notices prescribed by the Commission under this subsection; or

(B) fail to provide that the matter in the message that is initially viewable to the recipient, when the message is opened by any recipient and absent any further actions by the recipient, includes only--

(i) to the extent required or authorized pursuant to paragraph (2), any such marks or notices;

(ii) the information required to be included in the message pursuant to subsection (a)(5); and

(iii) instructions on how to access, or a mechanism to access, the sexually oriented material.

(2) PRIOR AFFIRMATIVE CONSENT- Paragraph (1) does not apply to the transmission of an electronic mail message if the recipient has given prior affirmative consent to receipt of the message.
(3) PRESCRIPTION OF MARKS AND NOTICES- Not later than 120 days after the date of the enactment of this Act, the Commission in consultation with the Attorney General shall prescribe clearly identifiable marks or notices to be included in or associated with commercial electronic mail that contains sexually oriented material, in order to inform the recipient of that fact and to facilitate filtering of such electronic mail. The Commission shall publish in the Federal Register and provide notice to the public of the marks or notices prescribed under this paragraph.
(4) DEFINITION- In this subsection, the term `sexually oriented material' means any material that depicts sexually explicit conduct (as that term is defined in section 2256 of title 18, United States Code), unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters.
(5) PENALTY- Whoever knowingly violates paragraph (1) shall be fined under title 18, United States Code, or imprisoned not more than 5 years, or both.

SEC. 6. BUSINESSES KNOWINGLY PROMOTED BY ELECTRONIC MAIL WITH FALSE OR MISLEADING TRANSMISSION INFORMATION.

(a) IN GENERAL- It is unlawful for a person to promote, or allow the promotion of, that person's trade or business, or goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business, in a commercial electronic mail message the transmission of which is in violation of section 5(a)(1) if that person--
(1) knows, or should have known in the ordinary course of that person's trade or business, that the goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business were being promoted in such a message;
(2) received or expected to receive an economic benefit from such promotion; and
(3) took no reasonable action--
(A) to prevent the transmission; or
(B) to detect the transmission and report it to the Commission.
(b) Limited Enforcement Against Third Parties-
(1) IN GENERAL- Except as provided in paragraph (2), a person (hereinafter referred to as the `third party') that provides goods, products, property, or services to another person that violates subsection (a) shall not be held liable for such violation.
(2) EXCEPTION- Liability for a violation of subsection (a) shall be imputed to a third party that provides goods, products, property, or services to another person that violates subsection (a) if that third party--

(A) owns, or has a greater than 50 percent ownership or economic interest in, the trade or business of the person that violated subsection (a); or

(B)(i) has actual knowledge that goods, products, property, or services are promoted in a commercial electronic mail message the transmission of which is in violation of section 5(a)(1); and

(ii) receives, or expects to receive, an economic benefit from such promotion.

(c) EXCLUSIVE ENFORCEMENT BY FTC- Subsections (f) and (g) of section 7 do not apply to violations of this section.

(d) SAVINGS PROVISION- Except as provided in section 7(f)(8), nothing in this section may be construed to limit or prevent any action that may be taken under this Act with respect to any violation of any other section of this Act.

SEC. 7. ENFORCEMENT GENERALLY.

(a) VIOLATION IS UNFAIR OR DECEPTIVE ACT OR PRACTICE- Except as provided in subsection (b), this Act shall be enforced by the Commission as if the violation of this Act were an unfair or deceptive act or practice proscribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(b) ENFORCEMENT BY CERTAIN OTHER AGENCIES- Compliance with this Act shall be enforced--

(1) under section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of--

(A) national banks, and Federal branches and Federal agencies of foreign banks, by the Office of the Comptroller of the Currency;

(B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 and 611), and bank holding companies, by the Board;

(C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System) and insured State branches of foreign banks, by the Board of Directors of the Federal Deposit Insurance Corporation; and

(D) savings associations the deposits of which are insured by the Federal Deposit Insurance Corporation, by the Director of the Office of Thrift Supervision;

(2) under the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the Board of the National Credit Union Administration with respect to any Federally insured credit union;

(3) under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.) by the Securities and Exchange Commission with respect to any broker or dealer;
(4) under the Investment Company Act of 1940 (15 U.S.C. 80a-1 et seq.) by the Securities and Exchange Commission with respect to investment companies;
(5) under the Investment Advisers Act of 1940 (15 U.S.C. 80b-1 et seq.) by the Securities and Exchange Commission with respect to investment advisers registered under that Act;
(6) under State insurance law in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled, subject to section 104 of the Gramm-Bliley-Leach Act (15 U.S.C. 6701), except that in any State in which the State insurance authority elects not to exercise this power, the enforcement authority pursuant to this Act shall be exercised by the Commission in accordance with subsection (a);
(7) under part A of subtitle VII of title 49, United States Code, by the Secretary of Transportation with respect to any air carrier or foreign air carrier subject to that part;
(8) under the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.) (except as provided in section 406 of that Act (7 U.S.C. 226, 227)), by the Secretary of Agriculture with respect to any activities subject to that Act;
(9) under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.) by the Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association; and
(10) under the Communications Act of 1934 (47 U.S.C. 151 et seq.) by the Federal Communications Commission with respect to any person subject to the provisions of that Act.

(c) EXERCISE OF CERTAIN POWERS- For the purpose of the exercise by any agency referred to in subsection (b) of its powers under any Act referred to in that subsection, a violation of this Act is deemed to be a violation of a Federal Trade Commission trade regulation rule. In addition to its powers under any provision of law specifically referred to in subsection (b), each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this Act, any other authority conferred on it by law.

(d) ACTIONS BY THE COMMISSION- The Commission shall prevent any person from violating this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any entity that violates any provision of that subtitle is subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of that subtitle.

(e) AVAILABILITY OF CEASE-AND-DESIST ORDERS AND INJUNCTIVE RELIEF WITHOUT SHOWING OF KNOWLEDGE- Notwithstanding any other provision of this Act, in any proceeding or action pursuant to subsection (a), (b), (c), or (d) of this section to enforce compliance, through an order to cease and desist or an injunction, with section 5(a)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3), neither the Commission nor the Federal Communications Commission shall be required to allege or prove the state of mind required by such section or subparagraph.

(f) Enforcement by States-

(1) CIVIL ACTION- In any case in which the attorney general of a State, or an official or agency of a State, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates paragraph (1) or (2) of section 5(a), who violates section 5(d), or who engages in a pattern or practice that violates paragraph (3), (4), or (5) of section 5(a), of this Act, the attorney general, official, or agency of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction--

(A) to enjoin further violation of section 5 of this Act by the defendant; or

(B) to obtain damages on behalf of residents of the State, in an amount equal to the greater of--

(i) the actual monetary loss suffered by such residents; or

(ii) the amount determined under paragraph (3).

(2) AVAILABILITY OF INJUNCTIVE RELIEF WITHOUT SHOWING OF KNOWLEDGE- Notwithstanding any other provision of this Act, in a civil action under paragraph (1)(A) of this subsection, the attorney general, official, or agency of the State shall not be required to allege or prove the state of mind required by section 5(a)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3).

(3) Statutory damages-

(A) IN GENERAL- For purposes of paragraph (1)(B)(ii), the amount determined under this paragraph is the amount calculated by multiplying the number of violations (with each separately addressed unlawful message received by or addressed to such residents treated as a separate violation) by up to $250.

(B) LIMITATION- For any violation of section 5 (other than section 5(a)(1)), the amount determined under subparagraph (A) may not exceed $2,000,000.

(C) AGGRAVATED DAMAGES- The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph if--

(i) the court determines that the defendant committed the violation willfully and knowingly; or

(ii) the defendant's unlawful activity included one or more of the aggravating violations set forth in section 5(b).

(D) REDUCTION OF DAMAGES- In assessing damages under subparagraph (A), the court may consider whether--

(i) the defendant has established and implemented, with due care, commercially reasonable practices and procedures designed to effectively prevent such violations; or

(ii) the violation occurred despite commercially reasonable efforts to maintain compliance the practices and procedures to which reference is made in clause (i).

(4) ATTORNEY FEES- In the case of any successful action under paragraph (1), the court, in its discretion, may award the costs of the action and reasonable attorney fees to the State.

(5) RIGHTS OF FEDERAL REGULATORS- The State shall serve prior written notice of any action under paragraph (1) upon the Federal Trade Commission or the appropriate Federal regulator determined under subsection (b) and provide the Commission or appropriate Federal regulator with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Federal Trade Commission or appropriate Federal regulator shall have the right--

(A) to intervene in the action;

(B) upon so intervening, to be heard on all matters arising therein;

(C) to remove the action to the appropriate United States district court; and

(D) to file petitions for appeal.

(6) CONSTRUCTION- For purposes of bringing any civil action under paragraph (1), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to--

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(7) VENUE; SERVICE OF PROCESS-

(A) VENUE- Any action brought under paragraph (1) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS- In an action brought under paragraph (1), process may be served in any district in which the defendant--

(i) is an inhabitant; or

(ii) maintains a physical place of business.

(8) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING- If the Commission, or other appropriate Federal agency under subsection (b), has instituted a civil action or an administrative action for

violation of this Act, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission or the other agency for any violation of this Act alleged in the complaint.

(9) REQUISITE SCIENTER FOR CERTAIN CIVIL ACTIONS- Except as provided in section 5(a)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3), in a civil action brought by a State attorney general, or an official or agency of a State, to recover monetary damages for a violation of this Act, the court shall not grant the relief sought unless the attorney general, official, or agency establishes that the defendant acted with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, of the act or omission that constitutes the violation.

(g) Action by Provider of Internet Access Service-

(1) ACTION AUTHORIZED- A provider of Internet access service adversely affected by a violation of section 5(a)(1), 5(b), or 5(d), or a pattern or practice that violates paragraph (2), (3), (4), or (5) of section 5(a), may bring a civil action in any district court of the United States with jurisdiction over the defendant--

(A) to enjoin further violation by the defendant; or

(B) to recover damages in an amount equal to the greater of--

(i) actual monetary loss incurred by the provider of Internet access service as a result of such violation; or

(ii) the amount determined under paragraph (3).

(2) SPECIAL DEFINITION OF `PROCURE'- In any action brought under paragraph (1), this Act shall be applied as if the definition of the term `procure' in section 3(12) contained, after `behalf' the words `with actual knowledge, or by consciously avoiding knowing, whether such person is engaging, or will engage, in a pattern or practice that violates this Act'.

(3) STATUTORY DAMAGES-

(A) IN GENERAL- For purposes of paragraph (1)(B)(ii), the amount determined under this paragraph is the amount calculated by multiplying the number of violations (with each separately addressed unlawful message that is transmitted or attempted to be transmitted over the facilities of the provider of Internet access service, or that is transmitted or attempted to be transmitted to an electronic mail address obtained from the provider of Internet access service in violation of section 5(b)(1)(A)(i), treated as a separate violation) by--

(i) up to $100, in the case of a violation of section 5(a)(1); or

(ii) up to $25, in the case of any other violation of section 5.

(B) LIMITATION- For any violation of section 5 (other than section 5(a)(1)), the amount determined under subparagraph (A) may not exceed $1,000,000.

(C) AGGRAVATED DAMAGES- The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph if--

(i) the court determines that the defendant committed the violation willfully and knowingly; or

(ii) the defendant's unlawful activity included one or more of the aggravated violations set forth in section 5(b).

(D) REDUCTION OF DAMAGES- In assessing damages under subparagraph (A), the court may consider whether--

(i) the defendant has established and implemented, with due care, commercially reasonable practices and procedures designed to effectively prevent such violations; or

(ii) the violation occurred despite commercially reasonable efforts to maintain compliance with the practices and procedures to which reference is made in clause (i).

(4) ATTORNEY FEES- In any action brought pursuant to paragraph (1), the court may, in its discretion, require an undertaking for the payment of the costs of such action, and assess reasonable costs, including reasonable attorneys' fees, against any party.

SEC. 8. EFFECT ON OTHER LAWS.

(a) FEDERAL LAW- (1) Nothing in this Act shall be construed to impair the enforcement of section 223 or 231 of the Communications Act of 1934 (47 U.S.C. 223 or 231, respectively), chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute.

(2) Nothing in this Act shall be construed to affect in any way the Commission's authority to bring enforcement actions under FTC Act for materially false or deceptive representations or unfair practices in commercial electronic mail messages.

(b) STATE LAW-

(1) IN GENERAL- This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.

(2) STATE LAW NOT SPECIFIC TO ELECTRONIC MAIL- This Act shall not be construed to preempt the applicability of--

(A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or

(B) other State laws to the extent that those laws relate to acts of fraud or computer crime.

(c) NO EFFECT ON POLICIES OF PROVIDERS OF INTERNET ACCESS SERVICE- Nothing in this Act shall be construed to have any effect on the lawfulness or unlawfulness, under any other provision of law, of the adoption, implementation, or enforcement by a provider of Internet access service of a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages.

SEC. 9. DO-NOT-E-MAIL REGISTRY.

(a) IN GENERAL- Not later than 6 months after the date of enactment of this Act, the Commission shall transmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce a report that--

(1) sets forth a plan and timetable for establishing a nationwide marketing Do-Not-E-Mail registry;

(2) includes an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a registry; and

(3) includes an explanation of how the registry would be applied with respect to children with e-mail accounts.

(b) AUTHORIZATION TO IMPLEMENT- The Commission may establish and implement the plan, but not earlier than 9 months after the date of enactment of this Act.

SEC. 10. STUDY OF EFFECTS OF COMMERCIAL ELECTRONIC MAIL.

(a) IN GENERAL- Not later than 24 months after the date of the enactment of this Act, the Commission, in consultation with the Department of Justice and other appropriate agencies, shall submit a report to the Congress that provides a detailed analysis of the effectiveness and enforcement of the provisions of this Act and the need (if any) for the Congress to modify such provisions.

(b) REQUIRED ANALYSIS- The Commission shall include in the report required by subsection (a)--

(1) an analysis of the extent to which technological and marketplace developments, including changes in the nature of the devices through which consumers access their electronic mail messages, may affect the practicality and effectiveness of the provisions of this Act;

(2) analysis and recommendations concerning how to address commercial electronic mail that originates in or is transmitted through or to facilities or computers in other nations, including initiatives or policy positions that the Federal Government could pursue through international negotiations, fora, organizations, or institutions; and

(3) analysis and recommendations concerning options for protecting consumers, including children, from the receipt and viewing of commercial electronic mail that is obscene or pornographic.

SEC. 11. IMPROVING ENFORCEMENT BY PROVIDING REWARDS FOR INFORMATION ABOUT VIOLATIONS; LABELING.

The Commission shall transmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce--

(1) a report, within 9 months after the date of enactment of this Act, that sets forth a system for rewarding those who supply information about violations of this Act, including--

(A) procedures for the Commission to grant a reward of not less than 20 percent of the total civil penalty collected for a violation of this Act to the first person that--

(i) identifies the person in violation of this Act; and

(ii) supplies information that leads to the successful collection of a civil penalty by the Commission; and

(B) procedures to minimize the burden of submitting a complaint to the Commission concerning violations of this Act, including procedures to allow the electronic submission of complaints to the Commission; and

(2) a report, within 18 months after the date of enactment of this Act, that sets forth a plan for requiring commercial electronic mail to be identifiable from its subject line, by means of compliance with Internet Engineering Task Force Standards, the use of the characters `ADV' in the subject line, or other comparable identifier, or an explanation of any concerns the Commission has that cause the Commission to recommend against the plan.

SEC. 12. RESTRICTIONS ON OTHER TRANSMISSIONS.

Section 227(b)(1) of the Communications Act of 1934 (47 U.S.C. 227(b)(1)) is amended, in the matter preceding subparagraph (A), by inserting `, or any person outside the United States if the recipient is within the United States' after `United States'.

SEC. 13. REGULATIONS.

(a) IN GENERAL- The Commission may issue regulations to implement the provisions of this Act (not including the amendments made by sections 4 and 12). Any such regulations shall be issued in accordance with section 553 of title 5, United States Code.

(b) LIMITATION- Subsection (a) may not be construed to authorize the Commission to establish a requirement pursuant to section 5(a)(5)(A) to include any specific words, characters, marks, or labels in a commercial electronic mail

message, or to include the identification required by section 5(a)(5)(A) in any particular part of such a mail message (such as the subject line or body).

SEC. 14. APPLICATION TO WIRELESS.

(a) EFFECT ON OTHER LAW- Nothing in this Act shall be interpreted to preclude or override the applicability of section 227 of the Communications Act of 1934 (47 U.S.C. 227) or the rules prescribed under section 3 of the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. 6102).
(b) FCC RULEMAKING- The Federal Communications Commission, in consultation with the Federal Trade Commission, shall promulgate rules within 270 days to protect consumers from unwanted mobile service commercial messages. The Federal Communications Commission, in promulgating the rules, shall, to the extent consistent with subsection (c)--

(1) provide subscribers to commercial mobile services the ability to avoid receiving mobile service commercial messages unless the subscriber has provided express prior authorization to the sender, except as provided in paragraph (3);
(2) allow recipients of mobile service commercial messages to indicate electronically a desire not to receive future mobile service commercial messages from the sender;
(3) take into consideration, in determining whether to subject providers of commercial mobile services to paragraph (1), the relationship that exists between providers of such services and their subscribers, but if the Commission determines that such providers should not be subject to paragraph (1), the rules shall require such providers, in addition to complying with the other provisions of this Act, to allow subscribers to indicate a desire not to receive future mobile service commercial messages from the provider--

(A) at the time of subscribing to such service; and
(B) in any billing mechanism; and

(4) determine how a sender of mobile service commercial messages may comply with the provisions of this Act, considering the unique technical aspects, including the functional and character limitations, of devices that receive such messages.

(c) OTHER FACTORS CONSIDERED- The Federal Communications Commission shall consider the ability of a sender of a commercial electronic mail message to reasonably determine that the message is a mobile service commercial message.
(d) MOBILE SERVICE COMMERCIAL MESSAGE DEFINED- In this section, the term `mobile service commercial message' means a commercial electronic mail message that is transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service (as such term is defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d))) in connection with such service.

SEC. 15. SEPARABILITY.

If any provision of this Act or the application thereof to any person or circumstance is held invalid, the remainder of this Act and the application of such provision to other persons or circumstances shall not be affected.

SEC. 16. EFFECTIVE DATE.

The provisions of this Act, other than section 9, shall take effect on January 1, 2004.